

MELBOURNE SURVEILLANCE TRACK



This walking tour was developed by Digital Rights Watch as part of the City of Melbourne's 2021 Melbourne Knowledge Week.

We acknowledge the traditional owners of the land that this track traverses: the Bunurong Boon Wurrung and Wurundjeri Woi Wurrung peoples of the Eastern Kulin Nation.

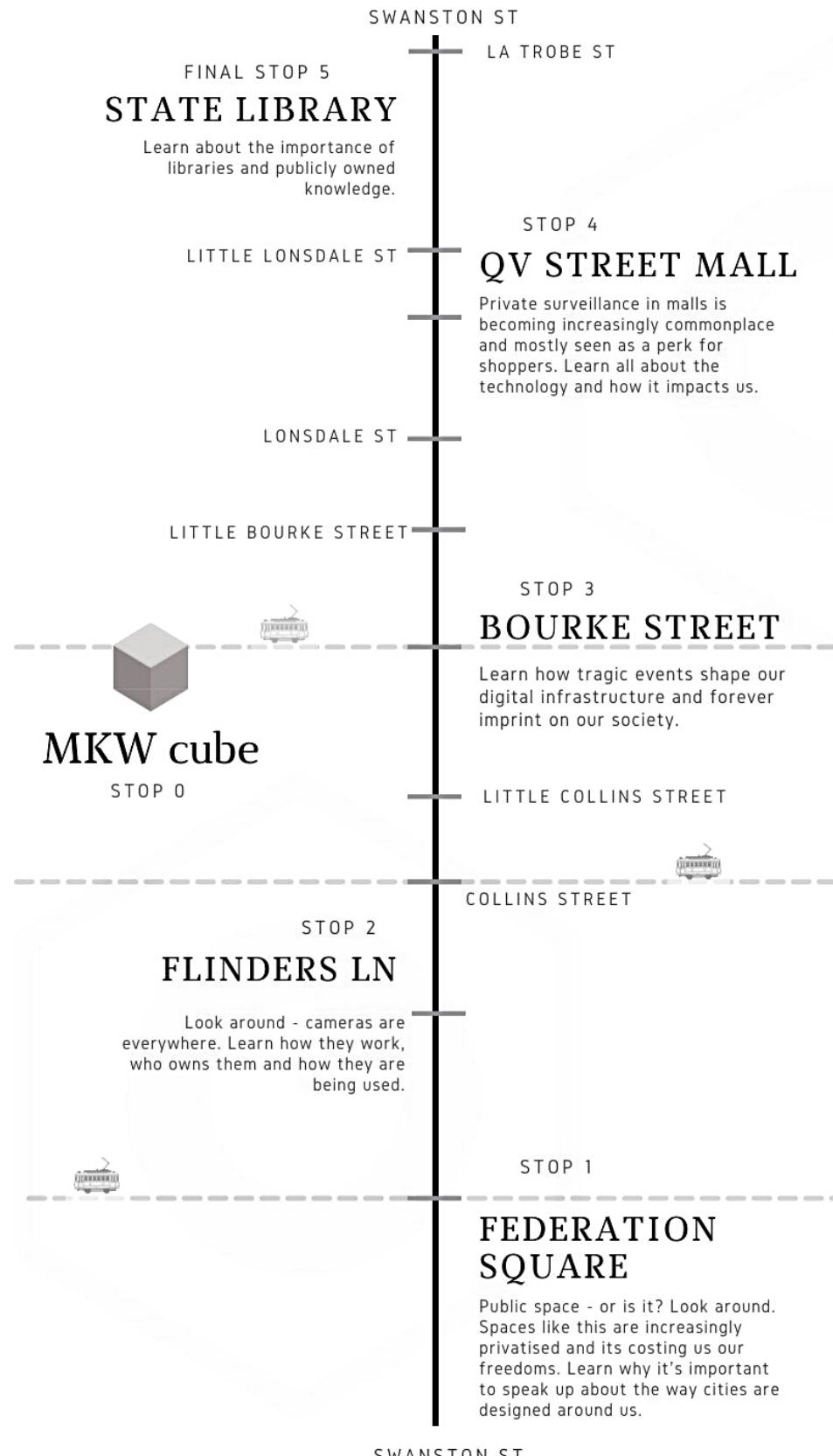
Many of the systems of surveillance discussed on this tour have roots in Australia's history of colonisation, and we must keep in mind that Aboriginal and Torres Strait Islander peoples in Australia continue to be subject to disproportionate surveillance and policing. We all have a role to play in understanding, questioning, and decolonising these systems.

We also want to highlight that Indigenous communities built rich systems of governance, justice, and knowledge sharing over thousands of years - which did not rely on pervasive surveillance. There is much to be learned from Indigenous knowledge about building strong communities.

We acknowledge that the sovereignty of this land was never ceded, and we wish to pay our respects to elders past, present, and emerging.



MELBOURNE SURVEILLANCE TRACK



THE ENTIRE TRACK FOLLOWS SWANSTON ST. WALK UP AND PLAY THE CORRESPONDING EPISODE AT EACH STOP.

Introduction

Surveillance is all around us - can you see it? Every day, as we walk around these public spaces, hop on a tram, go shopping, commute to work, and socialise with friends, surveillance is happening everywhere.

Government agencies, individuals, and private organisations of all sizes use public place surveillance, and it is increasing. Don't worry if you can't see it yet, by the end of this walking tour, you will be able to spot, and understand, the types of surveillance operating on the streets of Melbourne.

Our goal in this walking tour is not to freak you out. It's to equip you with an understanding of how we are observed, recorded, and tracked while going about everyday activities. As we continue to progress into an increasingly digital age, we have an opportunity to play an active role in the way our cities become "smart," but in order to do that we first have to understand what technologies are already at work all around us.

If you haven't heard the term 'smart city' before, it's a term used to describe the way that cities use technology—such as sensors, cameras—to collect data, which is then used to make systems more efficient. Sometimes this is really useful, for example, you may spot "smart bins" around the city which make the process of waste management more sustainable, environmentally friendly, and effective!

The bins don't collect any personal data, so it benefits us in keeping the streets clean, without spying on us!

Unfortunately, not all smart city trends are quite as... well, smart. Around the world, smart city technologies are beginning to seem more like pervasive surveillance.



While there may not be an expectation of privacy while we're out and about like there is in the home, that doesn't mean we agree to be tracked, monitored or recorded as we walk down the street.

As technology is increasingly being used in public spaces to observe and surveil us, it's also changing what it means to engage with public spaces. Will we still be anonymous on the streets in the future? Or will our face have a number whose movements are tracked and recorded? At Digital Rights Watch, we think technology is a powerful tool that can and should be used to help solve some of our most pressing challenges, but when it comes to smart cities, if human rights aren't at the centre, then they're just not that smart.

As we walk around today, we will keep coming back to this idea of smart cities, and how we might be able to shape them to be centered around the rights and needs of individuals and communities.



Stop 1: Federation Square

A thriving democracy needs public spaces for protest and celebration.

Across the world, parks, plazas, and promenades—which were once in the hands of public authorities—are coming under the control of private corporations. In a majority of cases this is to increase efficiency and defer costs to the private entity from the government's coffers. Yet, in spite of this overwhelming move to privatisation, it's vital for cities to find ways to preserve, manage and even create new public spaces. For one, research has shown there are physical and mental health benefits from using green open spaces. But perhaps more importantly, public spaces are the essence of a city. They are physical manifestations of the public sphere; places where different voices in society can be heard, and where people from all walks of life can meet or even protest—free of charge.

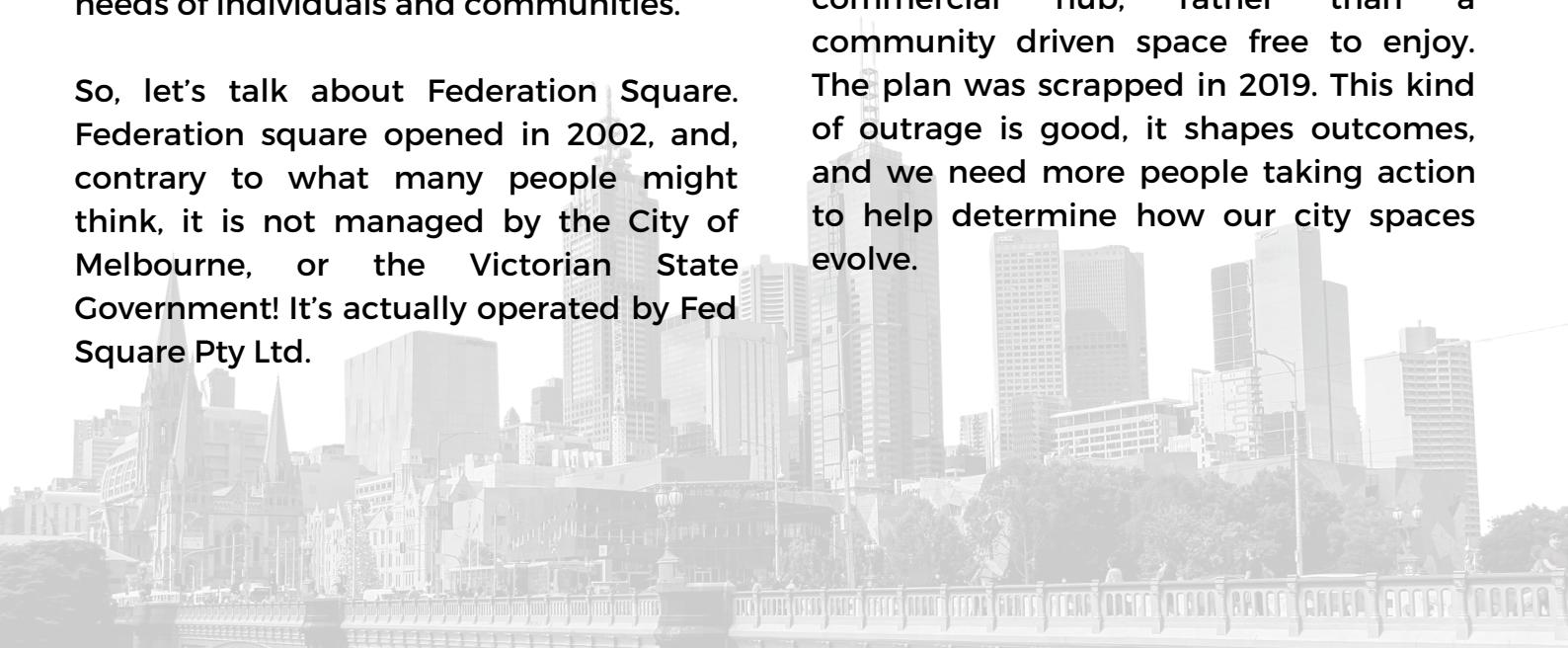
As we walk around today, we will keep coming back to this idea of smart cities, and how we might be able to shape them to be centered around the rights and needs of individuals and communities.

So, let's talk about Federation Square. Federation square opened in 2002, and, contrary to what many people might think, it is not managed by the City of Melbourne, or the Victorian State Government! It's actually operated by Fed Square Pty Ltd.

Going back in time to the early 1800s when Melbourne's grid layout was first designed, there was no allocated civic or public space, which made it unlike many other town designs. The lack of space that belonged to the people—a place for Melbournians to gather, celebrate, protest, and share ideas, was criticised as early as 1850.

Just up the road at the corner of Swanston and Collins streets, you may remember, once stood City Square—which only came about in the 1960s as Melbourne's official town square. But even back then it never really met the needs of the public, which is why in 2002 when Federation Square opened, Melbourne was thrilled.

But the encroachment of privatisation continues to threaten our public spaces. You may remember in 2017 when the Labor Government announced that a flagship Apple Store would be built at Federation Square. It provoked heated debate among Melbournians, many of whom were outraged at the prospect of Federation Square becoming a commercial hub, rather than a community driven space free to enjoy. The plan was scrapped in 2019. This kind of outrage is good, it shapes outcomes, and we need more people taking action to help determine how our city spaces evolve.



Federation Square (continued)

As a private entity, Federation Square operates a live camera stream that captures and streams a video of what is happening at Federation Square to their website, 24/7. Does it bring you a sense of comfort and community, or a sense of mild dread that you are being observed? For us it's certainly the latter, but let's hold off this for now, we will dive into cameras across our cities later along our surveillance track.

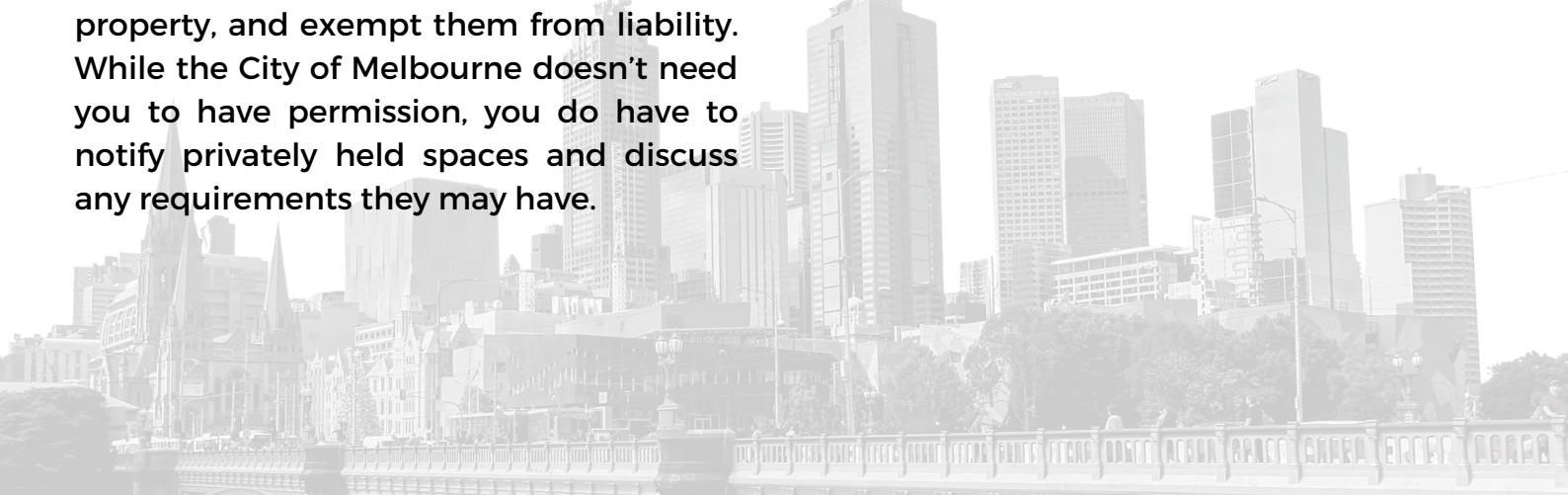
Private spaces also create challenges for protests and rallies. Our right to protest is a manifestation of freedom of assembly, freedom of association, and freedom of speech. These rights are protected by international human rights law to ensure that everyone around the world can live in free and just societies. And, as such, you don't need permission from the City of Melbourne to conduct a demonstration, rally or protest or other form of public assembly. You can let them know, and it helps with the city's planning, but it's an accessible and cheap option to gather and protest in public spaces.

This changes if your activity takes place in or passes through privately managed public spaces. There are complex fees, permits, and insurance that need to be in place to protect privately held assets and property, and exempt them from liability. While the City of Melbourne doesn't need you to have permission, you do have to notify privately held spaces and discuss any requirements they may have.

Do you know what these are in Melbourne? Well, we are at Federation Square of course, but there is also Parliament House, The Old Treasury Building, State Library of Victoria, and Queen Victoria Market. Quite a list!

So, what has this got to do with our digital rights? Well, as we will see over the rest of the track, digital rights ARE human rights, and the divide between the online and the physical world is actually much smaller than we might initially think. The right to freedom of association and freedom of speech must be protected offline as well as online, and the fact that public spaces where these rights can be exercised are shrinking is a huge concern. The existence of public spaces is essential to a thriving and fair democracy. When they are privatised, they lose a lot of their civic value and often come with increased private surveillance.

Are there other models out there? Yes, and we can rethink the maintenance of public spaces entirely. Across Europe there are many examples, like in the Municipality of Emmen, in the Netherlands, where communities experiment with a radical approach, giving power to the local people. Dream big! And talk to your local council about it, this is your city after all, so make sure it's smart in a way that works for you.



Stop 2: Flinders Lane

The City of Melbourne has the largest council-operated CCTV network in Victoria. Let's stop there for a second—what is CCTV?

CCTV stands for closed circuit television. A CCTV system connects a number of video cameras through a closed circuit or a loop, and sends the images it captures to a TV for monitoring or records them directly. 'Closed circuit' means that it's different from say, a broadcast network where anyone can tune in to watch. Modern CCTV cameras use digital technology and are part of a networked system, rather than actually operating on a closed circuit—but the name CCTV, even though not always accurate, has stuck and you will see them in cities across the world. Increasingly, CCTV is combined with software which is capable of smart surveillance. For example, some CCTV systems can track individuals, and some are compatible with facial recognition technology, allowing individuals to be identified when in view of the camera.

Alright, now back to CCTV in Melbourne. The City of Melbourne runs a 'Safe City Cameras Program' which is made up of 65 CCTV cameras around the city. (We will dive into the background of how this program developed at our next stop!)

Surveillance cameras generally have two goals: to proactively deter criminal behaviour by their very presence and to retroactively assist in crime reporting and investigations.

The notion that the presence of a surveillance camera could prevent crime from occurring is based on the theory that people will change their behaviour if they believe they are being watched—whether that is real or imagined. Often, private businesses will install cameras that are not connected to anything, just to create that fear, in the hope to deter crime.

In some cases, such as the reduction of crime, this notion of people changing their behaviour due to surveillance might seem desirable. However, the presence of surveillance can change other behaviours too, and left unchecked, has been shown to result in people self-censoring and becoming more conformist—which isn't a good recipe for a rich and diverse society or self expression. The way surveillance changes behaviour can also make it harder for people to protest and speak out against injustice—and that is not a good outcome for a fair and just democracy!

Research from 2019 has shown that the presence of CCTV in public spaces can sometimes reduce crime—but only when it is accompanied by a wide range of other approaches.

The CCTV cameras that are operated by the City of Melbourne are monitored by a team of people around the clock and have the capability to tilt, zoom and rotate 360 degrees. If you've ever been out in the city on a Friday or Saturday night, you might also have spotted Melbourne's security patrol vehicle. It roams the streets from 10pm - 6am on the weekends. It is equipped with 360-degree CCTV surveillance cameras and records everything it sees.

Flinders Lane (continued)

So the cameras are actively monitored, but is the data stored? Yes, the recordings are kept for 28 days—if no request has been made for the footage over that period, it is destroyed.

Okay, so those are the public city-owned CCTV cameras, but there are loads more cameras around Melbourne, so what are all the other cameras for?

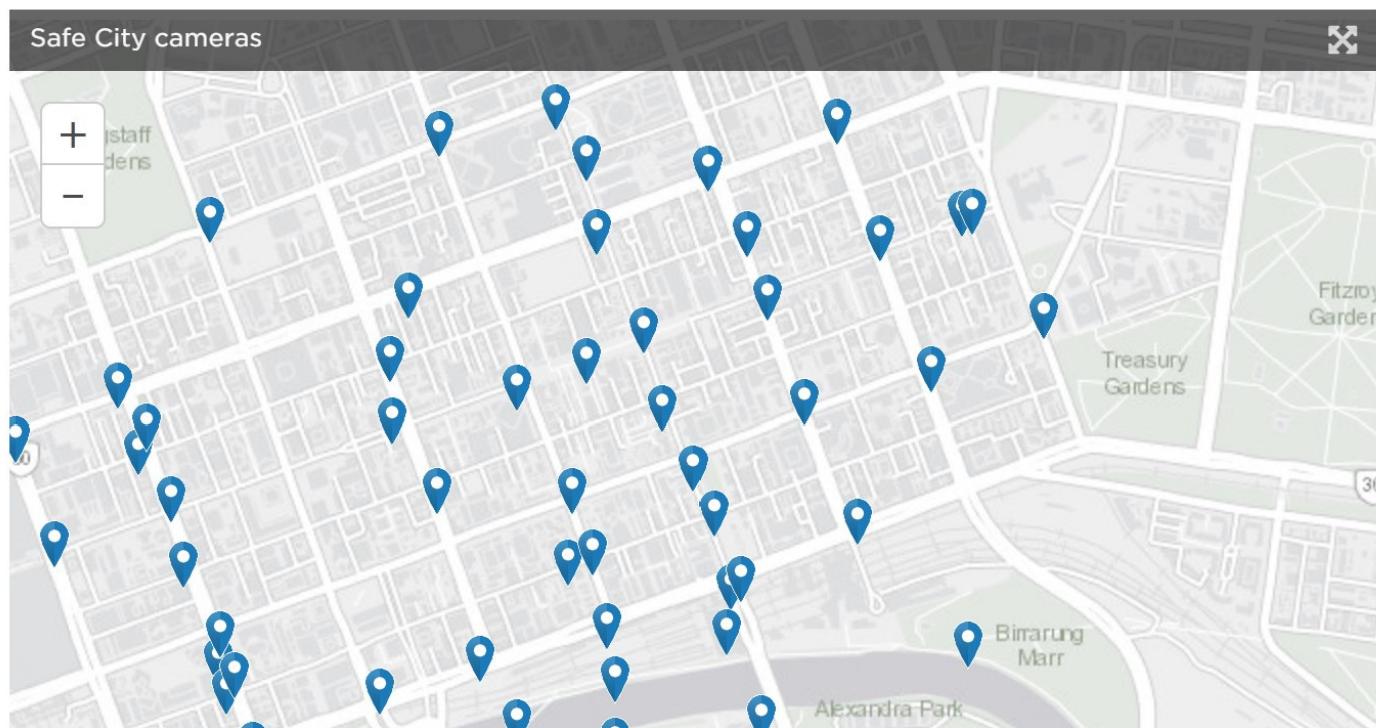
There are traffic cameras which are used to monitor and manage traffic—some owned by VicRoads, as well as private toll road operators like CityLink and EastLink. As of 2014 there were at least 700 fixed traffic cameras around Victoria, most of which can tilt and zoom. And while we're on the subject of traffic cameras, the use of automated number plate recognition systems is also on the rise. As you may have guessed from its name, this is a type of technology that automatically recognises car license plates.

On top of this, there are approximately 2000 locations across Victoria where **mobile cameras** can be operated at any time on any day—usually in unmarked vehicles parked on the side of the road, or on mobile units.

While we're here, you can see trams passing by. Transport operators also rely heavily on surveillance technologies. Cameras operate in almost all trams and trains. On top of this, Myki, the public transport ticketing system, uses RFID (radio frequency identification) in those smart plastic travel cards.

They keep a record of when people touch on and off, and of course, deduct fares. If you have set up your Myki card to automatically refill, your travel habits are associated with your identity. However, even if your name isn't associated with a myki card, it is still possible to identify individuals from their travel habits. In 2018, nearly two billion lines of myki data was released. Researchers found that it was possible to identify individuals in the dataset, despite it being 'de-identified'.

[image description: safe city camera location map]



Flinders Lane (continued)

There are also private cameras all over the city, operated by businesses and individuals. There is no mandatory or centralised CCTV register for privately owned CCTV systems, although some police stations have their own localised registers so they can call upon private operators to give them access to recorded footage when it's relevant to their investigation.

Many cameras are small and can be placed in obscure positions, and not all users of CCTV will erect signs to notify the public that they are in use. It is likely that many people do not realise the extent to which their image is being recorded as they go about their daily lives. Do you notice the cameras attached to sides of buildings as you walk about your day? If you are just realising the scope of surveillance in the city—don't worry, you're not alone!

All of these systems add up to create a complex web of surveillance around the CBD. And as we will explore in the coming stops, it isn't just about cameras. While a lot of these elements may be kept relatively separate (except for law enforcement, who broadly have access to everything if and when they want it subject to the law), the trend toward smart cities includes linking up previously distinct systems so they can work "smarter" together. We're not so sure that's the future we want to see.

Looking to the future, it is anticipated that we will see new and emerging uses of technology for surveillance purposes. For example, drones were once in the realm of science fiction...

..but are now becoming so commonplace that the police considered them as an option to enforce the pandemic curfews.

It's important that we consider how these advancements change the dynamic—these are not just CCTV cameras that fly. While in theory there are many similarities between drones and CCTV cameras, the added ability for drones to move, be controlled remotely, to peek into spaces where CCTV cameras just can't go, to catch people by surprise, and often with the added functionality to listen into conversations, completely changes dynamic—so we cannot just directly apply the way we think about CCTV to drones.

When people talk about privacy, you'll also often hear people talking about consent. You might read something like: "by using this app you consent to our terms and conditions" but what about, "if you enter this space, you consent to surveillance?" As we continue to walk, something to consider is, how could we meaningfully consent to the collection and use of our data when it is collected in ways we may not even be aware of, or understand? For example, when you walk into a shopping centre, are you implicitly agreeing to them recording your every move, or even tracking when and where you go in the store, what you look at and for how long, in order to perform behavioural analytics and increase sales? All of this already happens, both online and offline. Later, we will give more consideration to the things we're maybe 'implicitly' agreeing to, but for now, all we ask is that you sit (or rather, walk) with the question: did we consent to this? And how does this impact not just me, but everyone who moves around the city?

Stop 3: Bourke Street

Following the Bourke Street attack in 2017 where a man deliberately drove a car into pedestrians, resulting in 6 deaths and almost 30 serious injuries, the Victorian Government implemented a 52.5 million dollar security upgrade. This is not unique. Around the world, tragic events shape public spaces and rewrite legislation in reactive broad-strokes with often serious consequences to our rights and freedoms.

See those silver bollards at the entrance to the mall? There are 132 in Bourke Street Mall alone! These bollards were installed as part of this upgrade. Even the public furniture and flag poles in this area were strategically installed to create a protective pedestrian zone.

But aside from the physical measures, technological measures were also taken. The CCTV network that we spoke about earlier was expanded with an additional 31 cameras, as well as 95 sets of speakers installed around the city to create a Public Address System, so that messages can be communicated to the public in times of emergency.

While many of these measures may indeed be reasonable, the trouble is, in times of crisis, emergency or terror, we are much more likely to accept strict measures without stopping to think critically about what this may mean for our rights and freedoms. We have seen in recent history that it's very rare that these measures are ever rolled back once we return to a time of relative calm.

As an example, following the September 11 terrorist attacks on New York, Australia went through a kind of anti-terror legislation frenzy—and ended up passing more legislation than the US—much of which greatly impacts our civil liberties both online and offline.

As another example, throughout 2020 during the height of the coronavirus pandemic and Melbourne's strict lockdown measures, additional portable CCTV cameras were seen around public parks through Melbourne—to find and charge people who were 'breaking the rules.' There were also numerous reports of drone use for the same purpose. Maybe you saw them around?

While we're on the subject let's talk about what kind of surveillance law enforcement uses.

Law enforcement are one of the major users of public place surveillance. In Victoria, the police have access to state of the art surveillance technology. This includes, but definitely isn't limited to:

- **Optical surveillance**, such as CCTV, drones, as well as hand held devices, cameras fitted to police cars, and body worn cameras.
- **Audio surveillance**, such as listening devices which can be handheld or installed at specific locations.
- **Data surveillance**, through info provided by other government bodies and private organisations (according to the Victorian Law Reform Commission, this kind of collection and use of data frequently falls outside of the regulatory regime designed to deal with police use of surveillance).

Bourke Street (continued)

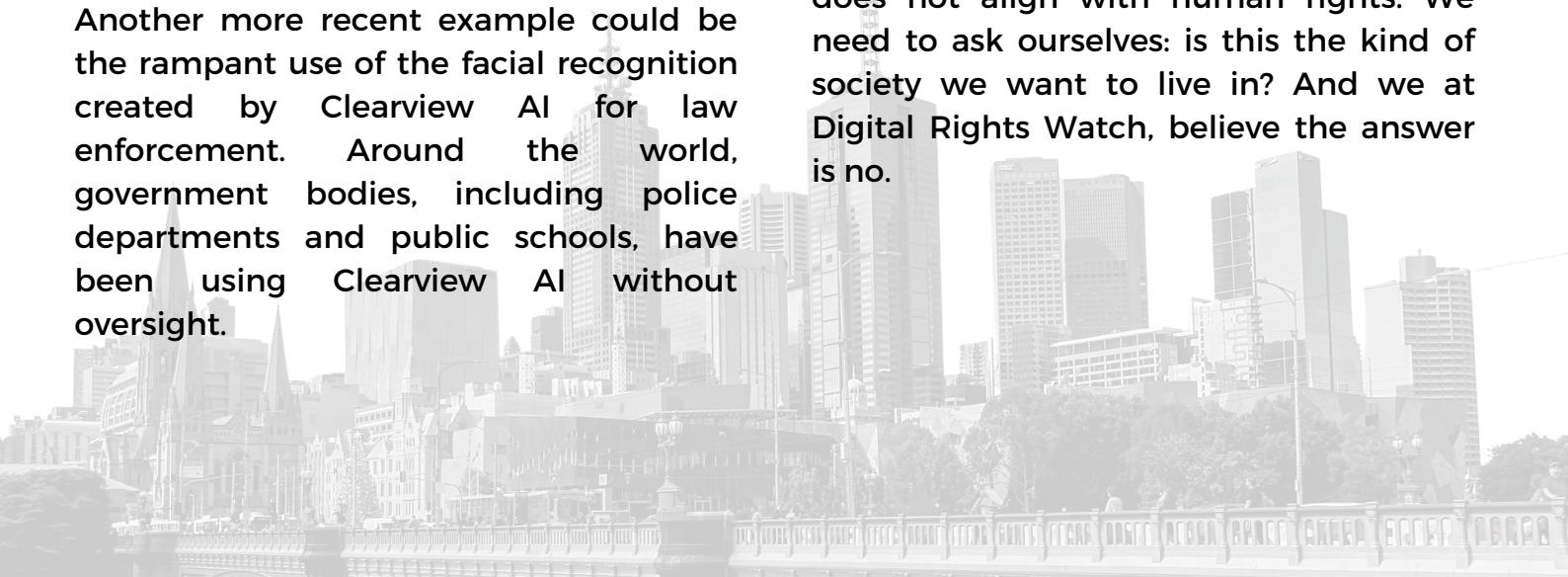
There are additional technologies, deployed during protests or other specific events, such as stingray phone trackers, used by the police. These devices essentially pretend to be cell phone towers so that when your phone sends a signal to a nearby tower (which happens whenever it receives a call or text, otherwise every half hour or so if it's not being actively used), it connects to the stingray which now becomes the middle man between your phone and the mobile tower. It sees all the traffic, that means messages, calls, images, that you send over the network during that time.

Part of the trouble is that it is hard for the public to know exactly what kind of technology is being used by law enforcement at any given time. Often, this sort of technology is privately contracted and hidden from public view. For instance, in 2020 it was reported in the US that the data broker Venntel was harvesting data and selling it back to several state departments and agencies. Data brokers who aggregate and resell data like that exist around the world and currently benefit from a regulatory grey area.

Another more recent example could be the rampant use of the facial recognition created by Clearview AI for law enforcement. Around the world, government bodies, including police departments and public schools, have been using Clearview AI without oversight.

The controversy stemmed not just from the fact that they are using facial recognition, but the fact that Clearview AI created and trained the tool by scraping data off the internet (Facebook and other social media). This is a good, albeit terrifying, example how public surveillance feeds and thrives on private surveillance and why we are concerned about both equally. The public and private sectors are in an increasingly symbiotic relationship which is being used to develop tools that police and watch us, rather than support and empower us.

Before we move on to the next stop, let's pause to consider facial recognition surveillance. Before we get ahead of ourselves, not all surveillance cameras use facial recognition technology - but the use of facial recognition is certainly on the rise, and it is something that should alarm each and every one of us. Researchers have demonstrated that the current technology available exhibits racial bias - which can lead to extremely harmful and racist outcomes when it is used in justice or law enforcement contexts. The trouble is, even if we get to the point where the technology works perfectly well, facial recognition surveillance fundamentally does not align with human rights. We need to ask ourselves: is this the kind of society we want to live in? And we at Digital Rights Watch, believe the answer is no.



MELBOURNE SURVEILLANCE TRACK



Stop 4: QV Street Mall

Ahhh, a shopping center! But it's not time for bubble tea or a quick dip to the bookstore just yet. We're here to talk about surveillance in shopping malls as they are private spaces.

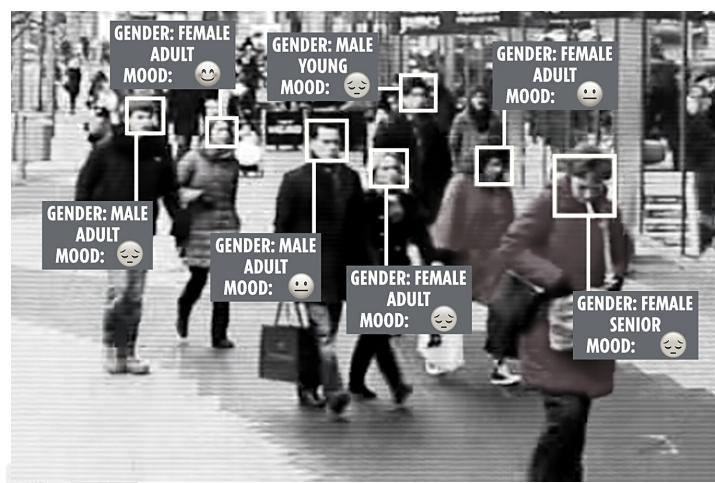
As we mentioned earlier at Federation Square, seemingly public spaces aren't always "public". It's easy to make the mistake that when walking in the halls of a shopping mall we are in a public space, after all, it's not owned by the shop until you cross their threshold right?

Actually, even open malls like this are privately owned and operated. When you walk into shopping malls, the minute you step in, you are walking into a private company's space, and inherently agreeing to their terms and conditions when you do so, even if you haven't read them... and let's face it—who has? Private companies are very aware that shopping malls are their spaces to control, and they surveil all parts of it. Some of that's for security, but increasingly that is surveillance for profit. And of course as a private company, they are not subject to the same legal limitations and restrictions that a public, government entity or agency would be. That's where regulation would come in, but unfortunately it's not keeping pace with technological developments and modern targeted advertising capabilities.

There are the obvious things, like security guards, and the security cameras that act as extra eyes because no retailer wants their stuff stolen of course...

... And spaces like shopping malls can be targets for mass atrocities, so we need to make sure we do what we can to prevent those. But the surveillance isn't always where you'd expect, and it isn't just used for preventing theft.

From now on as you walk through shopping malls and spaces, look at the advertisements around you—do you see any that are appearing on screens and other digital displays? Increasingly, these digital billboards aren't just designed to be looked at—they're looking back at you with embedded cameras and assessing your reaction and mood. In this way shopping mall corporations can get a lot of data about the people who come into their spaces by connecting these digital signage cameras up with facial detection technology. So, absent government regulation on the matter, that is precisely what they do.



[image description: mock up image of mood recognition software describing each person's gender, age, and displaying mood as an emoji]

QV Street Mall (continued)

Technologies like Val Morgan's "DART" system which stands for "digital-outdoor audience in real time" use facial analytics on the images their billboards capture (which means pictures of you, the people walking past it) to create datasets about the people using shopping centres, which they then sell back to the companies that run the centres.

The kind of analysis being performed on your image includes a lot of generalisations based on the way the ad companies' algorithms are programmed: what gender you appear to be, the age range you appear to be in, and even what mood you seem to be in.

Whether it's accurate or not, this data gets fed back to the companies that pay for it in order to show you "more relevant" ads as you walk past, or to test out different versions of ads on you to see which ones might do better with certain target audiences

Shopping malls and advertising vendors don't just use this data by itself, it gets combined with lots of other information collected about you. This can include things like shopping data. You may be surprised to learn that supermarket rewards cards aren't really about getting the best deal on a tub of ice cream, they're used to build profiles of your habits as a shopper which are then sold on to other data aggregators and brokers –and if you remember from earlier, these guys operate in legal grey areas and resell this information to the highest bidders, often combined with other datasets.

Beyond shopping data, they can also collect your individual path as you walk through the shopping centre. This is easy as the mobile phone most of us have on us actively communicates with the Wi-Fi routers they have all around the centre even if you haven't explicitly clicked to connect to their network.

Yep, even if you're not connected to the Wi-Fi, if your phone has Wi-Fi turned on, it's communicating with the routers using a unique identifier, and this can be used to track your location as you walk through the space.

This is useful for understanding practical things like crowd patterns, which can be helpful in emergency planning, but it also means they know which people go where, when—and they also know if you come back again at a later date, provided you're using the same phone. So imagine all that data stored in one big set: where you went gets cross referenced with the data advertising billboards collected about your reactions, and this profile of you grows over time. Makes you want to never go to the same shopping mall twice hey?

And we haven't even touched on the surveillance technology that's built into shopping centre parking, which scans the number plates of all the cars that enter and leave, and keeps a record of when they do. Of course at a benign level this is helpful to shoppers to find their cars in a large, multi-storey car park, but consider what a shopping centre operator could do with a list of registered vehicles that visited their building?

QV Street Mall (continued)

Shopping centre operators are able to do this kind of tracking of individuals so easily because they're not technically *identifying* you as an individual—a digital billboard won't directly link up your image to your driver's licence or your name, they're just seeing you as a data point among many.

However, we also know from studies, many of which are done by incredibly smart people right here in Melbourne, that anonymised data is very easy to de-anonymise if you try. In 2016, Vanessa Teague, a cryptographer from the University of Melbourne, and two of her colleagues reported on a dataset, published on an open government data website by the federal government, of 2.5 million Australians' Medicare and PBS payment history dating back to 1984 that had supposedly been de-identified so people were anonymous. In the research, they came up with seven examples where they were able to determine who the data was about based on publicly available but relatively unique information about that person—such as their birthday, dates of birth of their children, and other personal information. Once they had that, the researchers had a trove of their entire medical history, including medication purchases and tests conducted.

So, think about the wealth of data that shopping centres have about your movements and habits just from being in the space, and the sort of information about your life they may be able to derive about you—maybe you suddenly start coming in during the day suggesting you lost your job, or you only come in after work for specific items.

Moreover, what data does the city have about you as you move around *their* spaces? Let's head to our last stop.



Stop 5: Library

As gateways to knowledge and culture, libraries play a fundamental role in society. The resources and services they offer create opportunities for learning, support literacy and education, and help shape the new ideas and perspectives that are central to a creative and innovative society. Are you up to date on projects your local library is running?

For centuries libraries have been a safe haven for knowledge and ideas and it's why we have chosen the library as our last spot. Today we spoke about human rights a lot and it's important to acknowledge the role, the history, and the importance of that as we navigate this digital world of ours.

The Universal Declaration of Human Rights was an effort born out of necessity and on the back of two world wars (and arguably many wars prior)—an effort to prevent the most powerful from preying on the powerless. It makes us all even, worthy of the same things. At that unique moment in time, the international community agreed that everyone is entitled to the same baseline; guaranteeing dignity, freedom and fairness for generations to come. It's essential that we preserve, and staunchly defend, these rights in our digital spaces.

As cities around the world get smarter—including our beautiful city of Melbourne, we need to be paying attention to how data-centric projects may contribute to these systems of surveillance. We cannot let “smart” become a code-word for “surveillance.”

... We should all be able to live our lives without being constantly watched, monitored and tracked. If we want our cities to be truly ‘smart,’ they need to uphold the freedoms of the people who inhabit them.

Okay but is this type of surveillance legal?

Under the Victorian Charter of Human Rights, we in Victoria have the right not to have our privacy unlawfully or arbitrarily interfered with. However, in public places it is generally understood that we don't have a reasonable legal expectation of privacy, as we would in distinctly private spaces, like your home. This is true, but we do have an expectation of relative anonymity—that our identity is not known to strangers, and that our movements and activities are ephemeral—they aren't being recorded, stored, and analysed. The trouble is, as technology advances, this is becoming increasingly feasible, and is drifting dangerously close to the norm. Would you feel comfortable if you knew that everyone who looks at you in the city instantly knows who you are? Your age, maybe where you work and where you live?

Details of our movements throughout the course of the day reveal all kinds of information that we think of as personal and protected: the details of our love lives and relationships, medical conditions, participation in political movements, and our financial circumstances. On a societal level, the erosion of privacy is detrimental to our democracy, can exacerbate harm for already vulnerable groups, and increases the power imbalance between the people and governments or large corporations.

Library (continued)

The CCTV cameras installed in the city with the goal of reducing crime are unlikely to defy the terms of the Charter, and this may be a balance we are willing to accept. However, as the sophistication and use of other technologies such as facial recognition increases, the amount of information being collected goes far beyond a fuzzy recording of a streetscape.

The question of legality gets even more complicated when we consider that law enforcement actually gets all kinds of exemptions under existing privacy laws. What's more, we don't have a federal Human Rights Act to protect our rights on a national level, including privacy. Australian parliaments have not passed much in the way of legislation to enshrine our privacy, in fact, the trend is actually toward passing legislation that erodes our privacy. **So yes, it's probably legal, but does that make it right?**

Laws are made, updated, and constantly rewritten by those we elect into office. It's imperative that we question our own comfort level with these technologies permeating our lives and express that to our elected officials. Things that were illegal decades ago have been written into law, but that only makes them lawful, not always right.

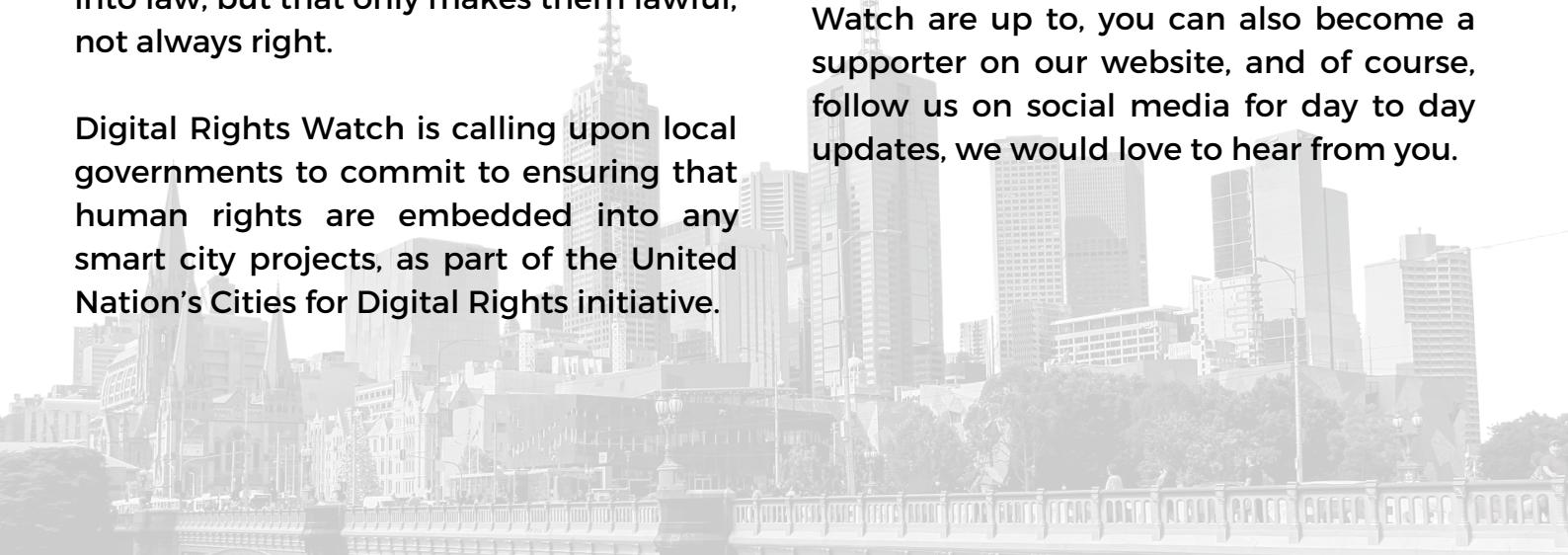
Digital Rights Watch is calling upon local governments to commit to ensuring that human rights are embedded into any smart city projects, as part of the United Nation's Cities for Digital Rights initiative.

... To be part of the initiative, cities sign on to the UN Declaration of Cities for Digital Rights. In doing this, cities make a commitment to embed human rights into their smart city plans, digital transformation initiatives, and frankly, all other areas of activity.

There are five key pillars:

1. Universal and equal access to the internet, and digital literacy
2. Privacy, data protection and security
3. Transparency, accountability and non-discrimination of data, content and algorithms
4. Participatory Democracy, diversity and inclusion
5. Open and ethical digital service standards

We hope that you have gained some important understanding about how surveillance is already happening all around us—but we don't want you to despair. We can and should continue to step up and demand from governments and private companies alike to respect privacy and human rights more broadly. If you want to take action, we encourage you to get in touch with your local council to let them know you care. You can visit our website for resources. If you want to stay up to date on what Digital Rights Watch are up to, you can also become a supporter on our website, and of course, follow us on social media for day to day updates, we would love to hear from you.



MELBOURNE SURVEILLANCE TRACK



Thank you for joining us for the Melbourne Surveillance Track! If you enjoyed this project, please consider becoming a supporter of Digital Rights Watch.

We are incredibly grateful to the City of Melbourne for including us in the Melbourne Knowledge Week program, but this track, from concept to materials were produced by our small team with no additional funding support but that of our supporters!

<https://digitalrightswatch.org.au/donate/>

If you have any questions or feedback about the track please reach out to us at, we'd love to hear it!

<https://digitalrightswatch.org.au/contact/>

Melbourne is just the beginning! We've made all of the resources of this tour available and free to use under a Creative Commons license. We would love to see others create similar projects in other cities. Feel free to get in touch with us at info@digitalrightswatch.org.au

