Submission No 3

INQUIRY INTO IMPACT OF TECHNOLOGICAL AND OTHER CHANGE ON THE FUTURE OF WORK AND WORKERS IN NEW SOUTH WALES

Organisation: The Australia Institute's Centre for Responsible Technology

Date Received: 26 August 2020

The Australia Institute
Research that matters.
Centre for Responsible Technology

Workplace surveillance

Submission to the Select Committee on the Impact of Technological Change on the Future of Work

Peter Lewis
Director, Centre for Responsible Technology

August 2020

About The Australia Institute

The Australia Institute is an independent public policy think tank based in Canberra. It is funded by donations from philanthropic trusts and individuals and commissioned research. We barrack for ideas, not political parties or candidates. Since its launch in 1994, the Institute has carried out highly influential research on a broad range of economic, social and environmental issues.

About the Centre for Responsible Technology

The Australia Institute established the Centre for Responsible Technology to give people greater influence over the way technology is rapidly changing our world. The Centre will collaborate with academics, activists, civil society and business to shape policy and practice around network technology by raising public awareness about the broader impacts and implications of data-driven change and advocating policies that promote the common good.

Our philosophy

As we begin the 21st century, new dilemmas confront our society and our planet. Unprecedented levels of consumption co-exist with extreme poverty. Through new technology we are more connected than we have ever been, yet civic engagement is declining. Environmental neglect continues despite heightened ecological awareness. A better balance is urgently needed.

The Australia Institute's directors, staff and supporters represent a broad range of views and priorities. What unites us is a belief that through a combination of research and creativity we can promote new solutions and ways of thinking.

Our purpose – 'Research that matters'

The Institute publishes research that contributes to a more just, sustainable and peaceful society. Our goal is to gather, interpret and communicate evidence in order to both diagnose the problems we face and propose new solutions to tackle them.

The Institute is wholly independent and not affiliated with any other organisation. Donations to its Research Fund are tax deductible for the donor. Anyone wishing to donate can do so via the website at https://www.tai.org.au or by calling the Institute on 02 6130 0530. Our secure and user-friendly website allows donors to make either one-off or regular monthly donations and we encourage everyone who can to donate in this way as it assists our research in the most significant manner.

Level 1, Endeavour House, 1 Franklin St
Canberra, ACT 2601
Tel: (02) 61300530
Email: mail@tai.org.au
Website: www.tai.org.au
ISSN: 1836-9014

Introduction

The NSW Select Committee on the impact of technological and other change on the future of work and workers in New South Wales terms of reference are wide-ranging and comprehensive. Their findings will hopefully provide a structure for long-term thinking on these issues and serve as an opportunity to develop model legislation that could be taken up in other jurisdictions as well as NSW.

This submission canvases the implications of workplace monitoring and surveillance, specifically four sections of the committee's terms of reference:

> (h) Whether current laws and workplace protections are fit for purpose in the 21st century, including workplace surveillance laws and provisions dealing with workplace change obligations and consequences,
>
> (i) Whether workers should have agency over the way the data they generate at work is used and, if so, what legal framework is required to provide this,
>
> (j) How employers and other businesses should manage and use the information generated by the workforce,
>
> (k) How government as a best practice employer should manage and use the information generated by its workforce

Most Australians are subject to electronic monitoring, with 70% of those currently in work saying that their workplaces use one or more methods of electronic or digital surveillance. Another 10% do not know if their workplaces use surveillance. Most workers agree that workers should be notified when any form of surveillance is being used, that there should be legal restrictions on using these technologies, that these technologies reduce trust between workers and employers and that electronic surveillance reduces the quality or pleasure of work. Most disagree that these technologies make people work harder.[1]

For further reading on some of these issues, see *Under the Employer's Eye: Electronic Monitoring & Surveillance in Australian Workplaces*. This report, by the Australia Institute's Centre for Future Work, details the main forms of modern electronic monitoring and their consequences and reports original polling research into the prevalence and perception of electronic monitoring in the workforce.[2]

---

[1] Henderson, Swann, & Stanford (2018) *Under the Employer's Eye*, pp. 5–6, https://www.tai.org.au/content/under-employers-eye-electronic-monitoring-surveillance-australian-workplaces

[2] Henderson et al. (2018) *Under the Employer's Eye*

Problems raised by technological change in the workplace

Technology has created new methods to monitor workers, from wearable GPS devices, to RFID chips in ID tags, to real-time monitoring of computer inputs, to Internet of Things (IoT) applications like movement and voice monitoring.

The constant monitoring and measuring of work are applications of "surveillance capitalism". The concept of surveillance capitalism was introduced and developed by American scholar Shoshana Zuboff. It describes the commodification of personal information, captured and produced by surveilling digital activity, especially on the internet.

In workplaces this data can be, and is, used to:

- increase work intensification (the greater effort required from workers during work hours),
- observe and control worker to worker interactions,
- tighten management control,
- shift risk to workers,
- predict future behaviour,
- on-sell to data brokers and management companies (value extraction), and
- drive human redundancy through job replacement and automation.

In all these cases, the benefit and control of this technology lies in the hands of the employer with workers merely an input into the value chain.

This will intensify as more companies seek to accumulate workplace-generated data for use in conjunction with Artificial Intelligence (AI) – machines that purportedly make "humanlike" decisions.

One striking change observed in surveillance capitalism not present in earlier forms of capitalism is the commodification of data, not merely the use of data. This concept, called "behavioural surplus", describes the use of behavioural data as a generator of revenue in itself, rather than simply to deliver a service or improve the quality of the service delivered.[3]

[3] For more on these ideas, see Holloway (2019) *Explainer: what is surveillance capitalism and how does it shape our economy?*, http://theconversation.com/explainer-what-is-surveillance-capitalism-and-how-does-it-shape-our-economy-119158; Zuboff (2019) *The Age of Surveillance Capitalism*, https://www.allenandunwin.com/browse/books/general-books/popular-science/The-Age-of-Surveillance-Capitalism-Shoshana-Zuboff-9781781256848; (2019) *The threat of surveillance capitalism, and the fight for a human future*, https://www.abc.net.au/religion/shoshana-zuboff-threat-of-surveillance-capitalism/11433716

The legal framework around workplace surveillance has not kept pace with technology; what legal provisions exist focus on privacy and consent principles.

Changes in work practice around the pandemic have only accelerated workplace monitoring – with increased remote safety and performance monitoring in external workplaces and increased oversight for home working. Many of these changes will persist, especially as employers find ways to put the new forms of data being generated to use: for health monitoring, social distancing monitoring and location tracking, for example.

Without a legislative/regulatory intervention, the trends will intensify and workers will be subject to even greater levels of monitoring and surveillance as a core element of the employment relationship.

Where are these new forms of monitoring being applied?

In short, everywhere. The market for technology that observes, captures and repurposes behavioural surplus is fast-moving and self-perpetuating.

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.

Current applications include:

- **App-based services** – From Uber to Deliveroo, the gig economy is built on data collection. Applications include GPS tracking of workers, customer ratings to determine work allocation and intense measurement of time to complete tasks.
- **Caring professions** – The development of app-style placement services for disability and home care workers create a model for intense "Fordist" monitoring of work outputs with focus on function over care.
- **Logistics and long-haul transport** – Amazon is pioneering surveillance in its warehouses globally with "smart wristbands" monitoring every body movement. Delivery workers and other offsite workers are subjected to similar tracking. This can be carried out in the name of health and safety but can lead to intense work design and automation.
- **Public transport** – Humans are being removed from the transport system. Video monitoring of trains to central base has replaced the need for guards, while a new fleet of driverless trains has been introduced. New trains are also incorporating "always on" audio-visual monitoring of drivers. For now, drivers are overseeing the operations, but their input will be captured with a view to long term human redundancy and the rollout of "driverless trains".
- **Mining** – Remote locations are already well-developed in the use of automated trucks and driverless trains controlled from a central point. More mining operations are becoming fully automated, with very few workers required.
- **Education** – Marking of student exams is becoming standardised for computer marking with a shift from discursive writing to multiple choice and tightly structured "PEEL" responses.[4] The real marking of teachers is captured and then replicated for automation, taking human oversight out of the evaluation process. Universities

[4] PEEL stands for "Point, Evidence, Explanation, Link", and describes a structured form of writing paragraphs in essays.

require lectures to be filmed, allowing them to be packaged and transmitted elsewhere.

- **Rural and seasonal work** – Not all surveillance is digital; employers exercise power over and monitoring of seasonal and visa workers through the control of their passports and visas.
- **White collar work** – White collar workers experience increasingly intrusive performance tracking and requirements to self-monitor. Cloud-based management systems, for example the SureView platform, report in real-time on keystrokes, mouse movements, document access and website traffic, and take invasive screen shots and webcam photos.
- **Working from home** – The pandemic and shift to home work has only intensified monitoring trends. The use of technology by employers to control workers will only intensify as more workers work from home. Examples include:
    - Auto-tracking of work functions
    - New “value extraction” techniques, including the gamification of workflows
    - Offloading of workplace responsibilities from employer to employee, for example workplace health and safety and workplace liability
    - Multi-shifting (providing care inside the home while working inside the home)
    - Function creep, for example well-being data used to more intensely monitor performance.

Issues arising from increased monitoring

There are a series of broader and interlocking issues about the future of work and the employment relationship.

Information and power

A new form of inequality and power imbalance is created when only employers have access to the information they use for deciding how workers are hired, evaluated and managed. Without access to this information, workers and their representatives have no ways of understanding and, if necessary, challenging employer decisions. This leads to a reduction in transparency and bargaining power.

There are also power imbalances present in terms of who *creates* the information used to decide how workers are hired, evaluated and managed. For example, ride-share drivers who will only receive work as long as their customer satisfaction rating stays above a particular level are put in a subservient position to customers who may be harassing or abusive.[5] Additionally there is a new imbalance with respect to data driven decision-making. In many cases predictions and determinations made by automated systems are not transparent and non-reverse-engineerable, which makes it harder to hold them accountable.

Data can be a powerful force for good in the right hands, which is why the asymmetry between the information that companies accumulate and the information that they reveal is so dangerous.

Google employees created a spreadsheet to share their salaries with one another, revealing that men receive more money than women at the same level in five of the company's six pay levels. Erica Baker, one of the spreadsheet's originators, was denied "peer bonuses" for creating the spreadsheet by her manager; being denied a peer bonus was something otherwise almost unheard of at the company.[6]

---

[5] Henderson et al. (2018) *Under the Employer's Eye*, pp. 14–15

[6] A "peer bonus" is an on-the-spot $150 bonus a Google employee can award a colleague. The pay gap identified in 2015 remained in 2017, well after Erica Baker had left the company. Google protests that the spreadsheet, which at the time had 1,200 entries, is "an extremely small sample size, and doesn't include location, role, tenure or performance" and that, "like-for-like", women are paid 99.7% what men are paid. Nisen (2015) *There's reportedly a big, secret spreadsheet where Google employees share their salaries*, https://qz.com/458615/theres-reportedly-a-big-secret-spreadsheet-where-google-employees-share-their-salaries/; Buxton (2017) *A Google Employee Spreadsheet Shows Pay Disparities Between Men & Women*,

Likewise, YouTube's "demonetisation" rules, algorithm and communication (which determine whether content creators are compensated for their work) have been described as "confusing and opaque", "random", discriminatory against LGBTIQ content, "will screw things up", "unclear", "a black box", "constantly changing", implemented without notification and "murky".[7] Business Insider uses the analogy that demonetisation is "like you've been fired from your job";[8] yet it is unlikely a workplace could dismiss someone using an algorithm as opaque and arbitrary as YouTube's demonetisation algorithm.

Companies, like Google, that have made data collection central to their business model are hypocritically reluctant to reveal information on themselves. That illustrates that their interest is in what information can do for them, not in the principles of transparency, greater knowledge or informed decision making.

Accuracy and bias

Inferential monitoring based on vocal risk assessment, expression and mood monitoring all create the potential for inaccuracy, bias and discrimination, particularly among marginalised workers.[9]

Journalist, tech activist and science fiction author Cory Doctorow makes the argument that machine learning is inherently conservative. This seems paradoxical, given the technology's seemingly revolutionary potential and its disruptive effects, which have already been

https://www.refinery29.com/en-us/2017/09/171485/google-employee-salary-spreadsheet; Wakabayashi (2017) *At Google, Employee-Led Effort Finds Men Are Paid More Than Women*, https://www.nytimes.com/2017/09/08/technology/google-salaries-gender-disparity.html

[7] Kafka (2016) *YouTube 'demonetization,' explained for normals*, https://www.vox.com/2016/9/4/12795214/youtube-demonetization-explainer; Radulovic (2019) *Creators make sense of YouTube's murky profanity rules*, https://www.polygon.com/2019/1/14/18182756/youtube-profanity-monetization-policy-creator-insider; Randhawa (2020) *How to Navigate YouTube's Unclear Demonetization System*, https://medium.com/super-jump/how-to-navigate-youtubes-unclear-demonetization-system-5c437c70e0ae; Romano (2019) *A group of YouTubers is claiming the site systematically demonetizes queer content*, https://www.vox.com/culture/2019/10/10/20893258/youtube-lgbtq-censorship-demonetization-nerd-city-algorithm-report

[8] Tenbarge & Goggin (2019) *"Like you've been fired from your job": YouTubers have lost thousands of dollars after their channels were mistakenly demonetized for months*, https://www.businessinsider.com/youtubers-entire-channels-can-get-mistakenly-demonetized-for-months-2019-8

[9] Vocal risk assessment assesses the purported "risk" of a person (e.g. an asylum seeker or potential hire) based on how they sound when they answer questions, not what answers they give. Expression and mood monitoring uses AI to analyse a person's mood.
For more, see Kofman (2018) *The Dangerous Junk Science of Vocal Risk Assessment*, https://theintercept.com/2018/11/25/voice-risk-analysis-ac-global/; Lewis (2019) *AI can read your emotions. Should it?*, http://www.theguardian.com/technology/2019/aug/17/emotion-ai-artificial-intelligence-mood-realeyes-amazon-facebook-emotient

observed. However, the effect of machine learning is to prompt with whatever has come before:

- Auto-complete prompts message writers to write the same thing they have written before.
- Serving ads online based on previous search history means consumers are "re-targeted" with products they may have already bought.
- Social media platforms prompt users to "friend" their stalkers, abusers and others who have their contact details.
- YouTube recommendations reinforce the user's preferences and interests instead of expanding them; watch one "flat earth" video and you will be prompted to watch others.
- Predictive policing targets the types of people who have previously been targeted by the police.

Likewise, hiring algorithms tend to reproduce past patterns of discrimination, as in the case of the automated resume screening system developed by Amazon that rapidly demonstrated a gender bias.

Doctorow quotes Patrick Ball from the Human Rights Data Analysis Group:

> A predictive policing system doesn't predict crime, it predicts policing.

Whereas a human being's potential for bias can be readily apprehended, algorithms and computers seem inherently objective. It is easier to believe that a human police officer may stop and search an Aboriginal Australian man on the grounds of the colour of his skin than to believe a machine would recommend doing the same – even though the machine has learned its behaviour from the past decisions made by humans. Doctorow calls this "empiricism-washing", hiding bias and privilege under a veneer of objectivity.[10]

Compensation

Granular tracking, particularly around contract and gig work, allows employers to determine when people are "working" and arbitrarily exclude "unproductive" periods such as downtime, problem-solving and sharing ideas. This creates an environment conducive to wage theft.

[10] For more, see Doctorow (2020) *Our Conservative AI Overlords Want Everything to Stay the Same*, https://blog.lareviewofbooks.org/provocations/neophobic-conservative-ai-overlords-want-everything-stay/; Sauter (2017) *Instant Recall*, https://reallifemag.com/instant-recall/

Job quality

New forms of measurement and quantification can pressure workers to forgo safety to meet efficiency benchmarks and to absorb the consequences of factors that monitoring and surveillance do not take into account. For example, “gig workers” in the home care industry are paid only for the actually delivery of a task rather than the travelling to and from different clients and, critically, any conversation with the person they are caring for.

Examples identified by Henderson et. al include Amazon workers facing a “countdown” to complete the next task as soon as each previous task is complete, microchipping of workers, and infrared monitoring systems that may be intrusive or anxiety-inducing.[11]

UK think tank Common Wealth collects other grim examples in its *Data and the Future of Work* report, including an “inactivity report” from Amazon in which an employee is accused of “talking with others between 7.27 and 7.36AM.”[12]

Hyper-granular, always on monitoring amounts can result in customised micro-management that erodes a sense of autonomy and responsibility in the workplace. As the sociologist Karen Gregory put it, flexibility (via working at a distance, for example) is not the same thing as autonomy: “Autonomy sits at the heart of meaningful work. These technologies chip away at that autonomy.”

[11] Henderson et al. (2018) *Under the Employer’s Eye*, pp. 15–17

[12] O’Brien & Lawrence (2020) *Data and the Future of Work*, p. 13, https://www.common-wealth.co.uk/reports/data-and-the-future-of-work

Potential solutions

The inquiry's broad terms of reference provide opportunities to consider a wide range of responses to the issue. Some approaches worthy of further consideration include:

Review and upgrade workplace surveillance legislation

The NSW workplace surveillance laws have been largely unused since they were introduced 15 years ago. However, they embed important foundational principles:

- The laws acknowledge the right for workers to not have emails with their union monitored by an employer. Does this principle provide a starting point for personal information that should *not* be accessed by an employer? For example, workers' personal interactions with co-workers to discuss workplace issues could be considered an extension of this right of association protection.
- The laws require employers to clearly state how a worker is being monitored. Requiring the type of activity that is monitored and how that information would be used would, in and of itself, provide important information to workers and their representatives about the scope of surveillance.
- The laws create a series of red lines around covert surveillance of workers, which require a magistrate's certificate and evidence of wrongdoing to be triggered.

Visibility and accountability

Where decisions about a worker's appointment, promotion or termination are based on data incidentally collected in their work, should there be obligations on employers to explain how those decisions are made?

This is an emerging requirement for government making decisions based on data, with recommendations for decisions to be explained and for humans to be accountable for decisions generated by AI currently the subject of a Human Rights Commission review.[13] Adapting these principles in a workplace context would allow for better scrutiny of the uses of workplace-generated information.

[13] AHRC (2019) *Human Rights and Technology Discussion Paper*, https://tech.humanrights.gov.au/

Rights to access and remove data

An alternative approach could be to adapt the principles of the European Union's General Data Protection Regulation (GDPR), which provide individuals with eight rights:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.[14]

For these rights to be adapted for Australian workers, these rights would need to be embedded in legislation which would prevail over the provisions of an employment contract to the extent of any inconsistency. For information on how GDPR affects workers' rights, see Cloudflare's guidance for employers on how to comply with GDPR while employees work from home.[15]

Right of entry to understand how data is being used

Unions have rights to access workplaces where they have members to inspect wage books and address members. This industrial right should be extended to give a workers' industrial representative rights to review the data collected by members in the course of their employment. Again, this would help workers understand how their information is being used and, critically, create a compliance framework for whatever sets of protections the review arrives at.

Incidental data production deemed an employment output and valued in terms of productivity

The extraction of surplus behavioural data in a workplace represents a secondary form of output for which workers are currently not compensated. If it is possible to calculate the financial benefit to employers (and it is) in terms of productivity, streamlined functions and increased work intensity, then this could be subject to industrial negotiations and recognition during wage negotiations. Revising NSW industrial laws to make the valuing of

[14] ICO (2020) *Individual rights*, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/

[15] Cloudflare (n.d.) *The GDPR and working from home*, https://www.cloudflare.com/learning/access-management/gdpr-remote-access/

this information an “allowable matter” in industrial negotiations would provide a mechanism for recompensing workers for this secondary output.

Discrimination laws

The Australian Human Rights Commission (AHRC) is currently proposing that automated decisions be subject to existing discrimination law, with mechanism for scrutiny of the underlying algorithms. Measures should be taken to ensure these principles apply with workplace technology.[16]

Public sector best practise

A full audit of current NSW Government processes and procedures with respect to the generation of incidental workplace data should be undertaken as part of this review.

Worker agency

There are a range of structures in existing industrial instruments around redundancy, termination and change that were designed to give workers input into technological change and its impacts. Intrusive monitoring is incontrovertibly part of a change process and workers should be involved in the process early and in a significant way.

Where data is being collected to “improve processes”, involving workers allows them to add value while respecting their agency. Requiring formal consultation mechanisms or works councils (workers’ representation at the level of the firm) would address the knowledge asymmetry in data acquisition that inevitably leads to greater power imbalances.

Data trusts

A broader approach would determine that data generated in employment relationship is outside the employment contract and should remain the property of the worker. Under this model, the information would be held on trust with workers (through a representative organisation modelled on industry super funds). This would ensure the information is used in the interests of the worker and that due value was returned to all members of the trust. Such a model would allow employers to negotiate the use of this data to improve a business while maintaining a stake for workers in how it is used. Establishing these vehicles in public

[16] AHRC (2019) *Human Rights and Technology Discussion Paper*

sector agencies would be an opportunity to incubate and pilot the concept. For more see the writings of Alex White, Secretary of UnionsACT, on data trusts.[17]

[17] White (2020) *The strategic urgency of building Workers Data Trusts*, https://alexwhite.org/2020/04/the-strategic-urgency-of-building-workers-data-trusts/

Conclusion

One of the largest private Silicon Valley companies is the data analytics company Palantir Technologies. The name is an allusion to the crystal balls in the *Lord of the Rings*.[18] In JRR Tolkien's books, the *palantíri* are used to see real events: past, present and future.

The name was probably motivated only by Silicon Valley's well-documented, if unreflective, love of Tolkien's books.[19] An all-seeing crystal ball seems like a good inspiration for a company that accumulates, analyses and makes decisions based on "big data" accumulated from a vast range of sources.

However, Tolkien scholar Tom Shippey observed that a recurring theme in the *Lord of the Rings* is that the *palantíri* provide information, but not knowledge. The *palantíri* produce true images, but when characters look into a *palantír* they come away with the wrong impression:

- Pippin is confused for Frodo Baggins, misdirecting the evil Sauron;
- a fleet is seen but its allegiance is mistaken, causing the steward Denethor to give up hope prematurely and commit suicide; and
- Aragon is seen with a special sword, causing Sauron to rush his military operations and ignore the true threat.[20]

By confusing information for knowledge, pursuers of big data and machine learning risk making the same mistakes as the users of the *palantíri*: drawing conclusions without full information, interpreting the information they receive through their own preconceptions, and over-estimating how much they truly know.

This makes for an unsound business strategy, but becomes a human rights issue when it affects consumers, workers and other stakeholders. Workers should not put their faith in crystal balls, or let their bosses surveil with them. As the UK think tank Common Wealth puts it:

> The risk of AI isn't in the human-shaped robot that will take your job, but in the power it affords to employers, which have long been wary of worker insurgency.[21]

---

[18] Maus Strategic Consulting (2014) *A (Pretty) Complete History of Palantir - Maus Strategic Consulting*, https://web.archive.org/web/20140516035733/http://www.mausstrategicconsulting.com/1/post/2014/04/a-pretty-complete-history-of-palantir.html

[19] Rodriguez (2020) *Why Silicon Valley is obsessed with "The Lord of the Rings,"* https://www.cnbc.com/2020/02/22/why-silicon-valley-is-obsessed-with-the-lord-of-the-rings.html

[20] Shippey (2003) *Road to Middle-Earth*, pp. 188, 423–429, Mariner Books

[21] O'Brien & Lawrence (2020) *Data and the Future of Work*, p. 14