REPORT ON PROCEEDINGS BEFORE

SELECT COMMITTEE ON THE IMPACT OF TECHNOLOGICAL AND OTHER CHANGE ON THE FUTURE OF WORK AND WORKERS IN NEW SOUTH WALES

CORRECTED

At Room 814-815, Parliament House, Sydney, on Wednesday 29 June 2022

The Committee met at 10:15.

PRESENT

The Hon. Adam Searle (Acting Chair)

The Hon. Lou Amato
Ms Abigail Boyd
The Hon. Greg Donnelly
The Hon. Courtney Houssos
The Hon. Shayne Mallard
The Hon. Shaoquett Moselmane

PRESENT VIA VIDEOCONFERENCE

The Hon. Anthony D'Adam
The Hon. Scott Barrett

* Please note:
[inaudible] is used when audio words cannot be deciphered.
[audio malfunction] is used when words are lost due to a technical malfunction.
[disorder] is used when members or witnesses speak over one another.

CORRECTED

The ACTING CHAIR: Welcome to the potentially final hearing, the Committee's ninth hearing, for the inquiry into the impact of technological and other change on the future of work and workers in New South Wales—although that is not a core promise. I acknowledge the Gadigal people of the Eora nation, who are the traditional custodians of the land on which we meet today. I pay my respects to Elders past, present and emerging, and celebrate the diversity of Aboriginal peoples and their ongoing cultures and connections to the land and waters of New South Wales. I also acknowledge and pay my respects to any Aboriginal and Torres Strait Islander people joining us today.

Today we will be hearing evidence from the Centre for Responsible Technology, academics, unions and industry groups, and other stakeholders, with our focus on the issues of workplace surveillance and automation. While we have a number of witnesses with us in person, some, including those in the first bracket, will be appearing via videoconference. I thank everybody for making the time to give evidence to this important inquiry and overcoming the travails of COVID, which, although it has dropped from the headlines, is ever present.

Before we commence, I would like to make some brief comments about the procedures for today's hearing. Today's hearing is being broadcast live via the Parliament's website, and a transcript of the hearing will be placed on the Committee's website when available. In accordance with the broadcasting guidelines, media representatives are reminded that they must take responsibility for what they publish about the Committee's proceedings. While parliamentary privilege applies to witnesses giving evidence today, it does not apply to what witnesses say outside of their evidence at the hearing. I therefore urge witnesses to be careful about comments they may make to the media or to others after completing their evidence today.

Committee hearings are not intended to provide a forum for people to make adverse reflections about others under the protection of parliamentary privilege. In that regard, it is important that witnesses focus on the issues raised by the inquiry terms of reference and avoid naming individuals unnecessarily. All witnesses have a right to procedural fairness in accordance with the procedural fairness resolution adopted by the House in 2018. If witnesses are unable to answer a question today and want more time to respond, they can take a question on notice. Written answers to questions taken on notice are to be provided within 21 days.

If witnesses wish to hand up documents or, in the case of those appearing via videoconference, email them in, they should do so through the Committee staff. In terms of the audibility of today's hearing, I remind Committee members and witnesses to speak into the microphone. As we have a number of witnesses in person and via videoconference, it may be helpful to identify to whom questions are directed and who is speaking. Finally, please turn your mobile phones to silent or off during the duration of the hearing.

CORRECTED

Mr PETER LEWIS, Director, Centre for Responsible Technology, The Australia Institute, before the Committee via videoconference, affirmed and examined

Professor MARK ANDREJEVIC, Professor, Communication and Media Studies, Monash Data Futures Institute, before the Committee via videoconference, affirmed and examined

Professor TOBY WALSH, Laureate Fellow and Scientia Professor of Artificial Intelligence, University of New South Wales, before the Committee via videoconference, sworn and examined

The ACTING CHAIR: I welcome our first witnesses. We usually allow for a brief opening statement of no more than three to five minutes from each of the interests before us. Mr Lewis, I might start with you and then see whether Professor Walsh has anything to add, and then we will go to questions. Mr Lewis, the floor is yours.

PETER LEWIS: Thank you for the invitation to appear today. I do apologise for not appearing in person, but I currently have COVID. I also apologise in advance if I am not firing at 100 per cent today, but this is one appointment in my diary that I was determined to fill. I am here in my capacity as Director of the Centre for Responsible Technology, which is an initiative of The Australia Institute. It is an independent think tank which exists to support sensible and evidence-based regulation. Joining me is Professor Mark Andrejevic, a global expert in digital media surveillance who can talk the Committee through some of the wild and wacky ways technology has expanded the reach of employers through the pandemic. Professor Toby Walsh, also suffering from COVID, has produced a terrific paper looking at how athletes are now being monitored, as a harbinger of even more intrusive workplace practices in the future. I do encourage the Committee to tap two global brains on this issue during this session.

When we launched the Centre for Responsible Technology in 2019, we identified the largely unregulated intensification of surveillance in the workplace as a key area of concern. We also identified the New South Wales Parliament as a natural home for leading regulation given its importance in establishing workplace surveillance laws. In the late 1990s I was proud to work alongside you, Chair, as part of the late, great Attorney General Jeff Shaw's team in ushering worker protections against video surveillance through the Parliament. In 2001, working with Unions NSW, those laws were extended to email surveillance, with the radical idea that employers should not routinely snoop on employee email conversations. While little has changed legislatively over the past decade, the online workplace has become another country altogether. One critical difference, which we may go into more deeply today, is that the regulatory binary of overt-covert surveillance has totally collapsed. Today surveillance is assumed.

Our submission, compiled after a round table with leading unions in 2020, spans the myriad ways employer surveillance over workers has radically expanded. The market for technology that observes, captures and repurposes behavioural surplus is fast moving and self-perpetuating. Only this month, we have seen the public outcry at facial recognition technology tracking tools going after both consumers and staff in major retailers, with only cursory disclosure and no real accountability. Absent regulation, technology companies will continue to seek to adapt their products to deliver value for employers by squeezing more out of their workers and reducing labour costs. While this inquiry has rightly spent a lot of time thinking through the rise of the gig economy, it is important that the consideration of the collection and exploitation of worker data is not limited to those types of businesses. While the app-based services in transport, food delivery and increasingly in caring services have data collection at the centre of their employment models, this is not a new approach by employers.

Our submission outlines how worker information is being collected and repurposed in transport, mining, education, logistics and long haul. It also shows how the pandemic and shift to home work has only intensified monitoring trends, with auto-tracking of workflows down to monitoring employee mouse movements becoming accepted parts of staff management. What is clear from this review is that the monitoring of workers has gone way beyond work performance. We know that workers in factories fitted with GPS are charting workflows that will ultimately be replicated to see them replaced by automation. We also know that there are growing secondary markets in data, with the potential for employers to sell their employees' data, creating a secondary digital market for their labour. And we have seen how companies use employee tracking to identify and intervene in union conversations. So it is not hyperbole to say that the workplace surveillance lying at the heart of a twenty-first century assault on workers' rights is every bit as calculated and effective as the industrial-age practices that summonsed in the factory Acts.

We would submit that a basic responsibility of lawmakers is to ensure that existing legislation is fit for purpose, and it is clear that, despite its history of leading on workplace surveillance, New South Wales has fallen behind the game. These laws need a review, if not a total rework, with a return to the core assumption of worker privacy unless there are specific reasons for monitoring, with clear no-go zones like union communication

embedded in the legal frameworks. There are other elements of workplace laws which we argue should be reviewed, including right-of-entry laws, which provide union representatives with the right to review wage books and address members. Should these rights be extended to give a trusted representative the right to review how the data of a worker is collected and used?

We also need to modernise termination, change and redundancy provisions. Are there grounds to extend these rights for employees to be consulted around change, to be fully informed of the way their data is used by the employer? Alongside our concrete recommendations, we also invite the Committee to reflect on the concrete steps the New South Wales Government could take in becoming a model employer when it comes to employee surveillance and monitoring. As our lived history has shown, this means ongoing review and, might I say, monitoring of the way technology is being applied, with a critical eye placed on the proposition that this is simply a prerogative of the employer. I'm happy to take questions, but I also urge the Committee to make use of the expertise of Professor Andrejevic and Professor Walsh.

The ACTING CHAIR: Thank you, Mr Lewis. I might just ask Professor Walsh. I think your research on sportspeople is a fairly distinct area. Do you just want to outline briefly to the Committee, in a few minutes, what the importance of that work is and what you've learnt?

TOBY WALSH: Yes, certainly. Thank you for the opportunity to give evidence to this Committee. I apologise for not being there in person as well. I am recovering from COVID [audio malfunction].

The ACTING CHAIR: Professor Walsh, can you hear me?

TOBY WALSH: Just a couple of [audio malfunction].

The ACTING CHAIR: Professor Walsh, can you hear me? You keep cutting out. Maybe turn your—

TOBY WALSH: Yes, I can hear you.

The ACTING CHAIR: At our end, you keep cutting out. So maybe turn your video off. That might improve the audio.

TOBY WALSH: Let's try that.

The ACTING CHAIR: That's much better.

TOBY WALSH: Thank you for giving me the opportunity to present today. I apologise for not being there in person. But, like Peter, I'm recovering from COVID. I will answer your question. I just want to say general remarks, which is why a professor of artificial intelligence is interested in these topics. AI leaves the university laboratory and turns up in our workplaces. We face a fundamental challenge, which is it is entirely dual-use technology. There are very good uses you can use of the [audio malfunction]. Equally, there are uses that are [audio malfunction]. As an example we see some very innovative and exciting uses of AI—

The ACTING CHAIR: Professor Walsh, sorry to interrupt. I'm told that Hansard is not able to properly capture what you're saying because you're still cutting out every few words. We're going to try and get you on the phone and see whether that's a better connection. I apologise.

TOBY WALSH: Okay. No problem.

The Hon. SHAYNE MALLARD: Resisting the temptation to talk about our surveillance capability, but—

The ACTING CHAIR: Yes, well, obviously our surveillance capability is not that good.

PETER LEWIS: I know. Discussions around technology are great when the tech falls apart like this.

The ACTING CHAIR: Yes. Professor Walsh, do you have your phone with you? We just tried to ring, and it went straight to voicemail. Are you perhaps in a bad reception area?

TOBY WALSH: Sorry. My phone has just decided to run out of charge at this one moment.

The ACTING CHAIR: We might just park you for the moment. I might just ask some questions of Professor Andrejevic. Professor Andrejevic, did you just want to outline for the Committee your work in this space and its relevance?

MARK ANDREJEVIC: Yes. Thank you for the opportunity to provide evidence. I also apologise for not being there in person. I had some travel plans that made that difficult. My work focuses on the use of digital technology and its interactive capacity for monitoring and surveillance purposes. When it comes to the workplace, some of the changes that Peter described—email, CCTV—those are shifts that took place at a rather slower rate than these changes that are happening now. So we're seeing quite rapid development of both the sensor technology

and the processing power and automated systems for making sense of large amounts of data. What this means is that the types of surveillance, of tracking, social serving and predictive analytics are [inaudible]—I guess the phone's working now—that we have become familiar with in online spaces are migrating into the workplace and public and shared spaces.

I'm particularly interested in the development of sensors of all kinds that are being implemented in workplace environments, including things like face recognition technology; remote biometric monitoring such as temperature analysis, voice print analysis and also the sensors that Peter mentioned that are built into the devices that we use for our work—computers, portable devices that we carry with us, that can be equipped with sensors that can track and monitor our activities.

The ACTING CHAIR: Professor, that's at a pretty high level. Can you just give us a couple of practical examples about how that technology is being deployed in workplaces or in the work context, if I can put it that way?

MARK ANDREJEVIC: Sure. One of the drivers for increasingly high-level surveillance is the forms of casualisation associated with gig work. If we think about, for example, Amazon delivery drivers or Uber drivers, they exist in a contractual relationship with their employers. They don't know their employers directly. They don't show up at the office, where they can be recognised. So one technique for verifying who they are has been facial recognition technology. So you're an Uber driver. You check in for your shift. You log in. You have to provide an image of yourself, which is then verified against a database of registered drivers. And if that technology doesn't work, you're locked out of your ability to do your work.

What's happened in London is some Uber drivers have actually filed a class action suit because the technology that identifies them they claim is biased by skin tone, so folks who have darker skin are more likely to be locked out of doing their work. They try to start driving. The technology doesn't recognise them so they're not accredited and they can't earn their living that day. That's a technology making a decision about them based on remote monitoring, so that would be one example.

We know that, during the pandemic, remote work has led to the development of a host of technologies that are used to monitor workers beyond the walls of the office, primarily through their portable devices or their home computers or their laptop computers. They do things like monitor time on screen, keystroke monitoring, mouse usage. There's software that's become quite popular that allows the tracking and sorting of workers based on their remote performance as recorded by their devices. This has led to a kind of granular level of tracking of work that didn't take place, for the most part, in the workplace prior to the pandemic. Those are a couple of examples.

The ACTING CHAIR: I might just now go back to Professor Walsh to just talk us through his work on the sports data framework and what sort of lessons can be derived from that about monitoring in the work context more generally.

TOBY WALSH: Yes. Good. I hope you can hear me better now.

The ACTING CHAIR: Yes. We can hear you better.

TOBY WALSH: Great. As I was trying to explain at the start, the fundamental challenge with deploying AI technologies like computer vision is that it is dual use. There are fantastic uses of the technology that we are starting to see in workplaces. So, for example, we're seeing it being used for health and safety purposes to monitor people around dangerous machinery and warn when they're at risk of injury. Equally we're seeing it to surveil people, possibly without adequate concerns. And the recent understandable and justified furore that we saw around the use of computer vision and facial recognition software in consumer stores I think is a good example of where companies may be starting to overstep the line and certainly doing it without adequate public concerns. Then that information is then used, of course, to track [inaudible]. We see examples of where, for example, in the United States it is believed that people have even been fired based upon the recommendations of algorithms alone, without any human oversight.

Specifically, I have been looking at this in the context of a study done by the Australian Academy of Science and the Minderoo Foundation looking at a very specific workplace, a sporting arena, and looking at the surveillance and use of such technologies in professional sports. We published a report in April, which I encourage members of the Committee to take a look at, that looks at the legal, societal and technical issues that that study raised. I think that particular area is one where perhaps technology is more advanced than many other workplaces and one where it may be indicating where other workplaces may eventually end up. The primary finding that we had is one that should be concerning to this Committee, which is that there is a huge amount of data collection going on without much clear justification that it is actually improving performance and that it is very invasive. It goes beyond the workplace into people's homes.

Professional athletes are being monitored even during their sleep and at other times in their homes, and the power balance is of significant concern. It is not clear that the athletes are in a position to refuse the demands for this information to be collected, and lots of information is collected without any clear idea, at least at the start, as to how it is then going to be used. Lots of questions were left unanswered as to who owns that information and what happens, for example, when the athlete leaves that sporting club and moves elsewhere. Are they allowed to take that data with them? Is it something that will be used in their post-sporting career, for example, to ensure that they have better health care? Or will it be used as a weapon against them perhaps to deny them health insurance because they have perhaps received too many knocks to the head? The data records that information, which is now something that is going to be detrimental to their future wellbeing. I encourage you to take a look at the report. I think it raises significant concerns that just because we can collect information, it does not mean that we should or even have the right to do so.

The ACTING CHAIR: Mr Lewis, I might ask you to questions. In the employer submissions to this inquiry, they make the case that there is comprehensive legal regulation of monitoring in the workplace through the workplace surveillance legislation and the Privacy Act. I would like you to talk us through where you see the gaps in terms of the New South Wales laws or any Federal laws. The second thing I would ask you to talk a bit more about is how employers are using the secondary data that they collect from their workforce and how they are able to monetise that and whether or not employees are being given a slice of that action or any agency over even knowing that that data is being collected.

PETER LEWIS: The existing legal framework, as I said in my opening remarks, particularly around the New South Wales surveillance laws, is around this idea of overt and covert, which is quite similar to the underlying assumptions of privacy laws, that deriving a form of consent allows you to do basically whatever you want as an employer. We all know that consent as a framework in the world of tech means you have to tick a box to say it is okay to get access to a platform. It is a similar to ticking a box to get access to a job. I guess the question for the Committee is, at the point of employment, if someone is clicking or ticking a box that says, "I consent to my data being used in a myriad of ways"—and often those consent forms allow employers to change the terms of those agreements as technology catches up or offers new opportunities without having to go back to the worker—whether that is appropriate or consistent with the original intention of the laws.

I know there is a national review currently underway of the privacy laws, where consent is a key area that is being reconsidered, but I also think that in the terms of the framework of the workplace surveillance laws, it is worth considering: Are there some things that require more than cursory consent? One of the interesting parts of the story last week around the facial recognition technology in Bunnings and a number of other retailers was that there were very small signs saying, "You may be being filmed," and is that sufficient to inform the public or staff that their information is being monitored. If you go back to the original assumptions of both the video surveillance and email surveillance laws, it was an assumption that there was a degree of privacy assumed to an employee, that they sold their labour but that there was also a sense that there were parts of their existence as an employee that should not be observed and monitored unless there was good reason.

If you remember the initial video surveillance, you would require a magistrate's certificate and due cause to be routinely filming a staff member. Now think about how the world has changed in the 20 years since then. The other point I would make is that our observation is that a lot of—and I think Mark alluded to it in his comments—the drive for this technology appears to be vendor driven. That is, a tech company will come up with a new application of monitoring tools and go to workplaces and employers and say, "We can deliver value to you on X, Y or Z." I think that was particularly the case during the lockdown when there was panic about how you monitor staff and performance when they are working from home. My experience is my staff never worked harder. I think there are a couple of boxes that need to be thought through.

The existing laws have not been reviewed for 20 years and complying with laws that were designed for video cameras and very crude email scans in a world where the potential is to monitor basically every eye movement, mouse movement and thought really does not bare scrutiny. In terms of the secondary market, to be clear, because of a lack of regulation we do not know how employers are using this information. I think there are three areas of concern. One is the storage of employer data and the second is the destruction of it at some point—during the life of which the employer will hold the information. To Toby's point, if you have health data, could that then be used as something that follows you later into your life? The third is exploitation of data.

We know that companies like Clearview AI routinely scrape social media profiles and take photos and then sell them on to another market. We do not know the scope of which employers or tech companies—as part of the terms of an employee using their tools—are then using that data in big data batches to build other forms of business. I cannot give you concrete evidence of how this is being used, but I am saying that the opportunity for abuse and exploitation of the information being collected is rife at the moment because there are no limits.

The ACTING CHAIR: I will pick up on one point and then throw to the Committee because I do not want to monopolise all of the questions. You mentioned some of this was being vendor driven. That is, a company has a product, particularly during the shift to home working that we saw during the pandemic—and in preparation for a paper I gave last year I found so many different companies like InterGuard and Teramind that all extol the virtues of remote employee time and productivity tracking software that they are all selling. Should the State be regulating or licensing the use of technology? There seems to be an unstated assumption that all technology is good and that it should be allowed to be used wherever. Our kids are using technology for their games, and that seems to me to be entirely unregulated outside of classification. Shouldn't there be some sort of testing before we allow technology on the unsuspecting public, for people to be subjected to it?

PETER LEWIS: Our position is that we're not anti-tech. That's like being anti-gravity. We say there should be regulatory guardrails and red lines. The best advice I've been given on thinking this through is just to start with the existing law. You don't go looking for new laws; you start with the existing law and you apply it to technology as it evolves. One of the reasons New South Wales is at a great position to lead on this is that the basis of those surveillance laws, which have been developed over the last couple of decades, creates a series of principles that can be built off.

Our proposition would be that there should be a requirement that, if employers bring in these sorts of monitoring, these new products for employees, they should comply with the basic principles consistent with these Acts, which is genuine employee—if we go back to the original rules, there should be due cause to use technology on employees. There should be clear communication with the employee, and there should also be, in terms of the broader laws in New South Wales, the right for the employee and their representatives to know what data is being collected and how it is being used. I don't know if you want to add to anything there, Mark, given your work on some of these new products as well?

MARK ANDREJEVIC: If I might just jump in, one of the things that I think is worth thinking about when it comes to regulation is the fact that the capacity of these technologies, combined with their data processing abilities, leads to new forms of decision-making that are not based just on what we might think of as individual invasion of privacy or monitoring. Is somebody being subject to video recording or remote monitoring on their computer? Those are important questions. A broader frame thinks about what it means to be able to make decisions where the target of surveillance isn't necessarily just the individual, but the pattern.

I'll give you an example. It's a small example, but I think it's suggestive. There was a company that was screening job applications for a large employer of call centres, and one thing that they found out for these electronically submitted applications is that if you just scrubbed the data and pumped it into an automated machine learning system to figure out what's going to be the best predictor of a good employee, it wasn't anything that was actually on the application, it was what software was used—actually, what browser was used to submit the application. And so decisions have been made predicting who is going to be a good employee based on a pattern that was discerned through large-scale data mining.

This is a decision that has an impact on somebody. It doesn't violate anybody's particular privacy in the sense that all of their data could be anonymised. But a pattern was discerned from it, and that's the type of monitoring that we're going to see more and more of. Once you have lots of data that comes from the sensors that are in the workplace, you may have a pattern. Past employees who did this have turned out to be better or worse employees, we'll do promotions or firings based on this pattern. That's a very powerful form of analytics.

It can be unexplainable. Where you have lots of variables and lots of data and you're using neural nets to make decisions based on that—it's very hard to explain to somebody you weren't hired because you used an installed browser rather than Chrome. What does that have to do with how good an employee you can be? The only answer there is really, "Well, the machine made the prediction." So you have a kind of unaccountable decision based on large amounts of data. I think it's going to be important down the road to pay attention to that kind of pattern-based tracking, where the surveillance isn't specifically devoted to individuals but to evolve patterns that are then used to make decisions about individuals.

TOBY WALSH: Can I pick up on that point, because it's a fantastically important point, which is that computers are really good at picking up correlations and they may not be causations. There may not be a causal link there. There are plentiful examples of injustices that have been committed because people have trusted algorithms, which are typically black boxes, who have made those correlations.

Ms ABIGAIL BOYD: Thank you all for attending, and for your fabulously informative submission, Mr Lewis. I wanted to pick up on that idea of the secondary market for data. One of the examples you gave in your submission, I believe, is in relation to teachers doing marking and being able to harvest that data over time to then be able to use that for software that then can more accurately predict the mark that might be given to a particular piece of work. Is this primarily theoretical in terms of the assertion that employers are the ones that

would be using that data to sell on to tech companies, or is it more the case that these tech companies, within their licensing terms, are providing this software to employers and then basically scraping the data to improve their future products? Can you comment on that, please?

PETER LEWIS: I think our point is that the lack of regulation and visibility means we do not know. Now, what we do know is that the marking—particularly the sort of higher education, and Mark can probably speak a bit more to this—is becoming increasingly automated. There are fewer roles for the human marker in areas, particularly around humanity—humanities. I apologise for my COVID brain. One of the observations I have made as a parent of a kid going through high school was the way that kids are being taught to write is almost like a machine now. There is a real structure that is required that lends itself to automated marking rather than human consideration and to an extent taking certain elements of creativity out of the process.

We know that the platform for a lot of education is now being driven by big tech companies and absent real transparency on how that's being used. I think some of those scenarios you were talking about are totally credible. Depersonalised, yes—so we're not saying that individual students are having their information attached to them. But this whole idea of what becomes the norm and what becomes—sorry, my brain is not quite working. But you know what I'm saying. What becomes the norm has to be something that can be easily replicated, rather than something that is evaluated by humans. Mark, you've done a lot of work on how the universities have changed over the last few years. I don't know if you want to speak to that as well.

MARK ANDREJEVIC: Sure. I think maybe one of the key points there is the one that you made about depersonalisation. It is in privacy law, or the Privacy Act. I'm not sure it gives us the tools to make claims about how decisions operate that are based on data that is collected but anonymised, or de-identified. In other words, let's say you get all this information about how student work correlates to subsequent grades. You can do that without identifying any students or linking anything back to a student. You can actually then create a system which can be marketed and sold that can be used—according to some claim, at least—to accurately mark future students.

What you have there is an automated system based on data collection making decisions about people that would affect their future life chances without actually impinging on the privacy of those whose data is collected. I think that's a new generalisable of principle, right? Once you collect data that can be de-anonymised or even collected without any identifying information, there can be certain patterns that can then be used to make decisions without running afoul, I think—maybe we need some legal experts here—of existing protections in the privacy law.

The Hon. ANTHONY D'ADAM: I wanted to explore the issue around facial recognition. I worked for a time with the Media, Entertainment & Arts Alliance. We represented performers and one of the issues that really came to the fore was about ownership of your image and the ambiguity in the law, both in the common law and in statute, about whether someone actually owns their own image. Given that facial recognition is increasingly your signature, do we need to look at some form of regulation around the proprietary control over an individual's image? Of course, that would then extend to their biometric information—fingerprints and, you know, the other devices that are used to uniquely identify an individual, which clearly have currency beyond the workplace where they might be being collected.

PETER LEWIS: That is a really, really interesting question that obviously goes beyond the scope of this inquiry. In a way, the assumption that is being, again, largely [inaudible] driven, is that you give up parts of your identity as part of the transaction to access different services, be it access to a platform, going into a public space where you agree—you consent—for your images to be taken, or the workplace. The ultimate way of looking at this and sort of one of the bigger recalibrations going on in thinking about our relationship with technology is the extent to which we should have more control of that information and give permission for it to be used under certain circumstances, rather than rendering our entire person accessible to whatever form of surveillance a different business or the employer or a platform cares to take. So I think you are onto something there.

To think that through in the workplace we would start looking at concepts like data trust. So the idea that, as an employee, the assumption is everything that you produce in the workplace, apart from your primary labour, is yours and that any use of it needs to be negotiated. There is some really interesting thinking around how that could end up being a way of capturing value as a group of workers. If you are delivering extra value to an employer in terms of productivity or efficiency—or, for that matter, secondary sale of the collected data, and you agree to that—should that be something where the benefits are shared back to the workers rather than just being assumed to be something the employer has to hold?

I think that is a bigger debate than simply updating workplace surveillance laws, but I do think an area like the New South Wales public service would be an excellent place to start thinking through what some of those structures could look like. Again, as we said in our submission, it is not just about setting laws; it is also about

setting rules. There is a real opportunity, I think, for New South Wales as, I would imagine, the largest employer in the State, to embrace best practice to lead the rest of the State and the State's employers on how we can do this well.

The ACTING CHAIR: Mr Andrejevic?

MARK ANDREJEVIC: I think it is a really important question. As recent events suggest, the issue around face recognition is not going to go away. It is becoming more pressing as the technology becomes more powerful, less expensive and more ubiquitous. I think it is going to be really important to have dedicated regulations to specifically treat the issues that are raised by face recognition. We are going to need that and it would be wonderful to see New South Wales take the lead. I know that the Human Rights Commissioner, Ed Santow, is working on model legislation around this.

The question of ownership of your image is a really interesting one because it almost divides into two. One is your image as it appears—and many of us know that our images are out there, whether it be for work your face is up there and on news coverage and so on. As we know from Clearview AI—that is a company that just scraped those images off the internet—often your images are connected to your name so it can be directly connected. But the other thing that face recognition does is it creates a biometric template based on your image and that template can then be used to uniquely identify other images of you.

The control over that template, what it means to create that template and what type of information that counts as, my understanding is that the Information Commissioner has treated that as personal identifying information because it can be used to uniquely identify other photos of you. But I think it would help to clarify that in the legislation and to develop regulations for governing what happens to that image, how it can be used, how long it can be kept, the security levels that can be stored and how it can be verified correctly. All of those seem to be key issues that I don't think are going to go away.

PETER LEWIS: Professor Walsh has his hand up.

TOBY WALSH: Yes. I just wanted to say that some really interesting questions that possibly go beyond the scope of this inquiry about intellectual property and about ownership of those rights—and certainly that's what we came across with looking at athletes in their workplace. You see it, obviously very directly, with people like actors, how quickly the actors union in the United Kingdom is lobbying on these issues about the fact that AI is now being able to synthesise actors' voices and the figure of actors, and then who owns the benefit to those? One more topic, since we are on face recognition, which is a really difficult and important topic that does need to be addressed and has not been raised so far is the inaccuracies of face recognition. Despite all the work over the last few years and all the concerns that were raised, facial recognition still does not work as well on people of colour and it still does not work as well on women, and it works even worse still on women of colour. It is not clear when and if it is going to be as accurate as humans and when and if we can start to not worry about the harms that will be caused by the errors that it will make.

The Hon. ANTHONY D'ADAM: This is also arising out of my former union experience, but I know in the New South Wales public sector they very quickly adopted, without much debate, the process of using psychometric testing for selection of job applicants. Obviously, the underpinning of psychometric testing is predictive analytics. I wonder whether you might offer some comments about, I suppose, the risks to workers of a psychometric regime being applied to candidate selection for such an important employer as the New South Wales public sector?

PETER LEWIS: I will defer to Toby, if you like.

TOBY WALSH: Again, fantastic question. It is a fantastically important topic and one where I am expecting there is going to be a huge number of civil action suits brought against tech companies that are introducing rather bogus machine learning techniques to screen applicants. We come back to the point raised earlier by Mark, which is that it is very quick at picking up correlations and they will pick out whether you are using a Microsoft or an Apple operating system and use that as a basis for selection—something that I suspect we would not want candidates to be selected on, on the basis of what operating system their computer happened to be using because a computer does not have any of our common sense and it does not have our empathy or understanding. If it is selecting candidates based on such criteria that is not going to satisfy our natural justice and indeed what perhaps explicitly we have already legislated against in terms of discrimination law.

The Hon. SHAYNE MALLARD: You have painted an Orwellian doom and gloom scenario there, gentlemen, and I just want to put the counter view from having a small business background. Some of the surveillance and facial recognition monitoring of staffing areas like accounts in banking and finance of what can be embezzlement or theft protects businesses as well and protects the honest workers. I just put it to you that—obviously you are concerned around the broader exploitation of data and so on. But so many businesses—I'm

talking smaller and medium businesses mainly—really have moved into an area of better efficiency and better confidence in their organisation by having access to these different datas. What would you say to that?

PETER LEWIS: My first response is that if a business needs to monitor its staff to that extent to feel that they are going to be able to operate, they've probably got bigger problems, that there will be cultural problems underneath it as well. A business has the right to protect its property. It has a right not to have staff stealing money—of course it does. But the approach of just monitoring everyone in order to solve that particular problem seems to miss the point. If you create frameworks which the staff have buy-in to as well, you are creating cultures where that is a lot less likely to occur. Even if your proposition holds—that you need to be monitoring staff to ensure they are not stealing from you—you need to do that in a way that the vast, vast majority of staff who aren't have their rights respected as well.

The Hon. SHAYNE MALLARD: I think that's the point.

PETER LEWIS: So, again, it's not about being anti-tech. It's about getting the right guardrails and red lines in place so that the technology can be used appropriately rather than—it is a Wild West at the moment and anything goes.

The Hon. SHAYNE MALLARD: Your point about buy-in, I think, is a valid point—getting staff buy-in at some point at the beginning of that process. I've had hospitality businesses and the big shift for us was when facial recognition came in. The staff just go up to an iPad, face recognise and log in for their shift, and another staff member doesn't sign in for them anymore. That used to happen—someone slept in, didn't turn up or was a couple of hours late. And also that software monitors the hours they are doing and helps compile the payroll, and also alerts the company to different issues like that they have worked too many hours or something. So they are positive tools as well.

PETER LEWIS: Yes. I think that's right and there's obviously a desire for businesses to receive those tools but, again, it has got to be contextualised and it has got to have a fair underpinning of it. Simply clocking on with your face—I don't think that is the biggest issue we are dealing with here, although how that data is then used beyond that is something that we just don't know. I don't know if you want to add to that—I know Toby has got his hand up there.

The Hon. SHAYNE MALLARD: There is an external app that supplies that process.

PETER LEWIS: And then do they get access to that data as well?

The Hon. SHAYNE MALLARD: I have one more question on that line. Is there a role for monitoring to address issues of sexual harassment or bullying in the workplace—that is, for the employer to make sure they've got a safe and secure workplace for their employees?

PETER LEWIS: There is a role to each. Employers have a positive obligation to provide a safe place of work, but if your only tool is blanket surveillance then your cultural problems are far greater. I think that there is a degree of tech-ceptionalism around the whole thing—that we will give you the technology to get rid of workplace bullying or sexual harassment. I'm an employer. I employ staff. You've got to do better than just say, "We're going to surveil you." You have got to create the cultures.

The Hon. SHAYNE MALLARD: I get that—just a tool in the toolkit.

The ACTING CHAIR: Professor Walsh, you have a minute.

TOBY WALSH: Yes. They are really interesting questions and, as I said at the start, there are good uses and bad uses of these technologies. I think the important thing is to try and work out what are the guardrails to put in place to ensure that we can get the positive uses that convenience people and improve productivity and also guard against wasteful expense. I think it's worth pointing out it does take us to a new place. Previously we got used to the idea there were lots of CCTV cameras everywhere, and we weren't so overly concerned because we knew there were too many cameras for people to watch. That was a device, post-hoc.

After something had gone wrong, some crime had taken place and the business had had something go wrong, you could go and look at the tapes and actually find out, "Oh okay, well, that was the customer," or, "That was the employee who was a force in that circumstance." But the challenge now is that we've got technologies that can do that in real time, and that does change the very nature of what's going on. You are actually surveilling people who are committing crimes. It's not going back and looking at the tapes, knowing that a crime had taken place.

The Hon. GREG DONNELLY: Given the time, I'll have to be to the point and place other questions on notice. Mine is a rather overarching question, and it is this: The actual matter before us is the utter workplace revolution that has taken place in recent time with respect to the use of technology, broadly defined. I think one

would be very brave to suggest that the rate of change is going to be slowing down anytime soon. So my question is, given this revolution that is playing out before us is likely to continue into the future, almost indefinitely as far we can see, I think, how can a society or a community set itself up whereby it can work through what is this myriad of issues that we have just almost, because of lack of time, been able to skate over in this conversation which has gone for about 50 minutes? It just seems to me that grasping the enormity of the issues is just a job in itself, which gets me to this particular question, that is: In terms of jurisdictions overseas which have grasped the enormity of this and have set in place frameworks or structures at that macro level to deal with some of these questions, I would appreciate any advice that you may be able to give about where those jurisdictions are.

PETER LEWIS: Greg, that's a fantastic final question and really wraps up this discussion. Do you know what? I think it could be here. If you look at the way this technology is being adapted in different parts of the world, you've got a hyper-capitalist vision of the technology in the States, which is very much driven by looking at everyone as a single consumer who can give up their rights with a click of a button. You've got a Chinese model of State surveillance where you basically build your credits as a citizen based on your observable behaviour. You've got a rules-based system emerging out of Europe which places a framework around it. And here we are in Australia trying to work out how we can create a framework for technology that reflects our values.

The really interesting work that Ed Santow, who Mark was talking about previously and who is a former Human Rights Commissioner, has come up with is the proposition: Can we imagine an Australian tech infrastructure that embeds our values of liberal democracy and anti-discrimination into the way our technology develops, creating frameworks for the development of AI that are compliant with anti-discrimination but also compliant with our labour laws? Again, back to my original proposition, we've got a great base from that 1996 Industrial Relations Act that has been evolved slowly over time, interlocked with the workplace surveillance laws which Jeff Shaw brought in 20 years ago. We've got a base to imagine how we can use technology that just doesn't accept that technology happens to us but that we can shape it, that respects the needs of employers to run profitable businesses but also respects the rights of employees. So this is where I think you guys have such a fantastic opportunity with this review to start putting some of those markers in place.

Ms ABIGAIL BOYD: I have one final question and I think it has been touched on slightly in that answer. That's this issue that has come out from all three of you in relation to effectively the ability for tech to be used in a discriminatory way. Some of the evidence that we have heard is almost pointing towards that sort of profiling. What browser you use or whatever is becoming—you can imagine how that could be used to really discriminate against whole groups of people. Should we be doing something to ensure that our laws stop that sort of discrimination through this sort of software?

PETER LEWIS: Yes, and in terms of the workplace and the rights of workers, (a) to have decisions explained to them, (b) not to be discriminated against and (c) to have a recognition that as workers they have certain rights to work collectively and not just as individual entities are all part of that mix. This is a really exciting moment for policymakers because the change is coming so fast, and the frameworks that this inquiry can recommend can have a real impact. I see Toby's got his hand up. I know we're almost out of time, but maybe Toby and Mark want to wrap it up.

TOBY WALSH: I wanted to add one more component, which is to keep human accountability. Many of these technologies we've talked about have very positive uses and will improve our efficiency and productivity. But equally, when you are using them, you have to make sure that there are humans to be held accountable. When those acts of discrimination take place, it will be that person who will be called to account for what that algorithm has advised or done.

The ACTING CHAIR: Just to give us a bit of programmatic focus, during the pandemic there was a lot more working from home. Anecdotally, both here and overseas, there has been intensification of work—people working longer hours, often unremunerated. Earlier this week the head of our workers comp insurer, icare, said that workplace stress claims are doubling every four years, including over the past two, because of not just workplace bullying and harassment but also the intensification of working from home, including being monitored. Elsewhere in the world, workers are talking about a right to disconnect from workplace devices and the obligation to respond to employer requests outside of set hours. Is that something we should be looking at here in terms of how technology has intruded into personal, family and non-working time more generally? Is that a programmatic response that we should think about?

PETER LEWIS: Yes, I think it's part of the puzzle. But there are so many moving pieces, aren't there?

The ACTING CHAIR: Yes, there are. We have come to the end of this session. I thank the three witnesses for their time and their insights. If members have additional questions, they might be placed on notice. I do not think you took anything on notice, but there is the facility for supplementary questions from members.

We will forward those to you, and you will have the right to respond within 21 days. Thank you for your time; this is all very thought-provoking stuff.

(The witnesses withdrew.)

Professor ARIADNE VROMEN, Professor of Public Administration, Crawford School of Public Policy, Australian National University, before the Committee via videoconference, affirmed and examined

Dr JOSH HEALY, Senior Lecturer in Employment Relations, The University of Newcastle, before the Committee via videoconference, affirmed and examined

Professor LEAH RUPPANNER, Professor of Sociology and Founding Director of The Future of Work Lab at the University of Melbourne, before the Committee via videoconference, sworn and examined

Dr BRENDAN CHURCHILL, Australian Research Council Research Fellow and Lecturer in Sociology, School of Social and Political Sciences, Faculty of Arts, University of Melbourne, before the Committee via videoconference, affirmed and examined

The ACTING CHAIR: I welcome our next bracket of witnesses. We usually allow a short opening statement of three to five minutes, not per person but per body or group. Are you evenly divided up into institutions? How should we evaluate your evidence? Should we take it as ANU, Newcastle and Melbourne? Do you wish to give an opening statement? There is no obligation to do so; we could just proceed to questions. Professor Vromen, if you have an opening statement of two to three minutes then you are welcome to give it, or we can just proceed to questions.

ARIADNE VROMEN: I've got a very short opening statement just about context and who I am and why I'm here, but it will be very short. You will see that the four of us do know one another and have worked together in different kinds of projects as well. My research focus that's relevant today is mainly on community and worker attitudes towards the future of work. I have long-term interests in how digital technology is transforming both society and politics, and I currently have two projects on women and the future of work. One of them is contrasting changes in the service sector and professional work by studying the law and the retail sector. The second one is looking at post-pandemic change in opportunities for work for young people in Australia, the UK and Japan. I've also undertaken earlier research on community attitudes to digital rights that focused on privacy, surveillance and changes in the workplace.

The last point I wanted to make, particularly as I know this is one of the last hearings of the Committee, is that COVID is a very important context for fundamentally changing how we see work. I think some of the things that the four of us will talk about today include thinking about hybridity and work intensification—who are even the frontline or essential workers within supply chains?—but also the rapid technological change that was adopted everywhere. It was often really necessary but in workplaces hasn't, still, always been thought through, regulated or managed in the interests of citizens or workers. That's all for me for now.

JOSH HEALY: I do have a brief statement, if you'll indulge me. I study labour markets and employment relations, and an area of strong focus for me in recent years has been around developments that shape the future of work. I've studied, among other things, technological change, automation, gig work and progress towards the establishment of a living wage. I want to briefly draw the Committee's attention, if I may, to three recent studies that I've been involved in that I think are relevant, to some extent, to the terms of reference for your inquiry. The first of these is a public report, and the other two are more academic contributions.

Firstly, I was a member of a team that produced a detailed report on the future of work for the New South Wales Government in 2017 and 2018. If that's not already on record then I'd very much like it to be. This was a piece of work that was commissioned by the NSW Department of Education as part of its Future Frontiers initiative that it was pursuing at the time. In that report we attempted to anticipate how new technologies could reshape labour markets, occupations and skill requirements in Australia over the coming decades. Among other things we show that technological advances are likely to continue to favour workers who are doing more cognitive, creative and non-routine types of work. At the same time we made the point that, while technology itself is a powerful driver of change, it's not the sole determinant of outcomes. Institutions and, indeed, policy choices continue to matter a great deal.

Secondly, as part of a team of authors in a 2017 academic book chapter, we again looked at how rapid technological change is sort of stretching or testing the conventional boundaries of employment and generating new forms of work and also new business models that I'm sure you're all by now well aware of—many of which fit awkwardly into existing paradigms that are predicated on stable, wage-earning employment. One of the points we made in that chapter is that while policymakers are often asked to accommodate or adapt to emerging technologies, there are also many possibilities for exploiting many of these same kinds of technologies to in fact assist with matters of compliance and enforcement of minimum employment standards and other kinds of employee rights.

Finally, and most recently, a paper that appeared last year in an academic journal was more focused on the way in which the COVID pandemic has impacted on our understanding about where the future of work is leading. We argued that the debate that had been very largely centred on concerns about automation and the emergence of the gig economy has splintered and expanded in many ways to take in a whole range of new and important issues that Professor Vromen alluded to in her opening statement, including, of course, remote work; the protection of essential workers; temporary wage subsidies; and, more generally, government's responsibility to maintain social cohesion and rebuild economic vitality after a major crisis like COVID. In that article we again highlight the enduring importance of government and other emerging opportunities for government's regulatory enforcement powers to be bolstered by the use of new technologies, using those technologies and viewing them not just as a threat but indeed as an instrument of regulation. So that's an important point that we made. That's essentially it. Thank you very much for the invitation and I look forward to the Committee's questions.

The ACTING CHAIR: Before I move on to the University of Melbourne, you mentioned the report for the Department of Education that you did in 2017.

JOSH HEALY: Yes.

The ACTING CHAIR: If you are at liberty to do so, are you able to provide a copy of that to the Committee? You can take that on notice and go away and reflect, but if you can that would be great.

JOSH HEALY: Yes, of course. That report is still publicly accessible, by the way.

The ACTING CHAIR: Maybe you could flick us the links and we could download it.

JOSH HEALY: No problem.

The ACTING CHAIR: Thank you. I don't know who wishes to do the brief opening statement for the University of Melbourne. Professor, I might start with you and see how we go.

LEAH RUPPANNER: I appreciate you deferring to me. Thank you very much for the opportunity. I will keep it brief because a lot of what we're saying is aligned with what's already been said, and I want to give you the opportunity to have time for questions. I have a couple of things to flag in addition to what's already been said. We're working quite critically—we're talking about surveillance as an outcome but we're looking at how the tech actually gets felt and, in particular, how gender bias or bias in general can be built into the tech before it is even delivered. I want to flag that as an additional component. As we think about surveillance, you're talking about the outcome but we have to think about the precursor and the way in which we end up with that product.

We're writing a micro-series on this, in particular thinking about AI and its implication for women. I know we've talked a lot about this—and we'll probably hit on this as a shared, aligned interest across our team, across the universities—how do you make sure that as these things are rolled out they don't intensify existing marginalisation? I think it's important to raise that in particular around caregivers—so surveillance at work and thinking about who's present and who's not, and considering that the contexts in which people are "absent" from their time on a computer may be because they're in caregiving roles et cetera. They are one or two things to summarise my own statement, basically thinking about how technology itself can be biased and thinking about the implementation as exacerbating bias. I've been thinking about the educative component about AI in short courses that already exist at our institution as perhaps one way to increase awareness about these issues for the general public. Brendan might have one little thing to add and then I'll be quiet.

BRENDAN CHURCHILL: I will, but I'll be very brief. I will add that part of my expertise is looking at youth unemployment. For the last 10 years I've been looking at youth futures, young people and how the GFC, or even the early days of COVID, have impacted young people. I think that's really important because it gives a lot of context for the future of work and how we think about the future of work for young people. What's really interesting to me as a sociologist is the young, despite the cliché of being "the future", are often absent in these debates about the future of work but they're very much impacted. A lot of my research speaks to thinking about young people, how they're going to be affected and how we can mitigate the impact of economic disruption.

The ACTING CHAIR: Thank you very much for those brief opening statements. I will proceed to questions from Committee members, given I think I took more than my fair share last time. I think there's general consensus around that proposition.

Ms ABIGAIL BOYD: I thank all of you for coming along to answer these questions. My first question is in relation to the potential for discrimination and building discriminatory norms into technology, which will only exacerbate inequality. Professor Ruppanner, would you like to elaborate on that and what we can do as policymakers to ensure that we don't end up with the application of discriminatory tech?

LEAH RUPPANNER: I will talk a little bit not necessarily about the intersection of surveillance, but we are working on a project right now about gender bias and hiring algorithms—so that one critical point of entry into employment. We are finding quite clearly multiple modes in which bias gets introduced. What we're finding can help broaden out to what will happen with surveillance tech. There is biased data that machine learning utilises, so all the algorithms that are being built are using data that usually captures the world in which we live, and we all know that the world in which we live is biased. So it's not a surprise when algorithms reflect back to you what we are.

We're thinking about that the data it's trading on is unequal and who's missing. We're talking a lot about the missingness in the data. If we're building tech apps that are capturing data from our world, some people aren't giving them data. That's just the truth; they aren't. Who are those groups and then what does that mean for the development of the technology? We're thinking about who the people are who are developing it. If we know that tech is disproportionally dominated by men, and in particular white men, what does that look like in terms of our priorities for how the tech got built? When we did this project—and a PhD student is continuing the work—on gender bias in hiring algorithms, we were finding it at all points. We were finding that humans have unconscious bias that gets built into the tech, the data is biased and then the application itself can be biased in the outcome. It's not a small problem, and if it were—the tech companies know this is a problem. So if there was a simple solution, there would be a simple solution. We need to be aware of it.

There are a couple of things in terms of government. One is how do you have awareness and understanding so that as you're rolling out the tech, at least you understand how this can exacerbate bias and inequality. How can you work more directly in partnership with the tech companies and universities? Because we bring a different specialisation and we have a different knowledge base. How can you create a government-tech-university that doesn't just sit in STEM. I'm going to say that again—that doesn't just sit in science, technology, engineering and mathematics. It's the moment for social sciences in part because this is increasingly part of our digital world, yet we seem to have these conversations—I'm going to get passionate about this—in very deep silos about how all we need to do is engage tech with engineering, math and computer scientists. It's so wrong, because actually if we all work together, we'll end up with better tech for everybody. Those are my solutions.

We're trying to do an educative process too for the public, so at least people can be part of the conversation and historically marginalised groups can be present. I am an academic, so I could talk for the next 35 minutes. I'll stop there. It's not an easy problem to solve. Government can't do it but government can nudge partnerships that can perhaps do a better job and be aware of how this is happening.

Ms ABIGAIL BOYD: Do any of the other witnesses want to chip in on that?

BRENDAN CHURCHILL: I would like to add one more thing. I want to ping off what Leah just said, which is that we need to make sure that we have the training pipeline that addresses that. She is right to point out that we need to consider humanities and social sciences in developing that pipeline. But perhaps an area that government can help is ensuring that we get equity groups through that can fill some of these gaps.

The Hon. ANTHONY D'ADAM: I was interested in Dr Healy's comments about enforcement. One of the things in terms of our industrial relations enforcement approach is that it's premised on physical workplaces in concentrations. Obviously we are seeing, through technology, the enabling of a much more distributed form of work organisation and work from home. When I was a union official, we used to have an award right to have a noticeboard in the workplace on the assumption that the union could communicate information about workplace rights via the noticeboard. But obviously noticeboards are anachronous now and the way that organisations communicate to their employees is technologically enabled. Can you perhaps offer some comments about how we might facilitate workers, via unions or through other mechanisms, to give them access to the information that they need to be able to enforce their rights at work?

JOSH HEALY: I think that's an excellent question. I'm not sure I have a complete answer to that. Of course, one of the realities of our present contemporary employment relations is that unions, to some extent, have struggled to find members in a variety of new sectors at work, and in a way the COVID experience sending much of the workforce—not all of it but much of it—into a situation of working from home has exacerbated some of those concerns. On the point about working from home, I did want to briefly say that this has really been transformational. In the years prior to COVID, despite much hype and talk about how technology is going to enable us to work remotely, there was no sign of any dramatic pick-up and the prevalence of that. Now of course, with COVID, it has become a much more mainstream experience and many organisations are contending with these sorts of hybrid arrangements where some workers don't want to go back into a full-time office environment of the kind that they had before, and that is creating new tensions.

In relation to the information dissemination points, again I think that there is a role here potentially for government to play. Of course, our enforcement agencies that are at a Federal level, like the Fair Work Ombudsman, have done a lot of work to try to get the message out there to working people about their various rights and entitlements. We know that there have been enormous problems with underpayment and noncompliance, if you want to call it that, by employers. The Fair Work Ombudsman has generated all sorts of materials of various different kinds—YouTube content, web content, going out there and running campaigns—trying to spread the word. I think that is a fundamentally important role of governments and State agencies in communicating that kind of a message.

It's also about talking, of course, to employers. This dovetails with some of what we were saying in the papers that I've mentioned around at least some employer groups alleging that the system is overly complex, that there are all sorts of trips and pitfalls along the way that employers potentially get caught up on, and that the use of these kinds of technologies might enable them to be more regularly compliant. That's an area where there has been a lot of talk about some industry-government partnerships of various kinds—a bit similar to what Leah was saying in her remarks about collaborating around the design of technology—where governments could conceivably work with employers and employee representative organisations to ensure that the kinds of information that are communicated are accurate and reliable and, in effect, putting on sort of a stamp of authority on that information so that the playing field, so to speak, with information access and information quality is as even as it can be. I guess that's speaking a bit around the core of your question. I will let others chip in, if they would like to, on that point.

ARIADNE VROMEN: I think it's a really interesting question. There are two bits of the question. Working from home, we found with our lawyers that we surveyed that there was a real gendered experience in that work intensified for women—they were working a lot more hours than ever before—but they also felt a lot more productive. A majority of women felt more productive working from home but less than a third of male lawyers felt productive. So there is a real tension there between how the hours can extend and become blurred into your private life and you can be working 24/7 when you're working from home as a professional worker. That's one point I think is really important.

The other point that your question was asking about, what happens when people aren't in the workplace, how they organise and talk to one another, and how collective action happens. I guess I will put my political scientist hat on. That's something that's always of interest to me as well. One of the things that happens is a lot of things move online and move informally into social media, and this is where we see the blurring between public life and private life. We talk about that as context collapse, that there is no separation anymore between your public and private life and communication becomes really informal. This can be kind of good for unions who want to engage with people on issues that matter to them and organise them, but it can also become dangerous for less powerful employees in the workplace when people can see into their private lives and might not agree with the kinds of things that they say or think.

We have also seen in our research with young people, particularly in hospitality and retail work, where they are already subject to customer abuse in real life but more and more of that is moving online as well from co-workers or through social media channels. It could be through work channels like Slack, or it could be people hunting you down on Instagram and following you and harassing you. We kind of see more and more evidence of this. It's kind of a catch 22: The informal space is good for raising issues, but it can also just really exacerbate that blurring between public and private life as well.

The Hon. ANTHONY D'ADAM: I asked the previous panellists about psychometric testing. It is also an area where I think the biases potentially could come to the fore. The experience—and certainly in New South Wales—is the psychometric testing is delivered by a third-party provider. There are questions about the data that they collect on applicants of who owns it and how it's protected and controlled. What do we need to put in place to allow those who are providing this very sensitive information about them so as to unpack the biases to try to uncover what the underlying assumptions are behind the use of these types of tests to select applicants? It's ubiquitous now in New South Wales public service, so it affects a very significant part of the employees in the State.

LEAH RUPPANNER: I think Brendan is working—sorry to throw you into this—on a project thinking about this. So he might have some insights.

BRENDAN CHURCHILL: I am, but we're not thinking about what government could do. I guess I want to say more regulation—I mean, that's obvious to you—tighter controls, making sure that information cannot be shared across companies and organisations and who has access to that information within organisations. I think they are probably issues that you are aware of.

LEAH RUPPANNER: Can I tell you more about his own project too, even though he is not as forthcoming as I want him to be? One of the interesting things that he's talking about, too—you're talking about the tech side of the regulation, which actually sits a little bit around my area. You were saying about if you have tech moving into your home life and now all the organisation stuff you're doing—you bring up this question about the psychometric testing but I would say, what does it mean if you are organising unions on an app like Facebook and where does that information data get fed to the union organisation? Who's owning the data if now people are in tech spaces? The answer is technology companies, and what happens on that.

But one of the interesting things that Brendan was thinking about—sorry to throw you in it—is that, in addition to that, if you get a diagnosis, or if you get one of those tests and then I get that test and I find out I am this type of person, how does that shape your career trajectory? How does that shape what kind of jobs you do and what type of roles you take on? How do you think of yourself as a worker or as a person? It's also that tech that then creates identity that may shape decision-making. I know that's not quite what you're asking but, in addition to that, thinking about those as being used as instruments that then shape you as a worker is actually that other critical point—and what kind of opportunities you open yourself up to. I'm sorry for squealing on you, but here I am.

The Hon. ANTHONY D'ADAM: I suppose the other element of my question is about the assumptions. Psychometric testing assumes certain characteristics and certain qualities that are going to be effective in a particular role. That's not necessarily—to those who are selecting and who have the formal responsibility for selection, it's not entirely apparent how those assumptions are actually filtrated through the methodology that underpins the psychometric testing.

LEAH RUPPANNER: It's going to be based on existing data, and the data is going to have some groups and not have others. So it's going to be the same issue you are talking about. We were in conversation with one of the big hiring firms a couple of weeks ago and thinking about how do you start thinking about people in terms of skills as opposed to matching them to—how do you shift it towards a skill-based approach to recruitment and employment, which is slightly different to what you're saying but the same thing. And then who do you have in your pool and who don't you have? I did one of these psychometric tests, and they told me I shouldn't do any data science. I didn't even get to the interview for a big US company because I wasn't good at data, based on some component of my personality. Don't worry, I've told them they're wrong every day of my life, but you're absolutely right. That was a door closed as opposed to a door opened.

BRENDAN CHURCHILL: To add to Leah, these groups are not perfect groups, but we tend to think of them as these kind of—the data is drilled down and you're put in a group. Changing your answer on one question on a test might've actually put you in another group. They're kind of taken as very serious, but the data—as Leah is talking about bias and algorithms—there's a lot of bias in these tests. I think that's a real problem about how these tests are deployed, who constructs these groups and how you get put into these groups. There's lots of anecdotal evidence in this project that I am doing of these traits—you're being assigned to a group because of a specific set of traits. You are then put into a team, and you are then told how to interact with other members of teams within the larger organisation. That opens itself up to work conflict and a lot of stress and anxiety around being in a particular group that is based on a questionnaire that you filled out at the start of the job. I think it's rife with a lot of issues, and further research needs to be done.

The Hon. GREG DONNELLY: Thank you all for participating in the inquiry. Mine is a very broad, general question. It's self-evident that we're looking at what is a myriad of issues associated with the subject area of workplace monitoring and the monitoring of individuals in their work. I get the sense that when you're understanding the boundaries of this, the boundaries keep moving. It's a moving feast, such that surely there are individual legislatures in the world—within individual legislatures, there is some stand-out work that is being done by those legislatures to try to understand this work revolution before us and the changes and how it's affecting people. Institutions also—particular stand-out institutions globally—have a particular strength in looking at and addressing these issues that we're trying to tackle. I'm just wondering, each of you, or those who might have the insight, are there particular legislatures and institutions globally that are self-identifying as being at the cutting edge of doing work in this area and have the wherewithal and ability to continue to deal with this over time?

LEAH RUPPANNER: I think you're looking at the institutions right now—the University of Melbourne and the Australian National University are here. I think this is really a moment for research where you need the depth of knowledge that's coming through academia, in part, because it's interdisciplinary and we're thinking about these things over time. That would be one of my ideas. It's the time for the strength in the university in terms of its depth of knowledge, but other people might have concrete—other organisations that they think are useful. But I think this is a moment of expertise. In a time of instability, it's a moment of deep expertise that actually is incredibly valuable.

JOSH HEALY: I would just add to that that there are undoubtedly some terrific institutions internationally that are doing fantastic work to try to understand what's happening technologically and what the response from policymakers and social sciences might look like. It is important, though, that we have a kind of national understanding about what's going on in Australia, and indeed in more specific jurisdictions within Australia. The kinds of social norms and expectations and the kinds of histories that we've got industrially and organisationally differ a lot. One of the things that has bothered me and others is that much of the thinking about technology, how it ought to be regulated and what the future of work is going to look like is very Americanised.

There are obviously terrific institutions that are thinking about these things, and much of tech is, after all, situated in the United States. Part of what we've been arguing is that we do need local expertise to understand what's manifesting in the Australian context, and things actually look quite a bit different. We don't yet have, fortunately, the same problems with inequality. Unfortunately, we are going further in that direction, but we don't yet have the same kinds of problems that are rife, and have been for decades, in the United States of earnings and income inequality, low pay and some of the working poverty. We're not quite yet as bad on some of those measures as other countries, so it's important that we are understanding what the future of work might hold to also understand the institutional legacy and the different trajectories that different countries are on. Australia does look very different and, for that reason, I would agree with Leah that we need good local expertise that's focusing in on these things and providing advice where we can to policymakers.

The Hon. GREG DONNELLY: I am just wondering, from a legislative point of view, if there are jurisdictions in Europe—if there are states or nations in Europe—that are doing particularly good work in this area?

ARIADNE VROMEN: I would say that the introduction of the data protection regulation in Europe has been incredibly important for privacy and turning privacy of data and the collection of data into—it's consent driven rather than consent to having the collection and sharing of your data being an afterthought. This is kind of a normative idea within Europe that is moving into the workplace and moving into institutions as well. It's slow, but it is changing the way we think about how citizens own their own data and also have a right to privacy. I think Australia is quite behind in having a level of sophisticated conversation in the same way that we can introduce regulation and that we can regulate technology companies to better protect their users and better protect data in general. This also needs to come into the workplace.

We're kind of seeing bits of it. Even the current public debate on the use of facial recognition software is really important. That's happening in workplaces. Even the debate we saw in the past few weeks about Bunnings and Kmart profiling their customers, they're already using this kind of surveillance software in their warehouses, profiling their workers and measuring the output of workers. In our work with retail workers, they feel surveilled by their employers. They also feel that customer feedback is being used to evaluate their performance. These things are already happening. It's really important that we start to develop expectations and benchmarks about what are acceptable and unacceptable levels of intrusion into privacy.

The Hon. SHAYNE MALLARD: This follows up on Greg Donnelly's line of discussion there. It's interesting that you talked about the universities being at the forefront of this policy debate and development. I have some involvement with one of the universities which is not on the screen, and during the pandemic its foreign students all went online. They are still online—mainly based in China. The 600 students in a lecture broke into subgroups with tutors. The groups are monitored in terms of the interaction of students with the tutor, so that they can assess how the tutor is going. So there are a whole lot of things in the university space that are happening. Of course, that goes to Leah's comments around the built-in prejudice and so on, and young people being involved in the software. So I wonder, in your universities, what protocols or framework or, as we heard the last witnesses talk about, guardrails you have in place around this sort of technology, with the university using it for students? No-one is answering.

LEAH RUPPANNER: I don't think we know. I want to say I don't know. The short answer is I don't know.

The Hon. SHAYNE MALLARD: In your own backyard? I'm not being critical, it's just—

LEAH RUPPANNER: [Inaudible].

The Hon. SHAYNE MALLARD: It's happening everywhere. It's not just in Bunnings, it's at universities and business schools and so on.

LEAH RUPPANNER: Absolutely. You are not wrong. You are not wrong in your way. Just something else to add, kind of, unrelated—although, Josh seems to have a passionate point, so I should just be quiet. But just thinking about even the fight that happened with the ABC and Facebook in Australia—so thinking about what's happening in terms of regulation and who owns the data and what happens, is like that fight about does Facebook

pay ABC for their content. And then Facebook said it will just pull out of Australia. I mean, your point is the point, which is, where is the regulation and where are the guardrails? And then, add to it, who owns the data? Who is the fight with? Is the fight with Zoom? Now, where are the guardrails? It's very messy. So when I say "we don't know," I mean that in part because there are so many stakeholders with so much power, and then how do you bring a service in that's coming, say, from the US, like Josh says, that's been built in the US based on US minds and technologies, and who owns it? Who owns a student's data? [Inaudible]. So I think that's where you—and we're saying to you that the university is not distinct from a workplace.

The Hon. SHAYNE MALLARD: There is an issue of trust, too. Foreign students have different expectations and concerns around their face being on a digital platform, particularly Chinese students. So you've got to be culturally aware of that.

LEAH RUPPANNER: Absolutely.

Ms ABIGAIL BOYD: In the last panel there was a suggestion that there was or could be a market for secondary data—data that has been collected from the use of this software and then sold on to another party or taken in by the original software vendor to improve future products. Are you aware of that occurring, and does anybody have any insight into how that's occurring legally and what we might do to address it? Any takers?

The ACTING CHAIR: Is anyone game to chance their arm there? Okay, we'll take that as a comment.

Ms ABIGAIL BOYD: Deary me.

The ACTING CHAIR: I will ask this question to the panel. It sounds like in Europe there's a pretty strong regulation about data use and collection, and privacy generally, and that's how it's being managed in workplaces. They're not approaching it from a workplace-specific focus, it's more from a general appreciation of data privacy and security, and there needing to be active consent. There's been talk, I think in Europe and maybe in North America too, about digital bills of rights. Is there anything you can tell us about those sorts of legal developments? Nobody wishes to jump in? Professor Ruppanner?

LEAH RUPPANNER: I'll answer all your questions with my opinion. Again, I'll say this is not necessarily where our expertise is sitting. With our Hallmark research we're looking at AI and policy, in particular, not what is the regulation or what is the regulatory framework around that. I can find some of that information, if it's useful for you. But this is, again, where I think what we're seeing is it's an interdisciplinary—you know, there's the centre for Artificial Intelligence and Digital Ethics at the University of Melbourne, where they have the lawyers there with the computer scientists. So this is why I'm saying to you—I'm going to double down on my statement that universities actually hold the depth of knowledge across the complicated questions like this and what government could do is to better link people together, and investment in these questions. So what I can say is, I don't know from my area of expertise, but I will say that there is a depth of area of expertise at the university. This is where you're asking very, very tricky questions that you really need an expert on AI law to answer that kind of question.

The ACTING CHAIR: Well, yes and no. I'll ask this question and see if you've got any views on this. In 2015 the economics writer of *The Sydney Morning Herald* postulated that if people only spent 10 minutes a day checking their emails outside of work that would theoretically earn themselves an additional week of annual holidays. She was making the point that people do a lot of work outside of core hours. The Centre for Future Work has found that in 2019 Australian workers worked nearly six weeks a year unpaid. The following year that has gone to nearly seven weeks. That's nearly $100 billion worth of additional work performed by the workplace for which people haven't been paid. So it's not so much just wage theft but also time theft. A lot of those additional hours have been facilitated by technology—people being able to get texts and emails outside of work hours.

Even before the pandemic we saw work—once upon a time being limited nine to five, Monday to Friday—leaching, bleeding, into people's personal lives. And now, as a result of the pandemic, it is bleeding into their homes. It is not so much working from home but living at work. That has led to work intensification, which you have given evidence about. Our workers comp insurer said earlier this week that that is one of the things driving increased stress claims, because of the intensification of work, as well as other workplace issues. So in other jurisdictions—Italy, Canada, the Netherlands, the European Union—and even here in Australia, there is a campaign for workers to have the right to disconnect from workplace devices outside of agreed hours. This is the idea of drawing a line, and it seems to be gaining momentum—not so much in North America, other than in Canada. Is that something that we should usefully think about as some way of protecting workers from burnout and from working too much unpaid overtime?

ARIADNE VROMEN: Yes. I think that it is really important that we point out this issue as a part of intensification—that expectation, particularly for professional and knowledge workers, of being online all the time and responsive all the time, just to manage their workloads. But it needs to be driven by employers.

Employers need to recognise that this is happening. They need to send emails only during work hours. Clearly, we are studying a very small group by studying lawyers, but they are at the pointy end of being on call all of the time, and that only intensified when they were working from home because there were no boundaries between work and deadlines. So I think it's really important that we work with employers to establish guidelines that limit where work moves into life, as well. Josh?

JOSH HEALY: I was just going to say a couple of things in response to that. This is one area where some sort of collective intervention—perhaps spearheaded by employers or perhaps driven by government—is necessary, because individual responses to this kind of an issue are not going to change the underlying structural problems, right? The other thing about that—so in answer to the final question that you put to us, yes, I think this is the question of a right to disconnect or some sort of entitlement to be offline in family hours, at antisocial times. I think that is well worth contemplating and thinking hard about. Of course, there is a long history of labour rights. The whole labour movement, to some extent, has been geared up around trying to regulate the extent to which we impose boundaries between working and non-working time, and new technologies have, sort of, done some damage to that and have eroded those boundaries.

But the other thing is—and I do not think you mentioned it in your comment—that this is partly about technology but it is also about the fact of precarious work. Many people are in casualised, non-ongoing, non-permanent, temporary and third-party managed varieties of work and those are circumstances that lend themselves to doing a lot of unpaid overtime because people feel insecure. The pandemic has made that worse and the availability of technology has meant that a lot more of that is happening. But it is also a structural facet of our labour market.

The ACTING CHAIR: That is true. I will come back to that. The New South Wales public sector is not just the biggest employer in New South Wales. It is the single biggest employer in Australia. How we grapple with these issues could have an important influential or normative effect on other work sectors. I think this is a really important thing for us to come to grips with and get right.

JOSH HEALY: Absolutely.

The ACTING CHAIR: One of the things that I have noted in talking to people working in the public sector at all different levels is they have noticed that this work intensification, driven through the COVID pandemic, is still there even though people are now more often returning to the office. They are still getting emails from their supervisors at 4.30 p.m. on Friday asking for a whole bunch of work product to be delivered by 9 o'clock or 10 o'clock or even midday by the next working day, which is Monday. And there is the little caption at the bottom of the signature saying, "We understand that me sending this email to you at 9.00 p.m. doesn't mean that you should respond at these times and you should respond at a time suitable to you." There is a lot of passive-aggressive stuff that seems to be going on at all levels of management even in the New South Wales public service which, in a sense, is not precarious work because people have ongoing employment, and yet people are anxious about their work security as a result of this intensification of work. It sounds like we need legislative protections for people because it does not sound like managers or workers are able to navigate this without some assistance.

LEAH RUPPANNER: Can I jump in? We have done some work on this. Now you have hit our area of expertise—well done. We did some work on this during the pandemic. I want to point out, with all respect, I think you are confusing some components.

The ACTING CHAIR: Sure.

LEAH RUPPANNER: There is increasing work productivity and what you are supposed to do in the week, which is different from flexibility and when and how you do it. They are two different ideas. I do not want to get it confused where people are being asked to do 18 hours of work in a 10-hour work week versus, "I actually have kids at home," or, "It works for me to send emails at 4.30 p.m.," or, "It works for me to send emails in the morning." Some of the things we were hearing from our interviewees during the pandemic was, "Hey, actually for me it works really well to switch off during the day to do the school run and then switch back on at 4.30 p.m. at night and I can send a bunch of emails." Those are two different questions.

One question is about are people being asked to do too much and has productivity gone up because we now have flexibility in work? Or is the problem that people are sending emails at non-standard hours? That flexibility of work means flexibility in how you do it, when you do it and where you do it as those three components. I want to protect that idea of flexibility in how and when because I think it works well for people with other demands and people who may switch off for a couple of hours and then switch back on at night.

The ACTING CHAIR: Sorry, I do not mean to interrupt you. Just on that, flexibility sounds good but I am getting feedback from both public and private sector workers where they are not allowed or it is frowned on

to clock off during the day. They are expected to do their core standard hours, but there is meant to be before-and-after hours flexibility in their availability. This seems to be the problematic aspect. Back to you.

LEAH RUPPANNER: Just to make sure we are talking about overwork rather than flexible work.

The ACTING CHAIR: Yes.

LEAH RUPPANNER: The problem now is overwork and then how do we address overwork. I just wanted to make that distinction because the problem is that people confound overwork with flexible work. Then the idea is, "Okay, we have just wound back nine to five," which is not the answer.

The ACTING CHAIR: If the issue was that people were just working flexibly, I don't think anybody would have an issue there. It is the fact that there are downsides that are causing concerns. Can I ask this of Professor Vromen: Can you tell us more about your research on worker attitudes to surveillance and automation? What sort of policy responses should we draw from that research?

ARIADNE VROMEN: Mainly we were looking recently at the surveillance of workers in retail. We wanted to get their attitude to feeling surveilled. We have not yet done part of the research that looks more at what happens particularly in warehouses or supermarkets, which are the bulk of the employees within the retail sector. Even as consumers we can see what has been changing rapidly over time within supermarkets in general and with other kinds of retail stores. But it was more that they felt under constant scrutiny. It was not that they did not feel that they could use the technologies; they knew how to use the technologies. It was more that employers were introducing technologies, both surveillance cameras within their workplaces—that that was being used against them around the use of their time at work and their productivity and efficiency at work—and also that vigilantly collected customer feedback was becoming part of their performance evaluation as well.

This seems to be happening in some sectors of work more than others. Going back to that issue about precarity in the retail sector, people are more likely to be young, women and on casual contracts than the rest of the workforce. They are also more likely to be from non-English-speaking backgrounds than other sections of the workforce. This means that a lot of these people do not have a voice to question the use of this kind of surveillance and customer feedback mechanisms within their workplace. It is very hard to say, "It is not the right thing to be doing. It makes me feel unsafe or insecure or pressured." It is really thinking about where we draw the line around the regulation of what are acceptable practices within these kinds of workplaces. Where are the trade-offs between a safe workplace and a productive workplace for both employees and employers?

The ACTING CHAIR: This is a question to each of you. We have talked and delineated a lot of the issues, which are very large and very complex, that are facing work and workers. If each of you could name one policy response that the Government or Parliament should adopt, what would it be? I might go to each of you, and if you do not have an answer you can take it on notice. Professor Ruppanner, would you like to go first?

LEAH RUPPANNER: What you said originally—that we have the potential perhaps to get the framework right through the New South Wales public sector in how to approach the future of work—I think you are right on that. I always say even the policies for child care are gradually even making sure that men can care. But let's put that to the side, let's note that. In terms of the future of work, when you said, "Hey, we have an opportunity to actually try to get our framework right, to understand the unique pressures of overwork, flexible work, new ways of working, hybrid work and how do we do it right," I think that is a really noble and valuable thing.

I would say, how do you make sure that you get a framework of working? How do you approach that and how do you it in your particular sector, thinking about protection, thinking about setting up norms? This is complicated because people have different interests, but is it this thing where you say, "We set a clear norm on what is productivity as opposed to time-based measurements"? Do we start with productivity measures? And we set those out very clearly between employee and employer about once you hit that productivity measure—done, that is productivity. Is it about setting norms about when emails are sent or not, or who works on weekends or who does not? That is workplace policy.

This is why I am saying these are separate things that have different workplace policies and approaches. And then do you give caregiving leave? Do you provide financial incentives for people to use money? This is my current passion. Do you give people resources and money to help them manage their work and family demands, small pockets of money? Or do you give them some sort of resource? I think those are interesting interventions that can be done right now that do not require big shifts in Federal governments or whatever. That would be what I would say. When you said that this is a moment where we can get it right, you are spot on. How do you do that in an evidence-based way?

The ACTING CHAIR: Professor Vromen?

ARIADNE VROMEN: I have a list of a few different things, but I'll just stick with one for now.

The ACTING CHAIR: With the rest, please provide them to us on notice, if you'd like to.

ARIADNE VROMEN: I can do that later on. One thing we would need to have is enforceable standards of privacy within the workplace, which includes more standardised training in the way that data is used, collected and analysed, particularly for managers and employers, and that this is not left to both IT sections of workplaces or human resources, so that all managers really understand any data that's being used about their employees at work.

JOSH HEALY: I think I would like to take the question about specific legislative responses on notice, if I may. If I can just reiterate the point that I made about—from my point of view, anyway—the fundamental importance of government leadership in some of these areas. I think it can't be understated, because we have become too reliant on individuals having the onus of the responsibility for adjusting to this and deciding where their own personal limits lie. That entails a degree of personal risk around some of the objections to being surveilled and around some of the ways in which data is used. Brave individuals, from time to time, do amazing things, but we can achieve much more, successfully, with less personal risk, in a framework that is established by good government intervention. I want to reiterate that point. I'm sure the Committee already knows that full well. I will take the specific question on notice, if I may.

BRENDAN CHURCHILL: I think I would like to take it on notice, as Josh just said. Perhaps, if I could just end with this comment, that we need to put in place access to good quality work—good jobs—and perhaps expand our definition to incorporate data privacy and the right to privacy as part of the idea of what is good work. Keeping that definition as broad as possible can kind of attenuate some of these issues. Addressing precarious work, addressing non-standard work, addressing data privacy as well, will make for better workplaces and better lives for working people.

The ACTING CHAIR: In conclusion, I think, Dr Churchill, you were talking about some of these platforms or devices or software that's used—particularly developed overseas, based on overseas data. People often think about technology as kind of being value neutral, but I think you are saying that there is a lot of subjective judgements that go into developing these algorithms, which can have either—I think, in terms of facial profiling—an ethnic bias or a gender bias, or possibly both. Do any of you want to address that issue in any more depth, around the idea that this is not some sort of value neutral solution, but other people have made a whole series of judgements, before we unleash it in our workplaces? Any takers?

LEAH RUPPANNER: I will just say that I said that, thank you very much, so I want to at least take credit. Women are stubborn and do like the credit. But I also say to you, in relation to what has been said from the other groups, that the risk is that if you don't step in—and I feel for you all because you're in a terribly challenging position to have to regulate this. The challenge is if you don't step in, or there isn't regulation trial and error, there is a void, and that's where the tech companies actually are the ones who are owning the data, utilising the data, selling the data, developing the data.

In the absence of government—in the void of inaction, actually, what you end up having is tech who is the owner, and the policymaker, and the developer, et cetera. This is 100 per cent true, and we don't actually know—and also, sorry, the last thing I'll say is related to that question of bias. It is a black box, and sometimes tech companies don't even know how the algorithms are making their decisions. So whether they are making biased decisions—they're not even aware, because it's machine learning and it's happening in the background. They're talking about creating explainable tech; that's a big discussion in that algorithmic space. How do you explain how the algorithm is making the decisions? In the absence of anything, you might do something—you might get it wrong, but the absence is a void, and the void is actually worse than any potential steps that you could be taking. I guess I am sending godspeed and love on this.

The ACTING CHAIR: I would like to thank all of you for attending and giving us your valuable time and your even more valuable insights to assist us with our inquiry. Committee members may have additional questions for you post-hearing. The Committee has resolved that answers to these, along with answers to any questions taken on notice today, will be returned within 21 days. The secretariat will contact you in relation to any of these questions.

(The witnesses withdrew.)

(Luncheon adjournment)

Mr BERNIE SMITH, Branch Secretary, Shop, Distributive and Allied Employees' Association (NSW Branch), sworn and examined

The ACTING CHAIR: Welcome, Mr Smith. We have the union's submission No. 19, dated 3 September 2020. In addition, did you wish to give a brief opening statement to the Committee?

BERNIE SMITH: Yes, that would be great. The SDA is the union for workers in the retail, online retail, warehousing and fast-food industries. They are industries that are on the frontier of technological change and workplace automation. Low margins, supply chain pressure, the pandemic and competition from behemoth online retailers are accelerating the implementation of automation strategies. Our members are feeling the impacts of technological change and automation on their daily working lives. Retailers are increasingly allocating work and communicating with workers through apps and deploying automation both front and back of house. Traditional warehouses are closing and new automated warehouses opening with smaller workforces.

Allocation of tasks in online retail and warehousing is driven by algorithms specifying how, when and at what pace a task must be completed. Fast-food orders are increasingly being made through apps and self-service terminals inside restaurants. Automation will continue to change how work is done in our industries. We recognise the productivity gains that automation can bring, but it only benefits our community if these gains are equitably shared. For workers, that includes work that is secure, safe and where workers receive a fair share in productivity gains. Technological change should not be used to create unsafe workplaces or to enable unfair work practices or surveillance.

Of course, for industry to capture the full potential of automation it also requires workers that have the skills to work with the automated technology. A fair and productive society is one that actively supports workers who might be affected by automation or risk being displaced by automation to be re-skilled. To support re-skilling, we need well-funded VET institutions, particularly TAFE; we need tri-party, industry-level decision-making on training needs; we need modern termination change and redundancy laws that focus on re-skilling and redeployment, with redundancy as a last resort; and we need funding for individual employees displaced by automation to be supported by employers and government to re-skill.

We don't want to halt technological change; we are not modern-day Luddites. But we recognise the potential benefits associated with technological change and, while we recognise that, we want to ensure that the benefits of technological change are fairly shared and implemented in a way that humanises work rather than dehumanising workers. We are at a crossroads where technology has the capacity to improve or reduce the quality of our workers' lives. Algorithms, coding and software are not impartial. They are not value-free. They have preferences and biases based on who pays the piper. Algorithms, coding and software should not be regulation free either.

The ACTING CHAIR: Thank you, Mr Smith. That was very comprehensive. I might commence questioning and just ask a couple of questions, and then throw to Committee members who express an interest in asking questions. What comes through very clearly with both your presentation today and the union's submission is this notion of, if I can use the term, informed consent—that is, workers have to know that they are being surveilled, they have to know what data is being collected and they should know how that data is then going to be used by the employer. Does this mean we need to provide workers with new tools, including new rights about meaningful consultation before new technologies are implemented at work?

BERNIE SMITH: Definitely, and not just related to workplace surveillance, I don't think either, in relation to that. The reality is that if we are going to accept the pace of technological change, workers need to be involved in that process. That is the only way that it works effectively. Workers also need to be involved in a process which enables them to be skilled up to be part of that process into the future. So if a business knows, for example, that they are about to build an automated warehouse, which will take five years to actually construct, is there time for the workers in the existing workplace to be re-skilled to have an opportunity to move to the new workplace and to take up higher level skill positions in those workplaces? We just recently concluded an agreement with a major overseas online retailer, which actually captures all the skill levels and high-paid, high-skilled jobs. It can be a good solution for people. It doesn't have to be a bad situation for people to come into.

But there is a real need for proper consultation. Most people would have been surprised, probably in recent weeks, to have read all the articles about just what happens when you walk into a supermarket and the amount of facial recognition technology that's there and a whole lot of other technology that's there. Some of that technology is there as much to the benefit of our members in terms of them being able to protect them, potentially, when there are issues of customer abuse and violence. We see that potentially as a positive. But I don't think there has been a lot of consultation about the true extent of what technology is in workplaces and what surveillance is

occurring in workplaces. I think that not just consultation with workers; I think there's a need for a review of the whole system of workplace surveillance in New South Wales at the moment.

The ACTING CHAIR: Yes. The legislation we've got hasn't been touched for two decades, yet there's been significant technological development in that period of time. It was very much based on this notion of a dichotomy between overt and covert surveillance, whereas we have certainly received evidence in this inquiry of, if you like—I think you used the term panopticon in relation to Amazon; this idea of total surveillance not just of what is happening in a workplace, but of people as they are working and employers trying to monetise that, turn that to financial advantage, particularly in an industrial system where there is now a focus on bargaining and productivity. Should workers not have, if you like, the right to obtain some of the benefits that the employer might accrue when they monetise and deploy that secondary data?

BERNIE SMITH: Definitely. In the end, if they accrue data based on a worker's work—that's their work that has created that data—they should have some sort of a proprietary right in that as well. They should be sharing in the benefits associated with that. There should be a sharing of productivity benefits that businesses attract from that. As you said, it's been almost two decades since the Workplace Surveillance Act was put back in place in 2005. It's not just workplace surveillance; it's outside of work surveillance. It's the accrual of data. It's not the old situation of what could you do with video surveillance, or could you have hearing, listening, surveillance.

The reality is every worker's movement is now tracked in a lot of our warehouses and online fulfillment centres. It's not just, "Are they watching you?" They're actually tracking your every single movement so people have wearable technology inside warehouses and in online fulfillment centres which tracks every movement they make. Overseas, Amazon is renowned for the fact that if people have time off task, it is called, that they particularly can draw the ire of their employer. The famous situation overseas is people peeing in bottles in Amazon to keep up with the Amazon pace of work. Yet at the same time a worker dropped dead on an Amazon factory floor and was never picked up for about two hours.

The Hon. LOU AMATO: When employees sign contracts, are they told about their rights and that they will be under surveillance?

BERNIE SMITH: Most—

The Hon. LOU AMATO: Are they aware of what is going on?

BERNIE SMITH: They are two different questions, I would say.

The Hon. LOU AMATO: Yes.

BERNIE SMITH: They may say, "I'm not signing a contract that says as to whether"—

The Hon. LOU AMATO: Yes, with a lot to do and I guess they're being monitored throughout the whole process.

BERNIE SMITH: If you go into a supermarket, it will have a sign up there, for example, to tell you too that you're under surveillance for the whole time you're inside the supermarket.

The Hon. LOU AMATO: Yes.

BERNIE SMITH: As to the real extent of people's knowledge of that, I think people would have been quite shocked in recent times to work out just how much surveillance they're under. For example, as a customer also—and I would say workers face the same issues when they use workplace apps—there is an amount of surveillance of online activity as well. So if you go to Europe and you were to go to a website of a retailer or, as a worker, if you were to log in to an app, you would be asked what cookies you want enabled or not enabled automatically. You can't just go straight through to the website as you do in Australia and automatically you are tracked wherever you go after that by cookies, but you actually have to make a conscious decision. It is the GDPR—the General Data Protection Regulation—of the European Union that actually provides that. So we are a long way behind in Australia in terms of dealing with surveillance of both workers and consumers.

Ms ABIGAIL BOYD: Just following on from that question then, I think we hear a lot about the idea of obviously we need to embody these rights within our laws to ensure that employers are doing the right thing when it comes to collecting this sort of data from surveillance et cetera, et cetera. But, in practice, how realistic is it to expect workers to, I guess, object to being surveilled? When you go for a job, how many potential employees would say, "Well, I'm sorry. I can't take this job because you're going to monitor me."? What rights do they have?

BERNIE SMITH: No successful employees would.

Ms ABIGAIL BOYD: Exactly.

BERNIE SMITH: You probably wouldn't receive the job if that was the case. That's why we need legislation and regulation to address this and that's what the European Union countries have been doing progressively. And even in parts of the United States we've seen some movements in that direction as well.

The Hon. COURTNEY HOUSSOS: Thanks, Mr Smith, for your time today. I just wanted to pull out a couple of things from your opening statement. You talked about obviously we are not unique in Australia. We are facing this challenge like we are around the rest of the world. You said in other parts of the world there was some legislation addressing this question about working by apps or through algorithms. I think a previous Committee member talked about your boss is no longer a person but is actually an algorithm. This is a huge challenge and an issue not just facing this inquiry but for the world.

BERNIE SMITH: No, that's correct, Mrs Houssos. I'm aware of at least two jurisdictions very recently which have implemented legislation. In California on 1 January laws came into effect, which were passed last year, and which is commonly called the warehouse worker protection Act. I think it is more correctly called the Warehouse Quota Assembly Bill 701. That was particularly about work allocated to warehouse workers through algorithms which dictated the rate, speed, at which they worked, time off task at toilet breaks—all those sorts of things, which are monitored by so many employers. That piece of legislation actually gives workers and their representatives rights to see how those conditions are set. So it is not complete transparency into the algorithm, but some right to request information about the parameters of how those quotas have been set to work and some capacity to complain about unsafe quotas.

Our biggest concern is that what we do see is people who are exhausted coming through the pandemic. There is a shortage of workers in many respects as well. Then there are these unrealistic workplace targets that people have to meet, which are based on a perfect-world scenario—that in a perfect world you can work to this capacity. In reality, you can work to that capacity for a few hours, but not for a few years. As you get older, everyone is different in terms of their work capacity as well. We used to have the situation that as people aged in warehouses, different jobs would become available to them. Increasingly, what we see is that if you cannot keep up the pace, there is no job for you. So that is the California law which we think is a really good step forward and is a model to be had a good look at.

In the European Union at the moment they are looking more broadly at something—I think the acronym is PAIR—which is about the regulation of artificial intelligence. The Spanish jurisdiction is ahead of the rest of Europe. They just enacted something last year which goes to the capacity of workers to actually have far more transparency into the code of algorithms and the capacity to be able to look into what the code actually requires, because, as we say, codes aren't value free. They are written by somebody to do something and they do the something that the person who pays them to do it is told to do. That can be to allocate work very simply by the fastest finger approach—if you hit the button first, you get the work. Or it could be a fair rotational offer of the work to people. But it could be we set the required work pace at what the average pace is plus X.

Now, if the average is whatever it is, how many people could work at average plus X over a period of time? So there needs to be a capacity to actually look into those codes and algorithms to find out what they are actually doing, and I think that that is important to be able to provide protections for workers so that algorithms can't be written in a way that are discriminatory in their nature. They might prefer younger workers to older workers or might prefer women to men or men to women. They might prefer a union worker to a non-union worker or vice versa. Those things I think are important so it is not discriminatory in its application but also, more importantly, it is not unsafe in its application—that it sets workplace targets that are not safely met over a period of time.

The Hon. COURTNEY HOUSSOS: Absolutely. This being glued to your phone, being glued to the app—it has a huge effect on workers. And it means that they're not just then working at work; it means that in their supposed downtime they are being forced to be glued to that. What's your experience? Advocating for workers, what has been the effect on workers of the creation of these apps?

BERNIE SMITH: The apps, say, in the retail world, for example, are increasingly common, about offering of work. Our position has been that there is actually a window of opportunity here where these apps could be a force for good, but they've got to be programmed accordingly or they could be a force for atomising work and making work even less secure for people. What we consistently hear from retailers is that 75 per cent to 80 per cent of a week's hours are pretty constant, week in week out, season to season. If the app helps us securely roster those base hours as permanent work for people, that's a good thing. It's not constantly changing. Whereas sometimes today you will find people with rosters that change every two weeks or every three weeks, needlessly. So there's a capacity for good there if it's programmed that way. Then you come to the additional shifts that are offered, where in the past somebody might have called up the people on the list and whoever is next on the list

they will call up to offer the next shift to. What we see now is that with these apps, you've got two choices, really. It's the fastest finger approach—or shift bidding, they call it—so the additional shift goes out on the app—

The Hon. LOU AMATO: Shift meeting, was it?

BERNIE SMITH: Shift bidding—so whoever gets there first. Whoever hits the button first gets the shift.

The ACTING CHAIR: This is what you said was like the digital version of the Hungry Mile—people bidding at the workplace.

The Hon. LOU AMATO: It sounds like an auction.

BERNIE SMITH: You're stuck at the workplace gate virtually the whole time because if you're not there, you don't get the offer of the shift. We had one terrible example of a mum—because the shifts were offered at this particular workplace at the one time. On her way to dropping her five-year-old child to school, she had trained her five-year-old child to hit the button when the offer came through because otherwise she wouldn't have got the shift offers. To that employer's credit, when we brought that to their attention, they withdrew that process and were working through different processes, but the problem is that the fastest finger is the easiest and cheapest solution for anyone to implement.

What we constantly advocate for with employers is they should go for a fair rotational system. So if you've got the required skills and capacity to do a particular task or a particular shift, maybe you get the offer this week, and then tomorrow the next offer comes up and Adam gets the next one, and then Courtney, and if Courtney is not available, it goes to Shaoquett, and then it comes back to Lou again. It just goes on a fair rotational shift. That way you don't have to always be connected to your phone. It is almost like people get a nervous switch when they hear their phone bing: Is that work? Is that what I have to deal with?

The Hon. LOU AMATO: Anxiety.

BERNIE SMITH: Yes. So we hear a lot in the professional world about the right to disconnect. The reality for retail workers is they need a right to disconnect and that includes how work is offered through these apps.

The ACTING CHAIR: Just on that very point, I think there have been a couple of examples—the ACTU and Unions NSW campaigning on the right to disconnect. Some European countries, I think, and Canada have taken some small steps, and that's essentially where there's an agreed set of parameters around which you would not be expected to receive or respond to electronic work communication, to stop the bleeding of work life into your personal and family life. This is particularly significant given the amount of working from home that's occurring. Is this something that would be very valuable in your industry, if people had a right to disconnect or there were firm parameters when the employer wasn't able to contact people?

BERNIE SMITH: Yes, as long as it's practical. Our members didn't get to work from home at all through the pandemic. They had to be on the front line, but the app meant that even when they weren't on the front line, they didn't get the downtime they might have wanted because they were always waiting to hear when that next shift was coming. I think that if the Parliament is looking at that sort of legislation, it needs to be broader than just email content or that sort of contact. What is a fair way for work to be offered? We accept that sometimes the work can be at very short notice and maybe it is who is available at the time but, bearing that in mind, there should be a right to disconnect so you are not constantly on call all the way through.

The Hon. SHAOQUETT MOSELMANE: What impact in general would that have? I'm thinking in terms of newly arrived migrants, where the second language is English, they don't understand the app and they don't understand the system. From your experiences, what impact has it had?

BERNIE SMITH: I would say that anyone who is not, including myself, technologically capable would be disadvantaged in terms of being able to apply for the shifts, and I think you are right that those people who are newly arrived to Australia may not have the same language skills or the same access to technology. We have a number of older workers who do not want to have a smart phone. If they don't have that smart phone, they can't apply for the additional shifts, so they're basically locked into their base roster now and even if they want extra hours, they cannot get the extra hours in different workplaces.

The Hon. SHAOQUETT MOSELMANE: So they are clearly at a disadvantage.

BERNIE SMITH: Yes.

The Hon. COURTNEY HOUSSOS: We had the opportunity to go out and visit the Amazon warehouse where obviously we got one side of the story, which was that they are really careful. Now, interestingly, Amazon

has declined so far to appear before us again, which is a little bit disappointing. I was particularly concerned about the part in your opening statement when you talked about how Amazon last year advertised for a job to undertake global surveillance of their workers and their activity. Was that job based in Australia or was that overseas?

BERNIE SMITH: It was based in Seattle, from my understanding, in the United States.

The Hon. COURTNEY HOUSSOS: Are you aware of their surveilling workers in Australia?

BERNIE SMITH: Yes. Can I say that every time an SDA official goes to an Amazon workplace, they are under constant surveillance. And it's permissible under the current Act, the way the Act is currently drawn. The only real exemptions from workplace surveillance are change rooms in the current Act. Worker break rooms are not restricted from workplace surveillance. The reality is under the Federal Act our right to engage with workers is in their break rooms. That is where we are most likely to be talking to people, so the capacity to surveil those workers in that area is obviously legal within the current framework but is disturbing. And I say disturbing because I know when I personally have been on site, the national HR turns up at the same time and is sitting in the lunch room with me. I'm sure it's a coincidence.

I think what is the most disturbing incident I've had was last year. During the pandemic I received some communication from Amazon about 10 days after a workplace visit by our organisers complaining that one of our organisers was within two metres of a worker. It was probably technically a breach of the social distancing rules, but what struck me was—and there were HR staff in the tearoom whilst our organiser was there; there always are—nothing was said to the organiser at the time to say, "By the way, you shouldn't have done that. Do you mind?"

The ACTING CHAIR: Assuming it's correct.

BERNIE SMITH: Yes. But the organiser would have said, "Fine. That's okay." The fact that it was done 10 days later means to us that somebody has taken the time to go through the surveillance footage and really closely look at the surveillance footage, and then somebody has communicated back to somebody, "Look, we've got a reason to be able to pull someone up here." Basically, it is Amazon trying to send a message to their workers and the SDA that, to paraphrase Sting and The Police, every step you take, every move you make, we'll be watching you, with whatever you do. I think it's a pretty clumsy attempt to do that, but it's legal at the moment in New South Wales and the reality is that the surveillance probably didn't actually occur in New South Wales. Whilst the work occurred in New South Wales, the surveillance was probably carried out by that person who was employed last year in Seattle to review that footage. I think that if we are looking at the Workplace Surveillance Act in New South Wales, it has to have capacity to make sure that all surveillance, wherever it occurs in the world, of work that occurs in New South Wales is covered by the Act. It should make sure that it excludes people's lawful industrial activity, and I think there's a real question mark over the need to have break areas under surveillance.

The ACTING CHAIR: Mr Smith, one of the themes that has emerged in the evidence to this inquiry has been that because of the rapid pace of technological change, a lot of what is happening in workplaces with electronic monitoring and surveillance is largely unregulated in the sense that the legislation has not kept up. Employers say there is comprehensive regulation; you have the Federal Privacy Act and the workplace surveillance legislation, and all of this is comprehensively covered. What do you say to those propositions?

BERNIE SMITH: I'd be surprised if it's all covered. I think you'd be surprised to think that your face being captured at a supermarket was covered by all the current regulations. I think you'd be surprised if you knew what happened with your online activity in terms of being tracked past the website you've been to. Obviously that's been addressed in other jurisdictions, so there's a real need to address it properly here in New South Wales.

The ACTING CHAIR: Make it front of mind, so that people are consciously aware.

BERNIE SMITH: Definitely. There needs to be proper consent for people to be able to be engaged in that sort of process of being tracked or not tracked. There needs to be proper understanding of what your data is being used for. If it's being used for commercial gain, why is that permissible or what part of that gain do you get? Take Amazon, for example. During the pandemic, because of the explosion in sales during the pandemic, they increased their market share by—they doubled their market share in Australia during that period of time. They increased their sales by 285 per cent over that period of time. Worker productivity improved by 20.1 per cent, and workers got a 2.3 per cent real wage increase.

The Hon. SHAOQUETT MOSELMANE: Did they put it down to surveillance? What did they put it down to?

BERNIE SMITH: At the beginning of the pandemic they slowed the work rates down, but towards the end of the pandemic—

The ACTING CHAIR: They were speeding up.

BERNIE SMITH: It's all speeding up again, in terms of it all. Again, we like productivity as long as the dividend of productivity is shared amongst workers fairly.

The Hon. LOU AMATO: With all the extra surveillance that is coming in and the technological changes that are occurring, are workplace incidents and accidents decreasing or increasing?

BERNIE SMITH: I haven't yet found an employer to use surveillance to decrease workplace accidents, I don't think. They might use it after the event to try and attribute blame, but they don't use it before the event to address issues that we've been aware of in any great way. I think that injury rates have been going up and customer abuse rates in retail have been going up through the pandemic, not down. We're working very closely with a lot of retailers to try and turn that around, but the reality is that the surveillance hasn't prevented that.

The Hon. LOU AMATO: I just wondered because I know that among the general public the surveillance—the Big Brother, as a lot of people say—is causing people a lot of anxiety out there. It has caused them to retaliate against the workers.

BERNIE SMITH: Which is very unfair. The workers are just doing their job, and people react to what surveillance might be in the workplace. That worker is subject to that same surveillance but for their whole working day. We're seeing very unreasonable behaviour inside retail environments of violence towards retail workers. Surveillance has a role to play to some extent—I will acknowledge that—because there's the capacity to upload footage to police services, and often that assists us to find offenders. We're not, again, saying there's no role for surveillance in these places, but what's the proper role for it?

I don't think the proper role for it is in workers' break areas, where they're trying to have a bit of downtime from a really stressful environment. I don't think it's in tracking workers, potentially, away from their workplace. If you're through a workplace app, we need assurances that those apps' location services don't follow them past their workplace, as well, so that once they're outside their workplace their phone doesn't register their locations. I think that would be an unfair thing. There's a whole range of issues that really need to be addressed. I don't pretend to be a technological whiz, but I do think there needs to be a very detailed review of the current Workplace Surveillance Act in New South Wales to make it fit for purpose.

The Hon. SHAOQUETT MOSELMANE: Do we know now whether they do follow employees past their workplace? Do we have any evidence or any information?

BERNIE SMITH: I couldn't definitively say for every employer. I know some definitely don't, but also some have it to a certain extent around the vicinity of a shop so you can sign on and off through your phone within a certain distance of the shop.

The ACTING CHAIR: Just on that, often an app will ask you whether you approve of tracking only while you are using the app or tracking generally. But it is a question of whether there is a trigger. I do not know, but when workers in your industry download this app, are they asked those questions? If they are not, we do not know how that information will be used.

BERNIE SMITH: I'll have to take that on notice. The other thing I would say, though, even if they are asked, that is: Do you have a choice? If you can't work without the app, do you have a real choice?

The Hon. COURTNEY HOUSSOS: Just on that, if you're required to have the app and sign in on the app and you cannot keep the app open, then obviously you need to agree, even with that protection in place, to allow tracking even when you close the app in order to do your work. That seems like a pretty clear way that they would get around it, which then gives them access the minute that you finish work as well. That is an excellent point that you make that tracking should not occur outside of the workplace.

The Hon. LOU AMATO: Which goes to an earlier point I was trying to make that people feel as though they are being tracked all the way from the moment they leave their home until they arrive back in their front door.

BERNIE SMITH: Yes.

The Hon. LOU AMATO: And this is causing a lot of anxiety to a lot of people. In some ways, productivity also goes down because of their heightened anxiety levels.

BERNIE SMITH: Yes, people are stressed. If they never get to switch off, then they're not going to be refreshed to switch back on when they go back to work. That's correct. I think that a constant sense of never being off work means that you never properly have a break, and that means that your productivity has to be lower than it otherwise would be. But it also goes beyond that, I think. In that Amazon example, that person in Seattle who

is employed to track people's union activity, it's not even at your front door. It's inside your front door; it's inside your study; it's inside your bedroom. It's wherever you're accessing your phone and doing legitimate activity on your phone. If I want to look up the word "union" and I work at Amazon and my data is accessible, then it probably flags it somewhere, unfortunately.

The ACTING CHAIR: As far as you are aware, Mr Smith, is this sort of monitoring or surveillance at work being used by employers in your industry to address concerns about workplace fatigue and avoiding workplace accidents, for example, or is it mainly being used for other purposes?

BERNIE SMITH: I'm not aware of it being used to address workplace fatigue. Again, there are valid uses for this surveillance. We cover delivery drivers who will deliver your groceries from a supermarket doing online work. Some of those vehicles are fitted with surveillance, which means that if you were to go over the speed limit, it would warn you. That's a good thing, so there is a legitimate role for these things here. But the app that does the algorithm that allocates the work has to allow you enough time to drive that course within the speed limit. There are multiple parts to this.

It's very well and good to have technology that is aimed at health and safety, and we support that, we think that's a very good thing. But you also have to provide the capacity and work capacity to meet your workload safely. I would say that in all the industries we cover, probably one of the number one issues people face is workload. When that workload is driven by an app or an algorithm, it's as though you should be able to keep up with the green, amber and red light—as to are you keeping up with the pace of work that you should be keeping up to? Which can be quite artificial, given that all of us are different. We're not robots. We're all different; we all have different capacities. When we're at different stages of life, we have different capacities to work as well.

The ACTING CHAIR: Going back to a point you made earlier, particularly at the point of interview, there is an unequal bargaining power between a worker and the companies for whom they are working. In order for workers to have knowledge about what information their work is generating and to have some kind of involvement over whether and how the employer uses it, particularly if it is used to derive additional revenue lines, those workers will need additional tools, won't they? The existing legislation, State or Federal, is not fit for that purpose, is it?

BERNIE SMITH: No, that's correct.

The ACTING CHAIR: There is a gap.

BERNIE SMITH: I would say historically, for example, unions have been able to check time and wages records for employees. You go in and check that, and it's quite restricted at a Federal level compared to what it was under the State regime, but the capacity to do that meant that you could keep employers honest about what they were paying people. In many ways we need the same right to inspect algorithms and the same right to inspect apps and how they operate, and how they work towards the employee's benefit or not, so that we can confidently say to our members, "Yes, we've got the right to inspect these apps. We've got the right to inspect the algorithm. We've got people engaged who can do that, and we can see that this app doesn't track you past your workplace. We can see that this app does allocate work fairly in the way it's done."

Or, conversely, "We see that this app seems to be setting unsafe work limits because it's designed in a way that the algorithm says that once you hit this work pace, we'll then stretch you to a higher work pace, then we'll stretch you to a higher work pace again if we can." I think the capacity to properly inspect algorithms, codes and apps is a right that should be extended to all registered organisations as the next step in ensuring safe workplaces, the same as we have the rights under workplace health and safety laws.

The ACTING CHAIR: It sounds to me like there also needs to be some way of interrogating work intensity. I know in the pandemic, those who were able to work from home have described an explosion of extra working hours, either expected or not expected. They spent more time at their terminals and there's been a productivity increase. But in your industry people have had to go to work, often at risk to their personal safety. Using the Amazon example, there's been a boom in economic activity, increasing the pace of work. Do there need to be new mechanisms to enable workers to navigate their workloads and to better regulate the work intensity?

BERNIE SMITH: Yes. I think workload is the biggest psychosocial hazard in the retail, fast-food and warehousing industries. It's the single biggest issue that people have. It's not made easier by the pandemic, we acknowledge, and the workplace shortages that people have had. But even before that, workers are working to the shape—the ideal curve—that they should be able to complete tasks within, which doesn't necessarily reflect the reality. That might be all well and good as long as there are no things called customers who get in the way of the perfect curve that you might have. In a warehouse that might be all well and good as long as something doesn't fall over that gets in the way of how you might go about undertaking your path of work. I think a lot of these things are done not in real-world environments over a period of time, so I think there's a real need for us to address

a whole lot of these workload issues—these psychosocial hazards that we've seen—in appropriate ways. I think it has to take into account somebody's working life as well.

The ACTING CHAIR: In terms of the psychosocial stressors, in a previous inquiry we received evidence that the work health and safety legislation in New South Wales wasn't really fit for purpose to deal with that. The regulator said that it could deal with that through codes of practice and what have you. From your perspective, based on your industry experience, do we also need to be looking at the work health and safety regime as well as the workplace surveillance regime to provide tools for workers and management about navigating workloads?

BERNIE SMITH: Yes, I think that's a correct observation. We were involved in the establishment of the code of practice in New South Wales. One of our officials was involved in the working group to establish that. But, as they constantly came back to me to report, they would have preferred it to be a regulation, something that is actually enforceable in some way, shape or form. We're currently seeing a trial being undertaken in Victoria with one of the major retailers about the WorkWell project, which is designed to look at the whole issue of workload. I think psychosocial hazards are front and centre. But I don't think that any jurisdiction in Australia currently has sufficient coverage of psychosocial workplace hazards.

A code of practice is better than where we were, so we're pleased that we've got that rather than the complete lack of anything that we had before then, but we do believe a regulation is at least required to properly address the issue so that it gives a much greater capacity to address an issue with an employer. It means that there are consequences, and when there are consequences people are far more focused on making sure they address it. I'll be honest, people in our industries are exhausted after the pandemic. But, to be fair, they were pretty exhausted before the pandemic started as well. So there's a lot of work to be done in this space.

The ACTING CHAIR: It sounds like detailed regulations dealing with these particular problems could be made under the Work Health and Safety Act in New South Wales, if there was a will.

BERNIE SMITH: Yes, and there's a current hook—for want of a better term—within the Act about psychological injuries for people. So there's a capacity to do this but there needs to be a willingness to do this.

The ACTING CHAIR: I made the observation this morning—I think there was an article in the Telegraph on Monday from the CEO of icare talking about workplace stress claims doubling every four years, particularly increasing significantly in the last two years as a result of workplace bullying and harassment but also the intensification of work, driven by the pandemic in different ways. Is that something you're seeing in your industry also?

BERNIE SMITH: It is. I find it ironic that icare is making this observation. We've been engaged with icare for a period of time now about the whole issue of workplace customer abuse and violence. We did some very productive work with them just before the pandemic started on some training about how you address workplace customer abuse and violence. What we've seen since the pandemic has been a watering down of that training provided by icare and an abandonment of the comprehensive suite of issues that need to go with it. So it's not just training workers to be more resilient to take more abuse, it's actually meant to be about—

The ACTING CHAIR: Stopping abuse?

BERNIE SMITH: —training workers to be more resilient where you can but in an environment where the employer will have zero tolerance towards abuse, which most of our employers do. But there are also other tools and commitments in place to those workers to make sure that the abuse is rooted out of the industry rather than making people resilient to more abuse. We are engaged in ongoing discussions with icare. But I must say that I've been disappointed in recent times, and I've expressed that to them. One of the biggest issues we see in our industry in terms of workplace hazards of customer abuse—we were really excited to see that the initial training and suite of activities could reduce customer abuse by 44 per cent. That was done with Griffith University, so there's rigorous academic evidence behind that.

Then the shortening and shortening of the course that they apply and the removal of some of the other commitments required with the course mean that there's no academic rigour left to it, so we don't know whether it's effective or not. In many ways it can be damaging to employees, if they feel that they've been trained to suck it up rather than being part of a process of "these are all the things we're going to do together to make us safe in our workplaces", which, at an industry level, most major retailers have committed to us to do, but there's still a long way to go for us in implementing that.

The ACTING CHAIR: In that framework of dealing with this issue with the safety regulator, what engagement or buy-in did you have from industry employers about their obligation to prevent the abuse in the first place or to have their managerial staff act to protect workers? If someone is at a check-out and they're getting

abused by a customer, they're not in a position to do anything other than suck it up. They're really relying on someone in management or the company to deploy people to diffuse or de-escalate the situation or escort someone from the premises. Are you getting buy-in from industry employers about this?

BERNIE SMITH: Yes, we are. I would say we've got very good buy-in at the senior levels of the industry. Implementation has been hard. I acknowledge that the pandemic has made everything worse in some of these areas. But, again, one disappointment is that most of the major employers in our industry are self-insurers. They can't access the training that icare developed with us and Griffith University because they're not a client of icare. We would like that to be made available to the whole industry. The whole idea was to spread best practice throughout the whole industry.

The ACTING CHAIR: There seems to be a gap.

BERNIE SMITH: If the co-developer, Griffith University, was to go to another entity and say, "Do you want to be involved in this program?" they would have to change the program by at least, I don't know, 35 per cent or 40 per cent, otherwise they'd breach icare's copyright on it.

The ACTING CHAIR: But if icare and Griffith University were willing, it could be made available even to self-insurers.

BERNIE SMITH: There's absolutely no barrier to that.

The ACTING CHAIR: It's a question of willingness.

BERNIE SMITH: The irony was that at the beginning of this process we went to icare and said, "This is what we want to work on." They said, "Do you want a grant? We'll give you the money." We said, "We don't want the money; we just want to work together to work something out." Now at the end of the process our biggest employers can't access that even though they would've given us the money in the first place. We didn't want the money; we wanted the program.

The ACTING CHAIR: It seems like a farcical situation.

BERNIE SMITH: Hopefully we can resolve that with them. It is one thing to make public comments about stress claims, it's another thing to say, "What can we do practically together?" We're still very open to working together to get a really good outcome for our industry.

The Hon. SHAOQUETT MOSELMANE: Amazon has been the key discussion point, particularly when you referred to the severity of workplace surveillance. Is there another company that you see as less severe or as a more workable example that the SDA and organisations like that can work with?

BERNIE SMITH: Can I say almost every company? Amazon unfortunately has a reputation around the world as being very anti-union. We don't understand that. We've made approaches to the company to want to engage with them about it. We have very constructive relationships with most major employers in the industry. We've got good relationships with a lot of online retailers, including the new pure play online retailers to the industry, and we work with people cooperatively to get good outcomes. We appreciate the explosion of work that everyone faced during the pandemic, and we've worked together with most employers to come up with proper safe processes where we can, but also acknowledge that there's a long way to go with all those employers. We work cooperatively with all the major Australian retailers, whether it's Wesfarmers, Woolworths or Coles, and most major fast-food operators—not all major fast-food operators. We believe that workers have a community of interest in common with their employer largely, and lots of space where we disagree. We're always open to working with people but we want practical solutions; we don't want motherhood statements.

The ACTING CHAIR: Mr Smith, thank you very much for your evidence and for your insight into the issues that the Committee is engaging with. If Committee members have additional questions, they can be posed in writing to you and you will have 21 days to respond. I don't think you took any questions on notice, but if I'm wrong in my recollection then the Committee secretariat will be in touch with you.

(The witness withdrew.)

Mr SAM MORETON, General Manager, Policy and Analysis, Business NSW, sworn and examined

Mr LUIS IZZO, Managing Director – Sydney Workplace Relations, Australian Business Lawyers and Advisors, sworn and examined

Ms NICOLA STREET, National Manager – Workplace Relations Policy, Australian Industry Group, before the Committee via videoconference, affirmed and examined

Mr BRENT FERGUSON, Director – Major Cases, Workplace Relations Advocacy and Policy, Australian Industry Group, before the Committee via videoconference, affirmed and examined

The ACTING CHAIR: I welcome our next witnesses. I omitted to mention earlier this morning that I know Mr Sam Moreton and Mr Luis Izzo. Mr Izzo, today you are representing the Australian Business Lawyers and Advisors?

LUIS IZZO: Yes.

The ACTING CHAIR: The protocol is to enable each group appearing before us in joint sessions like this the ability to make a brief opening statement of three to five minutes. Would each of you two gentlemen who are with us in person wish to do so?

SAM MORETON: Chair, just to clarify, we are actually from the same organisation.

The ACTING CHAIR: Whichever one of you who would like to can give the opening statement.

LUIS IZZO: I am happy to. Business NSW is the State's peak business organisation. It is a not-for-profit, independent organisation promoting the interests of business, particularly in New South Wales. Australian Business Lawyers and Advisors, which is where I work, is a wholly owned subsidiary of Business NSW. We are a legal practice acting both for Business NSW members but also for businesses generally around Australia. My role here is effectively to represent Business NSW, albeit as the firm that represents it and is owned by it. I am the managing director of Sydney Workplace Relations at Australia Business Lawyers and Advisors, and Sam is the general manager of Policy and Analysis at Business NSW.

In my experience, New South Wales has one of the most advanced regulatory regimes in terms of workplace surveillance in the country. It was the first to regulate with respect to workplace surveillance, in particular, and it is really matched only recently by the Australian Capital Territory. When I say "recently", it's sometime ago now, but the ACT followed suit and developed its own workplace surveillance Act, which looks very much like a carbon copy of the New South Wales regime. As you would know, it imposes very specific requirements for three types of surveillance: camera surveillance, tracking surveillance and computer surveillance. Those provisions, in my experience, operate in very broad and general terms in that the way it defines those modes of surveillance is both broad but very simple and effective in its simplicity.

I note there was a question, I think by the Chair, to the previous representative from the SDA about new forms of technology and things like that. I think when you look at the way that the form of surveillance has been defined, it is in two lines. It is remarkably simple, and by being that simple it's actually very broad in what it captures. If anything is caught by camera, it will be camera surveillance. If anything is capable of tracking the location of a device or anything that is used, it forms tracking surveillance. Similarly, computer surveillance is not just the hardware; it encapsulates software and those things as well. I actually think the way it was drafted is quite effective.

I am aware that there have been some previous submissions put to the Committee about new modes of activity and new modes of surveillance. The vast majority of those that I have heard mentioned still fall within the notions of either camera surveillance, tracking surveillance or computer surveillance. As you would be aware, there are quite detailed notification requirements already in the Workplace Surveillance Act about people being notified of that surveillance. The other topic that I probably wanted to address in opening is one that arose particularly during the pandemic—and we heard a lot of noises about this in the industrial arena from the ACTU—which was concerns about monitoring of people at home. There was this real sense that there was going to be an encroachment on either people's personal lives or home lives by some extra reach of surveillance into their personal life.

I think there is a level of conflation and confusion around that topic. We need to be clear that, obviously, no employer has the right to go and enter anyone's home. That's a matter of trespassing if you go and start inserting things into people's homes in terms of surveillance. What we are really talking about in terms of people being worried about surveillance in their personal life is, generally, the use or the taking home of an employer's equipment into the person's home by that person and then there being some concern that that equipment might be

used in some way improperly. I think we need to be very conscious that that's probably the only realm in which we are talking about surveillance at home.

Then there are a few things that you need to think about: whether people are taking their materials home voluntarily or not, and if they are, then there is less concern; the notification requirements of the Workplace Surveillance Act—if employers are going to be using cameras or tracking equipment on their own devices, which are obviously their own property, then there has to be some form of notification about that. But when we talk about this encroachment, we are just talking about property that belongs to the employer that has been taken out of the workplace. I think it's important to bear that in mind.

The only other thing I was going to talk about briefly—because I think the Committee is now also looking at and talking about data—is, obviously, to the extent that you start to turn to data, you need to bear in mind the operation of the Privacy Act, which has quite a comprehensive regime in place with respect to dealing with data and specific prescriptions for sensitive information. That is obviously something that you're gonna be aware of, but we have a regulatory regime in place there, so it is more about analysing whether there are deficiencies in the Privacy Act itself that you think are not being addressed. They were probably the opening matters I wanted to address.

SAM MORETON: Nothing further from me, Chair.

The ACTING CHAIR: We might ask Ms Street to give the opening submission for AIG if she wishes to, and then we will swear in Mr Ferguson.

NICOLA STREET: Thank you to the Committee for the opportunity to appear this afternoon. AI Group, the Australian Industry Group, has filed a brief submission in response to this issue, and we provided a copy to the Committee yesterday and hope that has been received. We would like to make a short opening statement, drawing out some key points from that submission.

Mainly, New South Wales employers who engage in workplace surveillance generally do so because there are lawful and legitimate purposes. Many of these reasons include to comply with or manage legal obligations relating to work health and safety; employee conduct—for example, taking steps to prevent sexual harassment, including online; and employment record-keeping requirements required by the Fair Work Act and regulations. There are other reasons that may justify surveillance regarding the protection of the organisation as well as protecting other people from harm or damage.

We also consider the area of workplace surveillance to be comprehensively regulated in New South Wales for New South Wales employers, and this is done through both the Workplace Surveillance Act of New South Wales as well as the Privacy Act and associated privacy principles. The Privacy Act and APPs—the principles—also apply, importantly, to individual persons and not just employees. Employers, we maintain, should not be constrained by privacy or surveillance legislation from complying with other workplace laws such as work health and safety, anti-discrimination laws et cetera. We also consider it vital that the employee records exemption in the Federal Privacy Act is preserved to enable employers to manage compliance obligations under other laws.

This is something that we have raised concerns about with the Federal Government in its review of the Privacy Act. We are certainly concerned about any proposal to narrow or remove that exemption. In respect of automation, automation, we can clearly see, has grown with the emergence of industry 4.0 and we continue to see the expansion of digital technologies and capability. With the rise of automation, employers are increasingly requiring knowledge-based workers armed with digital literacy. We are also seeing a [inaudible] competencies and values-based behaviour in the workplace. That ends our statement, Chair. We are happy to take further questions.

The ACTING CHAIR: Amongst the evidence we have received is that particularly during the pandemic—

BRENT FERGUSON: I can't hear you, sorry.

The ACTING CHAIR: You can't hear. I will get the Committee secretariat to try to do something about that. Technology—when it works, it's great. A lot of the evidence we have received concerns work intensification, which is often enabled by technology. Although this is not new, there does seem to be a continued blurring of what has been understood as work time and family and personal time. Of course, it was great to be able to communicate by text, phone or email to deal with emergency situations, and then it became normalised.

Research has showed that in the past couple of years Australians are working six or seven weeks a year unpaid because they're checking their emails and responding to out-of-work inquiries. This has really been driven by technology, and there doesn't seem to be an accounting generally by industry for this, either in terms of making sure that people get extra pay or, perhaps more importantly, get extra rest from working. The people I've been

talking to in the public and private sectors say that they're kind of being—their work intensification is getting extreme. Is this something that you're seeing from the employers' side? What are your insights into this issue or how it can be managed?

LUIS IZZO: You can't deny that there have been a number of—both technological advances but also the pandemic, in some ways, has changed the work experience. It would be very difficult to deny that people are now responding to the odd query outside of a formal work time. I think just with the progress of time, productivity and efficiency, you do tend to see some level of intensification. I think that is quite self-evident. With the pandemic, what we've seen as well is that there has been a shift to working at different times, times that aren't the traditional hours, not only that the employer may have set but the employer may think the work is happening then and it's not. It's happening at a different time. That poses challenges and benefits.

The challenge that you've identified, Chair, is that there may be time not being captured. There are benefits that are associated with that. People are—and we're hearing this from our clients quite regularly—there's a lot to do with people with carer responsibilities that are shifting their work day, notwithstanding that there has been no formal application to do so. If you think back to pre-pandemic, in the Federal system you have got formal requests for flexible work requirements to work from home or to change your pattern. You would probably formally apply to your employer to seek approval. A lot of this is happening informally now. That is a benefit to employees, but you've identified one of the concerns.

Part of the difficulty here—and it's interesting that we're talking about surveillance—is employers themselves are having difficulty, in some senses, trying to keep track. Particularly in a professional services environment, they notionally have staff work but, particularly when they're taking the liberty of working from home, they are restructuring it to suit themselves at their discretion. The traditional mode of award regulation, both in the State system and federally, doesn't really recognise that. It considers ordinary hours to be between 7.00 and 6.00, or 7.00 and 5.00, or 8.00 and 5.00.

It's interesting that this comes up in a surveillance topic because, in some sense, employers need to have new ways of identifying what hours are being worked. If we just assume that is going to be an old-school time sheet-keeping exercise, it's probably not the most effective measure in this day and age. We should be talking about whether technology can assist with that. Equally, you're quite right, Chair, that if employers do have people burning out or not being paid under the industrial instruments for the actual hours of work, that is a challenge the employer needs to grapple with. I'm not sure if that entirely answers your question, but that is—

The ACTING CHAIR: We're getting there, Mr Izzo. My colleague Ms Houssos wishes to ask—

The Hon. COURTNEY HOUSSOS: Sorry, Mr Moreton wants to add—

SAM MORETON: Chair, I would just add that the issue of intensification is something that has cropped up right through the pandemic. Leaving aside the global firms you were speaking about earlier and some of our larger members of Business NSW, we've certainly seen owners of smaller firms or smaller sized businesses likely to take on that intensity themselves as part of the substitution environment, with a low unemployment rate and difficulty getting access to the skills they need. You see it very practically—it might be in a retail environment or in a food and beverage service environment. Those are the obvious examples. Or it might be in a hairdressing salon or something like that, where the actual owner of the business is taking on a larger share of that intensification.

The ACTING CHAIR: They're often a worker themselves in their business.

SAM MORETON: Yes.

The Hon. COURTNEY HOUSSOS: I just wanted to follow up on the point that Mr Izzo made that, often, particularly in a professional environment, it might be that that's to the workers—they're sort of taking a bit of liberty themselves to make the flexible situation work for themselves. I think there are two clear distinctions. Certainly, the evidence from our previous witnesses showed that—the key point for us is that the worker has some autonomy or some say in it. If the worker themselves decide that they are quite happy to work until seven o'clock if they can go and pick up their kids at three o'clock in the afternoon—I can count myself in that particular pool of workers—it is a very different situation to if they're being tracked on an app that they're required to have on their phone in order to sign in to do the work once they actually leave the premises of work. Would you accept that there is a difference in those two conversations—the autonomy and the negotiating power, on behalf of the worker, that they have in that first conversation is different to the one in the second conversation?

LUIS IZZO: The first part is yes. What we are not seeing is workers being forced to change their pattern of work or forced to work from home, those types of things, except for in the health emergencies that we went through. That is generally being done at their discretion. In terms of your question about being tracked on an app

without a choice in the matter, again, I think we are probably talking about a scenario where any tracking is being done, in the vast majority of circumstances, on a device provided for by the employer. In some scenarios, I am aware that some more sophisticated businesses are using time and attendance software to provide the employer with the option of downloading an app to more easily check into a location. Often that is actually arriving at a physical worksite. I have seen that, particularly in the large-scale hospitality and services sector. It might be that to check in and start your day, you check in through an app, but it's actually in attending a physical location.

What I'm not seeing much of—I could be proven wrong—is people having to log in to an app at home or do anything like that. It is usually when they attend the worksite, and the businesses using that are big users of casual staff, things like that. It could be a large heavy industry or mine site or something like that, or it could be a hospitality or large catering industry supplier or something like that. But, generally, that's at the workplace. It's not at their home. I think that needs to borne in mind. So it is not necessarily, again, this concern of someone reaching into finding out where they are, where they shop and those types of things. I don't see that being the reach of this technology or its usage, at this stage.

The Hon. COURTNEY HOUSSOS: You don't have an issue then if that was outlawed? The surveillance or the ability to log in to an app, I think you make a point that this is where technology can enable workers. We're just concerned about some of those consequences coming. There would be no need, really, from an employer's perspective, to be collecting that data outside of the workplace.

LUIS IZZO: As in, where the person is located?

The ACTING CHAIR: Sorry to interrupt, but a good example we were given is, say, in the gig economy, or possibly even Amazon was one example, where you log on when you get to work and, obviously, the tracking has to occur while you're working, but the phone might be in your pocket. The question is when you then leave the workplace for the day, or for the shift, are you still being monitored? The answer is we don't seem to know, because as far as we know the workers weren't asked to agree or not agree to—you know how some apps ask you whether you should be tracked only when using the app or generally? We haven't had any evidence about whether that kind of prompt occurs and so we just don't know whether people are being monitored even when they're not at work as to where they are or what they're doing. It's simply that we don't know what's happening with the data information. In the case of Amazon, it's happening in Seattle. The information is being gathered here in Australia but pored through in another jurisdiction, although the recording is happening here. We seem to have a lack of visibility of what's going on.

LUIS IZZO: From our perspective and the clients we're speaking to, they have no desire—the businesses we talk to—to track someone outside of their work. I have not met—I deal with clients every day and business chamber movements every day. No-one has expressed a desire to do that. Most apps—just from my own personal knowledge—generally, once you log out or once you sign out, or there is some process, then the functionality will generally cease. I take your point, Chair, that some allow ongoing tracking, but that is generally in the control of the user of the phone. So provided the employee has the ability to ensure that the tracking ceases then I'm not personally aware of a scenario where business would require the need to track outside, nor have I come across businesses that want to do so. As long as, though, the technology they're using is capable of being enacted during work hours. That's where they need it.

Ms ABIGAIL BOYD: Coming off the back of that, employers may not be wanting to track their employees, but what assurance does an employee have that the software vendor isn't tracking the employee in order to—as we've heard in previous panels—improve their future software and/or sell that data off to a third party? If the employee doesn't have that relationship with the software vendor, they're not part of the licensing agreement and presumably they don't know if they're being tracked outside of their work hours.

LUIS IZZO: I think the response to that depends on the device. So you're either going to have a device provided by the employer, in which case you don't need the hard device on you—now in most circumstances I don't think that's what you're talking about. I think you're probably going to look more at a scenario where the person is using their own personal device, potentially, to log in to an app or software. In that circumstance, it will depend on the app and the provider. I mean, I'm aware from my own usage of, say, an Apple iPhone that you have a control in the settings to be able to allow apps to—what they can and can't do. So I would assume that employees have that control still today to turn off the tracking should they wish—just because of my own use of my own personal phone. I think this concern that you raise is at large. It's about any app you download, whether it's an app to do with the weather, whether it's an app to do with any particular—I mean, I've got 20 or 30 apps on my phone and the same dilemma would arise with all of them.

Ms ABIGAIL BOYD: We are talking about where the relationship between the software vendor and the user is interrupted by a third party, in this case, the employer. For instance, I used to work at a global law firm—and even here in Parliament I access work programs through my phone through a portal. I don't necessarily

have any kind of direct access over the software I'm using, because it's all through a portal that the employer or the organisation has control over. I think that's more and more common. So we don't have any assurance, do we, that an employee doesn't have software on their phone or that they are accessing through their phone that the employer has agreed the software vendor can take data from and use it?

LUIS IZZO: This is a reason I think we need to be careful here, because we're not just talking about phones in terms of software. Employees will—just bringing it back to a physical workplace—attend for work, log on to work systems and they will input all sorts of data to those work systems. They might be Salesforce-type systems, they might be all sorts of different programs and there are all sorts of data going everywhere in that scenario. So I think this issue is, in some instances, bigger than just what goes into a phone. So that's why I think some care needs to be exercised here because—

Ms ABIGAIL BOYD: But we are talking about—sorry, just to bring it back—the phone. Even when you're given a phone from your employer the assumption is that you will carry that phone on you at all times, in a whole bunch of different types of jobs and professions. It's not like you get given a phone that you just use when you're in the office. I don't think that's a very common scenario.

LUIS IZZO: No. If the concern is tracking, I understand the focus on the phone. But if the concern is broader than tracking—and this is why I think we need to have care, because we're all putting all sorts of data into our systems of work the whole time and there's a business need, in some senses, to have people work efficiently and to put that stuff in so then it can be used for whatever it is that the undertaking is. But if it's about tracking and that is someone's location, which is part of what's unique to a phone because it's on your body and so it follows you, then I can understand there being a sensitivity about tracking data—which is, in fact, already regulated by the Workplace Surveillance Act. But if it's about what you're entering generally, that's a much bigger discussion.

Ms ABIGAIL BOYD: It's kind of both, though, isn't it? I understand that there are those two different aspects, but if you are a software vendor then you are pretty keen on getting both of those bits of information—whether it's tracking if you are using software through your phone, whereas the more hard data about the way you're working is relevant to whatever device you're using at the time. I'm interested in drilling down into the assumption that it is the employer that's the one that's trying to get the benefit of the surveillance the whole time or getting the benefit of the data, when we don't have any real assurance that the tech company themselves aren't the ones that are gathering that data and using it.

LUIS IZZO: The thing that still concerns me is that when we are talking about data, the vast majority of data that you're inputting for work purposes is work data. For instance, if I'm asked to provide an advice for a client I'm typing in all of this stuff about a legal problem, or I'm typing into a client relationship management system the communications we've had—all these things. This is all information you're preparing for your owner, for your employer, for your business. So it's not really my personal data; it's data belonging to the business that I work for.

Ms ABIGAIL BOYD: If you are going onto a browser at lunchtime and shopping, are you saying that—

LUIS IZZO: No, that is very different. So that then—what I would be doing, though, is using my employer's equipment for my own personal purposes. So that's the thing, there's an element of discretion and choice there, because what the employer is doing—and it may be monitored under the Workplace Surveillance Act, whether it's the use of a news website, whether it's the use of a website for shopping or whether it's a gambling website. If I decide to do things for personal purposes then there is the possibility that the employer is made aware of that, but also there's no need for me to necessarily use that.

Ms ABIGAIL BOYD: Again, I'm not interested in the employer at this point; I'm interested in the vendor.

The ACTING CHAIR: I guess this is the question that's come out in the evidence. The employee uses the software and the equipment for their work purposes, but the issue is the data that is derived—not just the work inputs but how long it takes people to perform the task, all sorts of metrics about the performance of the work. Yes, the employer is gathering those and maybe monetising it—you know, using it to drive productivity, workplace re-engineering—in a way that the employees are not necessarily aware of and are not getting a slice of in terms of improved pay. The second issue, which Ms Boyd has raised, is: Is it the software company that is also deriving this data and using that to drive its own business models in terms of preparing its own emails? For example, I gave a paper not unrelated to this last year and I actually found a number of software companies selling software that extolled the virtues of cutting-edge employee management data tracking and productivity improvement tracking. It was quite clear that they got the information from the employer as well. So, again, you are doing the work as a worker. It is one thing for your employer to get it, but some company is then also getting it and getting the value of your work, but you are not getting a return on that as the worker.

LUIS IZZO: Under the Privacy Act, as you would be aware, there are very strict provisions about what happens with data except for employee records, but the employee records exemption only applies where it is directly related to the employment. That is the protection that you would see operating there, which is that if it is not directly related to the person's employment—that is, the data is not being collected and used for purposes directly related to the employment—the employer would actually need to go through all of the Privacy Act requirements. That will probably be the protection there.

The ACTING CHAIR: I guess the question is, are they? But I think the Australian Industry Group had a contribution they wished to make. Ms Street?

NICOLA STREET: [Inaudible.]

The ACTING CHAIR: You are on mute, Ms Street.

NICOLA STREET: Apologies, Chair. Thank you for that. We had a similar point with respect to the application of the privacy principles here and the probably limited role of the employee records exemption would apply with third-party vendors collecting worker data in that capacity and the range of privacy protections and obligations that would apply in those circumstances. The other point we wanted to make too is that the Workplace Surveillance Act itself also prevents the tracking of employees if they are not at work. We have identified the relevant section in our submission in general terms. We are aware that it is obviously an issue that we need to monitor and be aware of, but our view is that we have quite a complex, comprehensive framework with both the State Act and the Privacy Act, and that Act is actually under review federally as well. Our view is that we think there are practices occurring that are not going through or complying with the privacy principles, and that would be an issue for compliance with the current Federal law.

The ACTING CHAIR: On that point, I have had a brief look at the Workplace Surveillance Act, and while I do not have the Federal Privacy Act open, in neither of those two pieces of legislation is there a capacity for whether it is a worker or even just a consumer of an app who is a client whose data is being collected by a business—there is no capacity in either piece of legislation for them to be made aware of exactly what information is being gathered and then, more importantly, how it is being deployed by whoever has collated that data.

Thirdly, again there is no function for them to perhaps say no to some uses of that technology or that information that they themselves have generated either by working or by being a customer. Fourthly, there is no mechanism or capacity for them to share in any benefit derived from or monetised from that information. It sounds like the legislation is there, it may cover these activities, but there are some missing pieces for, on the one part, a worker who is working in an enterprise, but also even just generally, in privacy law, for customers whose privacy is being collected and turned to financial advantage—and, again, it is often without their knowledge. Would you agree that there seem to be some gaps in the legislative framework?

SAM MORETON: Chair, one thing that comes to mind, for everyone in the room who partook a year ago in the long lockdown and homeschooling, these are issues that transcend the workplace.

The ACTING CHAIR: Yes. So this is a societal problem?

SAM MORETON: Well, the idea of capturing data that can be monetised is a much bigger issue than the particular framework we are looking at today. For anyone who has worked in the public sector environment, in a high-security environment there are even more logging requirements. You know, pretty much every time you open an email in a Commonwealth context you would be logging in and providing that kind of data. You might be doing it on a train and giving away the location of where you are doing that work. These are important issues. They open up a much larger scope of discussion than the State surveillance—

The ACTING CHAIR: I think that is right, but certainly I think the surveillance of how and the way in which workers perform their work and how they might be observed by their employer is certainly part of a much bigger set of issues. Nevertheless, they are pretty important.

LUIS IZZO: Just on one of the comments you made, Chair. You posed a series of questions about "Am I aware it is being collected and what it is being used for?"—those types of things. If we move out of the employment context for one moment, the privacy principles are quite strict. You have to tell people why their information is being collected, they need to be aware of what the intended use is, who it is going to be disclosed to and they need to consent. There is an exemption for employee records, but only if the use of this information is directly related to the employment relationship.

To answer your last question—is there a provision about sharing the benefit?—no, there is not. But in terms of the first two or three of your questions, it is highly regulated by Australian Privacy Principles Nos 3, 4 and 5. There is what we say is an important carve out for employee records because it enables the employer to move with some level of alacrity, for want of a better word, about dealing with things whether it is super payments,

transferring money to clearing houses or to the ATO et cetera. But the employer can only have that breadth or that freedom if it is directly related to the purposes of the employment. If it is not, then they need to go through all of the Privacy Act hoops as well. That is what I was just going to say in response.

The Hon. SHAOQUETT MOSELMANE: Mr Izzo, earlier on you mentioned something about if the property is owned by a company then there seems to be a potential attached right to surveillance or tracking. Is that the implication of the property attached to rights? Is that what you were saying?

LUIS IZZO: I think the effect of the Workplace Surveillance Act is that if you have employer property and you comply with the notification obligations that exist and that are attached to that property then, yes, you have the right under the current regime to engage in camera surveillance, tracking surveillance or computer surveillance.

The Hon. SHAOQUETT MOSELMANE: In respect of what time? Whether your work is from nine to five or?

LUIS IZZO: If it is the employer's property, that is the present State of the law, correct.

The Hon. SHAOQUETT MOSELMANE: So it attaches to—

LUIS IZZO: To its property, provided they have notified the employee, though, of the matters. And there are quite a range of them that you need to notify. So an employee would be well aware of what it is being used for. But yes, the employer then has that right under the current regime.

Ms ABIGAIL BOYD: I think both Ms Street and you as well, Mr Izzo, said at the beginning—I think Ms Street's comments were that this area is comprehensively regulated in New South Wales. I think I get from your comments as well that you believe that the regulation in New South Wales is pretty much sufficient. The laws here have not been updated in any substantial way for some time and we know—and I am sure you know—from other areas of the law that, as technology has moved so fast, the law has lagged behind and has been in need of updating. Given everything that has happened with the way people are working, particularly over the last two years, how can you say that there is no need to update our laws at this point?

LUIS IZZO: I am happy to go and then I will hand over to Ms Street. The reason I hold that view, particularly in this Act, is that the very definitions of "tracking", "camera" and "computer surveillance" in the Act are two lines—each of them. When you look at them, they are so broad. The fact that they are not specific is what has actually enabled them to continue to capture the new ways of working. So if you had been more specific initially, you may find that the Act would not still have the breadth of coverage that it does. But because of their sheer simplicity I am yet to understand a form of surveillance that is not captured by those three categories.

Ms ABIGAIL BOYD: I'll come to Ms Street in a minute because I'm interested to hear her views as well. But, obviously, there is the letter of the law, and then there is the way that the law operates and takes effect more broadly. As circumstances change, the law doesn't always have the impact that it used to have. It doesn't matter how broadly it is defined if power balances, for example, are changing. If, for example, we were to insert a new provision that allowed employees to install software that told them what was being monitored—that sounds like something that is not covered at the moment under the law but perhaps would be a fair response to the concerns over the last two years over the relative employee imbalance. I just put that out as an example for why we might want to be amending the laws. Do you take that point? Do you think there would be any problem with employees being able to proactively monitor their employers' compliance with the laws?

LUIS IZZO: I think the difficulty with that is you would presumably be installing that on the employers' property. The employers can install whatever they want on their personal devices. Really, to install this kind of software to find out what monitoring is going on, you're talking about putting that onto the employer's own equipment. It would be unusual for an employee to have a right to start modifying equipment that doesn't belong to them—that belongs to an employer, that's been optimised in a particular way. And then you'd need to have an understanding of what that's doing and what data that's collecting. You have the same concerns then about what happens with this data the software's collecting, Where's that going?

Certainly, I don't think employees are going to be in a position to comply with Privacy Act type obligations to notify their employer, "Well, here's Australian Privacy Principle compliance 2, 3, 4, 5." They're not going to have the sophistication. Particularly if the concern is employers aren't complying, I don't see how employees are going to be able to give the level of satisfaction that, "I'm going to install this on your device and monitor your monitoring of me, and I can assure you that no improper use of this data will be made." I think there would be some concerns around that, for that reason.

Ms ABIGAIL BOYD: I want to ask about the idea that all these devices are owned by the employer, whereas we know that it is an increasing trend that these devices are owned by employees, with software installed by their employer on their device. Would that make a difference?

LUIS IZZO: I think if an employee installs software on their own phone to find out when they are being tracked, I think they have that right, now, and I wouldn't seek to take that away from them. It's their personal device. If the employer is going to take the risk of saying, "I'm going to have some of my work done on someone's personal device", the employee, I think, does and should have the ability to monitor what tracking or monitoring is being done on their own personal devices. Absolutely.

The Hon. LOU AMATO: Mr Izzo—and open to anybody else—there have been some concerns raised to me, particularly by parents. Some employers may be looking into their employees', or potential employees', social media—particularly Facebook. By doing so, it could be jeopardising their job positions or prospects of employment or prospects of promotion. Are you aware of this occurring, or is there anything in place to stop that occurring? Particularly for young people—we have all been young. Fortunately, I came from a generation where we didn't have to worry about this. But they do post things on there. I know, with my own children, I've told them, "Don't post anything stupid on there", because I believe that could very well be occurring.

LUIS IZZO: There is no doubt that when people post things publicly—so on Facebook, Twitter, wherever it is—employers do, particularly in the job recruitment part of business, look at what people post publicly. I don't think there's anything improper, unlawful or unethical about that. Someone has decided, voluntarily, to put something out in the public space. There is a public record of it. The employer can monitor that. If the employee wants their Facebook page to be private, they can do that through Facebook. None of that is of concern to me. I don't think there's anything unethical about that. It's information in the public domain. It's no different to googling someone.

I think the difference is if the employer is using data to somehow nefariously, illegally and fraudulently log in to that person's Facebook account and then see the inner workings of that person's personal account. I suspect that's probably illegal. Even if it's not, it would breach a whole range of privacy principles, I suspect. It wouldn't be directly related to the employment. You'd have all sorts of noncompliance, at least with the Privacy Act, but I suspect otherwise, because you're fraudulently purporting to be someone else. So that is illegal. I'm not aware of that being done by our clients or members. But I am aware of them looking at stuff in the public space, absolutely, and I don't see that as being a problem. I think that's more a societal issue of children and young adults being informed they need to be really careful of what they put online. Again, I'm not sure if Ms Street wanted to respond.

NICOLA STREET: I just want to make sure I understood that question from the Committee regarding Facebook usage, whether that was from prospective employees or others in the community and whether there was some concern about the reputational damage.

The Hon. LOU AMATO: It plays into people going for employment or people going for the prospect of an advancement in their current position. Some employers may be looking at what their employees are doing, in order to maybe move them on from their position or give them a promotion or not give them a promotion. Parents of young people have approached me—over the last couple of years, particularly—going, "Look, I'm a bit worried, particularly about what my son or daughter are doing. If their boss is looking into it, it may jeopardise their future positions."

NICOLA STREET: It's not something that we see lot of, at all. I think, to do that, would be a fairly time-consuming activity—to be monitoring the social media accounts of prospective employees or current employees. I also think if that information was relied upon that was not relevant to the employees' job, that's something that may be addressed through protections like the unfair dismissal regime, for example, if that was enlivened. There have been cases in the commission that concern employee conduct outside of hours that have poorly reflected on the reputation of the employer, where there's been that connection. That's not necessarily been a bar to meet for an employer who wants to rely on that information. But, as a general practice, it's not something that we consider to be widespread at all.

The Hon. SHAYNE MALLARD: I'm interested in the issue of multinational corporations that operate in Australia and have different policies in their home country like the United States, for example. Are there loopholes in our legislation, the privacy and anti-surveillance regulations, with respect to using technology for surveillance on Australian employees by external corporations, like multinational companies? I don't want to name a company, but they have some different policies and frameworks for monitoring staff behaviour in some global multinationals.

LUIS IZZO: And then that gets applied in Australia, in breach of—

The Hon. SHAYNE MALLARD: So, let's say XYZ company has policies that monitor staff and they have passed that down through their subsidiaries. Can that cause a problem with our—

LUIS IZZO: In my experience the answer is no for two reasons. When you are talking about multinational companies that are big enough that they have an Australian presence, they tend to have, in most cases, localised management—so, talk about localised HR; localised legal, potentially; localised CEO, certainly. What they soon learn—particularly if we're talking about America, if you put privacy aside for one moment—is that there are a whole heap of laws in Australia they don't know exist that are more onerous than overseas they need to quickly get across. Employment regulation is a great example. What is an award? What is all this stuff about people being able to take leave? Unfair dismissal—unheard of. So, quickly, they need to have a local presence that ensures that their activities, which would ordinarily not be compliant, become compliant. Even our neighbour as close as New Zealand—they don't have penalty rates. They don't have awards. Our regulatory system of employment is very complicated, so they need to arm up.

I think that is the cause of the upskilling. Then what happens is, if you do have a scenario like privacy, for instance, because you have a localised HR management, ER management, whatever it is, that are already applying an Australian regulatory lens, they tend to do that for everything. So if there was something that was not permitted, that would get caught at the local level because it is not just a privacy issue; it's an everything issue. So I don't think that's a problem. It has really worked more the other way around, in my experience with multinationals. It's the European ones. Europe has a very particular privacy regime and often it can be a little bit difficult with those companies sometimes. They have global policies that make it a little bit more difficult to access information quickly. But I haven't seen that problem, no.

The Hon. SHAYNE MALLARD: Conversely, I am aware of banks operating in the Pacific. The regulatory regime there is a lot more relaxed than it is here and management who go there from here have to adjust to that too, and it becomes a cultural problem for the owner in regards to banks and privacy because we are much more strict here, and they're not so strict over there.

LUIS IZZO: Yes.

SAM MORETON: Chair, just earlier some comments, I think, relate to that regarding—without naming firms, we were talking about investment banking, it might be, or dress circle law firms and the culture of expecting that someone takes a work device that I think was described as 24/7.

The ACTING CHAIR: Yes.

SAM MORETON: There's nothing to stop someone with their tool of trade leaving it home, to the honourable member's question earlier, and I think people need to understand that in the Australian and New South Wales environment, that is where they are domiciled. They are the basic standard rules that we are seeking to set, enforce and follow up. It may be a different environment if you are an aspiring partner in a dress circle firm with the expectation of the course of dealings that they have, but they are not broad societal norms. I think it is really important to not make that assumption or extrapolate that top-down approach that we are talking about here. I'm conscious of time but, from our perspective in Business NSW, this is very much about engaging on practical steps: what this means for mid-size firms and larger firms, what it means for family-owned businesses, and where we draw the line and, for example, work with SafeWork to have guidelines that help educate business owners on what their obligations are in this space at that very practical level.

Ms ABIGAIL BOYD: Just on that, I think—and we talked about this before—this inquiry and the idea of surveillance is clearly referring to a bunch of very different workplaces and very different workers within those workplaces. Again coming back to what your rights are under law versus how easily you can enforce those rights, if you are what I'd term a baby lawyer, for instance, going into one of those law firms as a graduate, you are not getting a massive salary, although you are definitely on the more privileged side of society. Saying, "I know it is my option to keep my device at work but I'm not going to do that," clearly would be career-limiting. I think that is where we have the problem: There are the laws and then there is the application of the laws, and the application is obviously impacted by a power imbalance. So what would you do, or what could you suggest, in terms of how we might adapt the laws or change the laws now to try to restore that power imbalance?

SAM MORETON: Obviously, through the Chair, not everyone has the means to separate work and private life through their devices, but in that particular context, certainly advising young members of my own family, having your work devices as work devices and having your other devices as your own and personal is certainly the sort of step that someone in that environment would well be able to do. It is a different environment if you are a truckie with surveillance equipment in the cabin of your truck, obviously.

The ACTING CHAIR: Just getting back to a point that Mr Izzo made earlier, when you look at the workplace surveillance legislation, there is the requirement to notify—

SAM MORETON: Yes.

The ACTING CHAIR: —but there's not really an approval process and there is no capacity for those who are being notified to resist or to argue the toss about "Is this surveillance necessary? Is it reasonable? Is it intrusive? If there is a legitimate issue to be addressed, is this the right mechanism, or is there another mechanism?" There just seems to be a bit of the puzzle that's missing.

LUIS IZZO: Primarily because what's being surveilled—and the point I think I have made—is the employer's equipment or their worksite, and that's why there is inherent, I think, in the Act this notion that the employer can surveil in that environment.

The ACTING CHAIR: That is the thrust of it.

LUIS IZZO: That's right. I mean, interestingly—

The ACTING CHAIR: The question is whether those lines need to be redrawn.

LUIS IZZO: Well, that is probably the question the Committee is looking at. Interestingly, before this Act came in, this type of notion was not regulated anywhere in Australia.

The ACTING CHAIR: I am painfully aware of that.

LUIS IZZO: There are listening devices Acts across the various jurisdictions, but this notion of workplace surveillance—New South Wales kind of led the charge and the ACT followed with very similar legislation. But they echoed your legislation and I think they have brought out into the open and appropriately dealt with it. But, obviously, that is the issue we keep running around.

The ACTING CHAIR: I thank the witnesses—those in person and those online—for sharing their time and, more importantly, their insights into these complex and challenging issues that we will have to wrestle with. Members may have additional questions for you, which they can put on notice and you will be notified. You will have 21 days to respond. I do not think you took any questions on notice, but if you did, again, you will be informed and given 21 days to respond also. Thank you very much.

(The witnesses withdrew.)

The Committee adjourned at 14:56.