Worker Data Right: the digital right of entry

Colleen Chen and John Howe

Policy Brief 5, 2022

Centre for Employment and Labour Relations Law
Melbourne Law School
The Centre for Employment and Labour Relations Law’s policy brief series aims to distil academic research in the fields of employment, labour relations and equality law into policy analysis and clear recommendations, drawing on cutting-edge research by leading scholars at the CELRL and other academic institutions around Australia, as well as from our wider international networks. The initial policy briefs are based on some of the presentations to a symposium with the theme ‘Labour Law Reform under the Albanese Government’, hosted by the Centre on 12 August 2022, and timed to coincide with the Albanese Government’s ‘Jobs and Skills Summit’ held on 1-2 September 2022. However, the series is intended to be an ongoing forum for clear and concise discussion of current policy issues as they emerge. The series is edited by CELRL Directors Associate Professor Tess Hardy and Professor John Howe.

Colleen Chen is a Research Fellow at the University of Melbourne School of Government and works at a leading data science company. She has a Juris Doctor from the University of Melbourne and a Master of Data Science from the University of Adelaide. From 2019-2021, Colleen led policy development and industry engagement for the Defence Artificial Intelligence Centre within the Department of Defence and served as the Secretary of the IEEE P7010 working group for Ethical Artificial Intelligence and Autonomous Systems. Colleen was the founder of Australian employment law advocacy association, Interns Australia (2013-2020) and is a key contributor to the research project ‘A Fair Day’s Work: Detecting Wage Theft with Data’ at the Melbourne School of Government.

Professor John Howe is Director of the Melbourne School of Government and Director of the Centre for Employment and Labour Relations Law at the University of Melbourne. John’s research interests include labour market policy and regulation, regulatory design, and corporate accountability. He has written extensively on the role of the state in regulating employment and labour markets, and on the intersection between state-based regulation and corporate governance. John is presently engaged in research concerning regulatory enforcement of minimum employment standards and labour dispute resolution in Australia and the Asia-Pacific region. He is also leading the Program on Regulation and Design at the School of Government.
**Introduction and Recommendations**

Over 59% of Australian businesses use digital technologies to monitor their workers, a figure that is only likely to increase given the exponential growth in remote work brought on by the COVID 19 pandemic.¹ Unlike traditional forms of workplace surveillance, worker-related data is increasingly collected through digital platforms for the purposes of improving workplace safety, delivering employee benefits and improving productivity.² The types of data being collected include sensitive information about the employee such as biometric data, financial data and medical data. However, under the current regulatory environment, the data collected is not accessible by workers and is often sold to third parties without the worker’s informed consent.

Misuse of worker data can cause harms such as unfair dismissal, unlawful discrimination, physical injuries and identity theft. Yet, due to the lack of transparency in the data collection process, misuse of the worker’s data cannot be detected and only surfaces where harm has already occurred. The *Privacy Act 1988* (Cth) (*the Privacy Act*) does not apply to employee data collected within the scope of an employment relationship.³ Other regulatory frameworks governing monitoring and surveillance of workers in Australia are outdated, and do not extend to misuse of worker data.⁴

Many of these concerns would be addressed by the enactment of a national Worker Data Right, along the lines of the already existing Consumer Data Right. The Worker Data Right would consist of a portable database (data trust) consisting of all employment-linked data of a worker, held by the worker or their nominated representative.⁵ The Worker Data Right proposal addresses the issue of worker data being inaccessible to both workers and regulators, and will also help prevent that data being misused.

The Worker Data Right would hold the employment-linked data in trust for the benefit of the worker, giving them control of the impacts on their wellbeing. It would also provide a one-stop portal for worker representatives, service providers and regulators to access data that would support strategic enforcement and compliance monitoring.

**Recommendations:**

1. That data collected within the scope of an employment relationship is no longer exempt from the *Privacy Act 1988* (Cth).
2. That the federal government establish a framework for safe and secure data sharing of worker data under a legislated Worker Data Right that is modeled on the Consumer Data Right and its infrastructure.

---


² Negron, W (2021) 'Little Tech is Coming for Workers', *coworker.org*.


Alignment with the Jobs and Skills Summit

The Worker Data Right (WDR) supports the federal government’s Jobs and Skills Summit agenda of delivering secure, well-paid jobs and strong, sustainable wages growth. In particular, data transparency in the workplace will underpin the ability to "ensure workplaces are safe and fair, particularly for those people at higher risk of harassment, discrimination and other breaches of workplace minimum standards."6

Wage theft, or the underpayment of workers, is an ongoing policy challenge due to the difficulty in detecting misconduct at scale. While the Fair Work Ombudsman and unions continue to recover record amounts of underpayment, there is still no proactive and systematic method of detecting underpayment at a business unit level.7 For instance, even though the Business Longitudinal Analysis Data Environment (BLADE) dataset is a comprehensive administrative dataset covering almost all Australian business activities from 2001 onwards, it can only be used for research purposes and unit level records cannot be used for enforcement purposes.8

To address the challenge of accessing administrative data for workplace compliance, the WDR can provide the data required to identify underpayment and other forms of workplace misconduct in a timely and systematic manner. With the worker’s permission, community legal centres, unions and regulators such as the Fair Work Ombudsman and Safe Work Australia, would be able to access the worker’s data to support the worker in an employment-related issue.

As with the success of the Consumer Data Right in driving new solutions to boost competition in financial services, access to employment-linked data will bring new approaches to improving working conditions by way of new products and services aimed at workers. For instance, SafetyCulture (workplace safety), EmploymentHero (payroll and benefits) and Deputy (shift management) are all valued in excess of $1 billion, having raised over $100 million in capital from investors. Arguably, such high valuations result from the value of the data about its subjects (the workers), and as such, worker data should be seen as a valuable resource not only for emerging startups but also for protecting the rights and wellbeing of workers and improving Australian workplaces.9 The Worker Data Right will bring an unparalleled degree of transparency to the workplace for workers, for their representatives and for regulators.

The WDR will spawn innovation in workplace relations by giving workers the choice to share their data for the purpose of receiving better services, better workplace representation, streamlined workplace support and evidence-based policymaking. Data transparency in the workplace will also enable regulators, unions and other work advocacy groups to deliver stronger digital rights of workers in accordance with emergent best practices set out by UNI Global, the global union federation for the skills and services sectors.10

---

Why we need a Worker Data Right now: Argyle Case Study

Another reason for enacting a WDR is to protect vulnerable workers from potential misuse of their data.

Argyle is a US-based global financial data broker company that seeks to become the “Gateway to Employment Data”. Argyle claims to have already acquired the employment records of over 80% of gig economy workers and over 40 million Americans in the United States. Argyle has access to workers’ data from major corporations that employ a large segment of low-wage workers such as Amazon, Walmart, Starbucks, Uber, FedEx, and Target.11

Initially, Argyle claimed that their employment data was used for income verification services for general loan servicers, lenders, and insurers. However, in a note to investors they mentioned that their clients were largely payday loan providers, which offer ‘fast’ loans at high interest rates.12

These revelations are concerning for the following reasons:

1. The sale of data to payday loan lenders enables predatory behaviour targeting workers in vulnerable financial situations since payday loan lenders are exempt from the 48% interest rate cap established under the National Consumer Credit Protection Act 2009 (Cth);13
2. If the records of the workers were inaccurate and were sold to third parties such as general loan servicers, lenders, and insurers, then the worker would not know to correct the inaccuracy, nor would they be able to correct the inaccuracy; and
3. Without a general right to access this data, Argyle has no obligation to make the worker’s own data available to them for a purpose such as pursuing a workplace claim.

The Worker Data Right would mitigate the harms identified above by:

1. Enforcing the ban on the unauthorised sale of the worker’s personal data and preventing vulnerable workers from being targeted by payday loan lenders;
2. Allowing workers to see how their previous work information was used by banks and insurers when assessing their suitability to access financial services. The WDR will require that worker be given an opportunity to provide more context to the data and to be able to rectify inaccuracies in the data so that they are not unnecessarily financially penalised;
3. Giving workers access to their own data at any time so that information collected about them can be used by them for personal benefit such as processing a workplace claim.

What is the Worker Data Right?

The proposed WDR is a data trust framework for managing data collected over the course of a person’s employment across multiple employers throughout their working life. The framework mirrors the Consumer Data Right (CDR) established in 2019. CDR is a secure online system overseen by the Australian Information Commissioner and the Australian Competition and Consumer Commission (ACCC) through which consumers can consent (or not consent) to their consumption data being shared with accredited third parties. The security and integrity of the CDR system is protected by 13 privacy safeguards, contained in the Competition and Consumer Act 2010 and supplemented by the CDR Rules. Similar to the CDR model, under the WDR, the worker would not need to manage the storage or the processing of their data. The worker would only need to decide whether to give informed consent to the services that will store and use their data to benefit the worker. For instance, the worker would need to understand the purpose for which a union wishes to access their data – eg for enterprise bargaining purposes- before the union could use this data. It would also be the union’s obligation to ensure that before they access any worker data, that they are an 'Accredited Data Recipient' under the WDR and are able to handle the data securely and correctly.

The WDR seeks to leverage the CDR model and its existing infrastructure to ensure that workers are just as empowered as consumers to manage their personal data. As we outline below, the CDR does not extend to worker data collected by employers, and currently the Privacy Act does not apply to employee data collected within the scope of an employment relationship. However, as we noted earlier, the amount and variety of employee data collected by employers has intensified over time due to the proliferation of workplace monitoring and surveillance technologies. Employee data is no longer used exclusively for core business purposes, such as payroll, taxation, superannuation, pre-employment checks and reporting. Rather, as evidenced by the Argyle case study, employee data is shared and traded with third parties for the employer’s financial gain.

Inconsistency of Data Rights, the citizen as a consumer and as a worker

---

The emerging applications of employee data creates an inconsistency in regulation and leads to a situation whereby one individual’s data can be handled differently by the same entity depending on how it was collected. For instance, if a person were a customer with bank A, and bank B wanted access to the person’s data from bank A, bank B must register to become an Accredited Data Recipient with the Australian Competition and Consumer Commission under the CDR. Once accredited, bank B must obtain consent from the individual before accessing their data.

However, if bank B were to access such data from a large employer to market its financial products to the same individual, then bank B does not need to seek the individual’s consent if the activity were directly related to the employment relationship. In this case, bank B could simply pay the employer a customer acquisition fee to use the worker’s data to market special offers in a salary packaging discussion or expose its products during a company financial wellness presentation.

Financial data and health data collected by banks and healthcare providers respectively can also be collected by employers. Due to this overlap, the WDR proposal is based on the premise that data rights should be extended to the workplace so that loopholes affecting the policy intentions of the CDR are removed. The CDR currently covers the financial sector and will be expanded to cover the energy and telecommunications sectors.17 The expansion of the CDR to other sectors suggests that this model and its infrastructure is capable of, and is intended for, broad application across the economy. The enactment of a separate WDR modeled on the CDR will benefit workers by reducing the current regulatory inconsistency between consumer data and worker data.

At the same time, the employee records exemption under the Privacy Act should be abolished, while safeguarding the right of inspection of employee records by regulators and authorised worker representatives to ensure compliance with workplace laws. In 2021, the Australian Law Reform Commission considered removing the employee records exemption under the Privacy Act.18 It noted that where employee health records and biometric information were concerned, the Commission has been calling for the employee records exemption to be removed since 2003.19 The Commission did not consider the compliance burden on businesses to be significant and suggested that removing the employee records exemption would allow the Privacy Act to be consistent with the regulatory practices of the United Kingdom and the European Union.20 The Commission’s view that businesses should be capable of adopting “good information-handling practices” is reflected in the increasing scope of the Single Touch Payroll system, which requires employers to report on granular employment and taxation conditions such as income types and child support deductions.21

---


How it would work

The federal government can legislate to create the Worker Data Right, just as it did for the Consumer Data Right in 2019. The WDR would be its own instrument, just as the CDR is an instrument made under section 56BA of the Competition and Consumer Act 2010. The appropriate federal legislative and regulatory ‘home’ for the WDR, and its constitutional underpinnings, will need to be resolved. However, we recommend that the WDR be modeled on and integrated with the CDR infrastructure as much as possible, as illustrated below:

<table>
<thead>
<tr>
<th>Consumer Data Right</th>
<th>Worker Data Right</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applicant applies for an account to access Consumer Data Right Participant Portal</td>
<td>Applicant applies for an account to access Worker Data Right Participant Portal</td>
</tr>
<tr>
<td>Authorised deposit-taking institutions (ADIs) can complete a streamlined application form. Non-ADI applicants must complete the standard application form.</td>
<td>Accredited Data Recipients (ADR) can complete a streamlined application form. i.e. If businesses have gone through the CDR process, they do not need to go through WDR. Non-ADR applicants must complete the standard application form.</td>
</tr>
<tr>
<td>The ACCC may accredit the applicant, accredit the applicant with conditions or refuse to accredit the applicant based on accreditation criteria.</td>
<td>The regulator may accredit the applicant, accredit the applicant with conditions or refuse to accredit the applicant based on accreditation criteria.</td>
</tr>
<tr>
<td>Accredited data recipients (ADR) need to pass Consumer Data Right Register on-boarding requirements, including a level of conformance testing, before they can be added to the Consumer Data Right Register.</td>
<td>Accredited data recipients (ADR) need to pass Worker Data Right Register on-boarding requirements, including a level of conformance testing, before they can be added to the Worker Data Right Register.</td>
</tr>
<tr>
<td>Consumers give permission for the ADR to access personal or business data. Consumers will be able to see and manage the data consented to share and can withdraw consent at any time on the provider website or app.</td>
<td>Workers give permission for the accredited businesses/union to access personal data. Workers will be able to see and manage the data consented to share and can withdraw consent within parameters of consent given.</td>
</tr>
<tr>
<td>Data is transferred from the data holder to the prospective ADR. Consumers receive new services from ADR.</td>
<td>Data is transferred from the employer to the approved businesses/union. Workers receive benefits from controlled data sharing.</td>
</tr>
</tbody>
</table>

---

The WDR will allow the following consent models to offer workers full flexibility over how to manage their data:

- **Self-managed**: the individual worker manages consent to all WDR requests
- **Delegated**: individual consent is delegated to an intermediary, such as a data trust, to manage all WDR requests based on a predetermined data sharing policy
- **Bundled**: the individual worker’s consent is delegated to the employer

When an employer becomes an Accredited Data Recipient and seeks access to use employee data to share with third parties, it must obtain consent from the employee before the data is used. Depending on the consent model selected by the worker, access to data can be automatically accepted or rejected by the worker based on its intended application. The proposed initiatives may proceed with the full or partial support of the workforce, or be withdrawn due to insufficient data granted by workers, showing a lack of support for the initiative. The illustration below shows how the data of 10 workers in a business will be affected under the WDR based on their preferred consent model.

**Worker acceptance of employer data use - an example**
Conclusion

The Worker Data Right aims to provide a meaningful feedback loop on data use in an employment relationship, bringing the worker’s agency over their personal data in line with the consumer’s agency over their personal data. As the quantity and nature of worker data gathered continues to expand through technological advances, the Worker Data Right will ensure that the outcome of increased data collection can be managed in a democratic manner.

This paper has outlined several ways in which Worker Data Right will spawn innovation in workplace relations and tackle the information asymmetry between workers, unions and regulators, and employers. Giving workers a secure way of sharing their data can result in better workplace representation, streamlined workplace support and richer insights to support policymaking. Data transparency in the workplace will also enable regulators, unions and other work advocacy groups to deliver stronger digital rights for workers.