Privacy and Responsible Information Sharing
CPSU/CSA consultation query responses.

Q1. Does the absence of privacy legislation in Western Australia concern your organisation? Please explain your answer:

The CPSU/CSA is broadly supportive of ex-President of the Australian Human Rights Commission, Professor Gillian Trigg's statement that digital regulation should be viewed as human rights law. Too many reforms or new operations, built on technology which has not been adequately discussed or considered by civil society, runs the risk of government failing to define a baseline of human rights governing a citizen's digital surveillance, information collecting and digital footprint.

Some basic digital human rights which should inform the drafting of legislation include:

- the right to communicate freely through electronic devices and the internet while retaining rights such as freedom of expression, freedom of association (such as with an employee's union), cultural and political participation, self-determination and freedom from discrimination.
- the right to control one's personal data and not have it misused, breached, lost or stolen.
- the right to legal redress if one's rights are infringed. (p14 Digital Rights).

Q2. Ideally, Government would inform the public:

- ***the purposes for which they collect personal information;***
- ***any consequences of not providing personal information to the organisation; and***
- ***whether the entity is likely to disclose personal information to authorised third party recipients.***

Is there anything else the WA Government should tell you when it collects information?

Any new legislation should seek to develop privacy and digital rights as a widely understood and defined set of social norms in Australia. The government should consider the publication of a digital rights kit to educate the public about how and why their data is used and their digital rights.

The CPSU/CSA would broadly support Western Australian agencies adopting the federal government's 'Five-Safes Framework' for safe data keeping. These questions inform digital rights which should be shared and communicated to the public. The public service workers should be able supported to provide sufficiently detailed responses to the questions posed by the five-safes framework when asked by a concerned member of the public.

The Australian Bureau of Statistics have published practical examples of the various control measures used to reduce the risk of privacy disclosures related to the Five-Safes framework. These include:

1. User training in systems collecting private data – ensuring new staff know the risks and refresher training is provided.
2. User authorisation processes - the need for staff members to sign legally binding confidentiality undertakings and compliance declarations.
3. In addition to the above, all users must detail purpose of use.
4. Secure logins provided by the employer with secure hardware. Direct identifiers are removed, data is cleaned and optimised to maximise usefulness for research or statistical analysis purposes.
5. A dedicated unit assesses disclosure identifiers and privacy risks and takes appropriate steps to reduce risk.

The CPSU/CSA would support the 13 Australian Privacy Principles (APPs) developed from the *Australian Privacy Act 1988* being used in creating a basic set of digital rights.

The CPSU/CSA is of the view that, in relation to APP 7 (Direct Marketing), private data should not under any circumstances be used for marketing of anything other than community consultation functions and access to publicly driven healthcare initiatives.

Further, APP 11 and 12 (Security and Access to personal information) should prompt public sector procurement and ICT reform leaders to be highly aware of the risk of the sector becoming reliant on the provision of software and technology from private interests. A digital infrastructure provider is able to 'capture' the public sector unless very clear and deliberate early decisions are made to ensure the public sector can run data sharing and private information storage independently. Early work to ensure the sector is not captured by the technology provider would place the rights of citizens in an advantageous situation in the long term.

This risk is articulated in the paper 'Digitalisation of Public Services: A Labour Perspective':
"The dependency on private digital technology providers and the increasingly blurred lines between public and private space boundaries in highly digitalized public services carries an intrinsic risk for the confidentiality and control of users' and workers' data. It can also represent a threat that public authorities lose control over the data they normally collect and control, and end up having to pay private "gatekeepers" to which they outsource services to access users' and citizens' personal and consumption data." (p15)

It is vital there is adequate consultation in operational changes relating to client data. For instance, the December 2016 Centrelink 'robo-debt' debacle illustrated the real impact of a rushed reform agenda relating to Centrelink users.

Restructures had replaced human-led calculations and analysis with an algorithm comparing ATO employer data with the Centrelink client's self-reported earnings. The algorithm then generated an automatic notice of debt. The mental health of many recipients was endangered with false accusations of enormous debts and hounding calls from private debt collectors (who all received a per cent of the invented debt collected). A survey of Department of Human Services by the CPSU – PSU, the Union covering Australian federal public servants, found that 95 per cent thought the Department should restore the role of staff in verifying the accuracy of information used to raise debt notices before they are issued.

This failed reform of services could have been avoided if public users were given more consultation in how their data was about to be used. Instead, the robo-debt errors (which made national news for some weeks), completely undermined public trust and confidence in the Department of Human Services as a whole. As one public sector worker reported:

"The simplified data match, which is wholly inaccurate, has created a crisis of faith in the impartiality and accuracy of the debts raised within the welfare system. The process is flawed, the outcome is immoral. For customers who challenge the debt - good, but they have no faith in the outcome of an appeal. But what about the customers who have not challenged the outcome? They suffer in silence. The whole program is legislatively and morally indefensible." (p4, CPSU)

Q3. What activities should be permitted? For example:

- ***purposes related to the wellbeing, welfare or protection of an individual;***
- ***supporting the efficient delivery of government services or operations;***
- ***research and development with clear and direct public benefits;***
- ***supporting evidence-based decision making; and***
- ***assisting in the implementation and assessment of government policy.***

What else should be included? What changes would you propose to the above list?

The CPSU/CSA supports the above list but also for de-identified data to be used for:

- Academic research and development of knowledge to identify trends, relevant findings and information of importance to policy and analytical staff.
- 'Knitting together' the various and multiple service journeys of members of the public in order to analyse where the taxpayer dollar can be best spent on targeted programmes and services.

The CPSU/CSA would ask the government to also consider increased reliance on digital technologies and data from an industrial perspective. Internationally, unions are beginning to draft new agreements about how disruptive technology is used to improve the workplace. For instance, British and Irish trade union UNITE has developed a Draft New Technology Agreement which addresses key worker concerns:

- the right of displaced workers to retraining and reskilling (No One Left Behind);
- solidarity and the acknowledgement that technology reform is not about one classification of workers against another;
- fair use of monitoring and surveillance of public sector workers;
- the freedom of the worker to leave work at the workplace after working hours have concluded (The Right to Disconnect);
- creation of new jobs which recognise the potential in creative, human tasks;
- any impact on public sector worker mental health that increased digitalisation of the workplace may bring.

Q4. When sharing information with third parties, what should the WA Government do to make sure confidentiality is maintained and privacy is protected?

The Office of the Victorian Information Commissioner recommends all agencies follow a 'Five Step Action Plan' as part of developing a Protective Data Security Plan. The publicly available resources around this are vague and it appears data security is generally left for each agency to develop plans and infrastructure around individually. This increases the workload for public servants and increases the risk of siloed approaches. Plans are supported by voluntary attendance with the Victorian Information Security Network. The CPSU/CSA believes the WA state government's approach in developing the Office of Digital Government (ODG) may be a better path forward. Resourcing to the ODG should be made to ensure a uniform high standard in data security for WA agencies.

The New Australian Government Data Sharing Issues Paper lists some questions for a purpose test for whether data should be collected in the first instance (p14):
-Does it inform government policy making?
-Does it support greater efficiency in government service delivery or operations?
-Does it assist in implementation and assessment of Government policy?
-Does it inform research with clear and direct benefit to the general public?

It is unfair and unrealistic to place a legal onus on an employee to protect private data if the employer has not adopted sufficient protective hardware, software, operational systems and policies to protect the data. Staff must be protected and confident that they will be taken seriously if they raise concerns with directions to transmit data in a non-secure method (for example; without encryption).

The CPSU/CSA would appreciate more detail from government on how private client data would be shared or stored by external third parties under the legislation. For example, if a for-profit prison service provider ran a medium security facility for prisoners and in doing so, gained access to the private government data profiles of a high number of vulnerable West Australian citizens, what would be the obligations on the service provider to protect, update and return the data? This is just one of a few key concerns the union would list. More concerns include:

- The ability of a private service provider to copy data to their own data infrastructure and use it for business operations.
- The ability of the private service provider to keep the data accessed in perpetuity.

- The ability of the service provider to update/amend/rewrite client data profiles and ability of the public sector to verify/police new data.
- Inadequacy of penalties for cases where incorrect data is added to public data assets, or when data is not updated/added at all (may be in breach of a contract).
- Stymied public access to details around privacy and data security, as well as personal data itself due to misuse of 'commercial in confidence' provisions.
- Small to medium sized private service providers arguing the cost of data privacy protections is unrealistic, too expensive or too onerous for a community-based organisation, leading to a tendering environment where only medium to large sized operators are capable of securing contracts.

Q5. How should breaches of privacy be managed in WA and what action should be taken in response to a breach? Please explain your answer:

Victorian privacy law stipulates a difference in penalties between a data breach with intention and one that occurs unintentionally. This is highly important given the key role of infrastructure in protecting records.
Similarly, the Commonwealth's Data Sharing and Release Legislation issues paper states that penalties should consider whether the disclosure of private data was intentional or not (p21).

The CPSU/CSA would appreciate a shared, sector-wide statutory code of conduct/practice/operational pathway stemming from the Act. It is important to ensure the code can be applied across as many affected agencies as possible. This limits risk to clients of having their data misused in case data is transferred between departments, or if agencies are merged. This would also reduce the number of difficult questions around use of assets in the event of data transfer, agency reform or agency mergers.

Breaches can be hugely expensive for the government – for this reason it is critical that any breach is rapidly dealt with and the public service is appropriately resourced to contact and support victims of a breach immediately. When a breach occurs, of immediate importance is the need to inform affected parties that the agency has failed to meet its data security obligations. Alerting affected parties of the breach as early as possible minimizes the damage a data breach can inflict. This view has also been put forward by the Australian Law Reform Commission.

Q6. Could the WA Government be doing a better job of sharing information between agencies to make your life easier?
What type of streamlined benefits would you like to see from improved information sharing by public sector agencies?

There is considerable public interest in using collected data to develop better Government policy making, program management and service planning and delivery by agencies. Where possible, the successes earnt by smart use of data must be communicated clearly with staff. Accurate and complete data collection is critical for improved information sharing and realising benefits. However, inputting data takes time. Public sector workers need to be adequately resourced to perform this function.

The potential of service pathways that are shared by multiple agencies are now well-known across the WA public service. For instance, a disadvantaged Western Australian child may have multiple service interactions with Local Government, the Department of Education, the Department of Communities and even the Department of Justice. In order to allow CPSU/CSA members to better cooperate with one another in planning and delivering services, data should be developed to best assist multi-agency collaboration and assistance.

The rules on what information is shareable needs to be clearly defined. Agencies should be clear that they must not request data that they are not explicitly allowed to access. For instance, in 2016 it was revealed that the Australian Taxation Office, the Department of Foreign Affairs and Trade, the Department of Agriculture, Department of

Education and Department of Social Services had all requested that the Australian Federal Police conduct metadata searches for them. Examples such as this erode trust in the public service.

Q7. What powers or responsibilities do you think a WA Privacy Commissioner should have?

"Safeguards must be in place before any thought of data and information sharing occurs. These safeguards have to be external to the bodies who breach the legislation, enforceable, immediate, reliable and providing appropriate remedies to those whose lives can potentially be ruined with the release of inappropriate information (e.g. HIV positive or mental illness and the associated job and insurance implications this brings). Once information is released the damage cannot be undone."
-CPSU/CSA member and patient data custodian, Department of Health.

A recent survey of 1600 Australians found that 47 per cent were concerned about privacy violations caused by or relating to government data. Only 38 per cent felt in control of their data (University of Sydney). Clearly more is required to grant Australians confidence that their digital rights are being protected.

In terms of modern public service delivery corporate structures, the European Data Protection Supervisor's office demonstrates how work could be conducted. This office includes a supervision and enforcements unit, a policy and community consultation unit, ICT policy unit, media and communications unit with adequate business supports.

Where possible, agencies may also consider the creation of Data Protection Officers/Data Privacy Officers. These staff members would be responsible for:

- Advising/educating staff on information governance
- Undertaking Privacy Impact Assessments (PIAs)
- Ensuring compliance and undertaking compliance reviews following the relevant state/federal law
- Providing advice to staff faced with decisions about data sharing
- Liaising closely with the Chief Data Officer/WA Privacy Commissioner's offices to ensure uniformity in standards and codes
- Liaise with any Process Automation Officers who would be considering worker interests, good work design and instilling confidence and trust in the system.

CPSU/CSA members currently work with Public Key Infrastructure (PKI). PKI is an encrypting cybersecurity measure which protects data sent between a government agency server and any users. There are two keys involved – a public key and a private key. The public key is given to any user accessing an agency website, while the private key is reserved for less transparent interactions. Both keys may encrypt and decrypt data sent. A Certificate Authority and a Registration Authority are used to authenticate users, ensuring no falsified identities can gain access.

CPSU/CSA members use Auskey, a secure login which Commonwealth agencies use to allow access to government online services. This model will be replaced in March 2020 by MyGovID and an authorisation service named the Relationship Authorisation Manager, or RAM. The Commonwealth includes designated categories of files, such as Confidentialised Unit Record Files (CURFs) and Public Use Files (PUFs). The Privacy Commissioner's office could be given a role in ensuring each agency uses PKI for all necessary transfers and is resourced to work effectively with MGovID.

CPSU/CSA members responding to this consultation period informed the union that they had doubts around the inclusion of internal "integrity units" within agencies. Having an internal integrity unit opened the mechanism up to influence from within the agency, whether through personal relationships, career prospects after leaving the unit or a lack of wider context. Members communicated that integrity functions were better served by an outside, independent, well-resourced unit, such as within the PSC or a Privacy Commissioner's Office.

Q8. What should the role of a WA Chief Data Officer be in ensuring the proper sharing of information for public's benefit?

One operational concern would be how the Chief Data Officer (CDO) would request data from various agencies. The CDO would require powers under legislation to request this information from agencies. However, what efforts will be undertaken to ensure each agency is resourced and equipped to meet such requests? Who will have the authority to refuse a request around restricted data? The CPSU/CSA is inclined to support the Victorian approach, which allows a data authority hold data as their central capability, which then has resources (staff, training, networks) deployed to agencies who can realise the most advances from data. Agencies should be resourced to make the most of this data without being completely reliant on an external authority. The NSW's large pool of data approach could create usability risks in terms of uniform standards and datasets which may not intermesh easily.

The Victorian legislation makes specific references to data that is exempted from Freedom of Information laws. It is highly important that any exemption from FOI is drafted in a way so that;

- Simply providing data to the CDO does not make information immune to FOI laws across the entire public sector;
- Data itself is not immune to FOI, but sensitive data (commercial secrets, disclosure of identity, ongoing public investigations and law and order matters) is protected;
- Australian Privacy Principle 1 overcomes restrictions created by commercial confidence protections for corporations.

Under S33 of Victorian legislation, the Chief Data Officer is responsible for issuing policies and guidelines to protect privacy and confidentiality in data, establish data security safeguards, secure technology platforms, assign risk mitigation frameworks for data handling and storage and establish protocols for data integration projects. These standards apply to any 'data sharing body, designated body or a data analytics body'. This should be supported in WA.

Q9. Do you have any general comments on the proposal for privacy and responsible information sharing legislation in WA?

The CPSU/CSA would be interested in receiving more detail about what would occur in an instance of data fraud. For example, if a financial incentive is introduced to outcomes-based commissioning models of contracts, where the provider must prove clients have experienced positive results from services delivered (for example, successful alcohol and other drug rehabilitation, completion of job or skills based training, successful treatment of a health related issue), this can create a reward to mislead in client data records. This could create a risk for data integrity.

If a service provider or external financier will only receive a 20 per cent bonus on a contract if 50 per cent of clients receive successful interventions, there is a clear motivation to send incorrect data back to government. Therefore, the public service runs the risk of contaminating data if editing rights are entrusted with external providers. This would be fraud, but it may be worse, as bad data that is not discovered for months or years may go on to influence key policy decisions.

The government will need to consider management plans, protections, risk for the risk of 'bad data' that may be caused by motivating external service providers with payment by results KPI-focused service models.

CPSU/CSA as a Data Custodian

The CPSU/CSA works cooperatively with government to request, analyse and comment upon current corporate structure and workforce statistics for agencies covered by the union. In this way, the CPSU/CSA could be considered an authorised third party and a data custodian for HR data. Unless otherwise specified, staff details are de-identified but the data is able to demonstrate resources towards appropriate staffing levels for a unit or agency.

Also of interest to the CPSU/CSA is worker's compensation statistics, disciplinary statistics, staff turnover statistics and PSC Employee Perception Survey results. This data is important to determine where resourcing, systems and practice improvements should be made ensure fair, equitable, safe and healthy workplaces. Without a holistic view of how each component of the public service operates, the Union runs the risk of organising towards myopic goals. For instance, prison programmes may not require additional FTE if there are concurrent strategies to ensure sentenced individuals are able to work, train, be supported or rehabilitated while remaining in their communities.

The CPSU/CSA appreciates the opportunity to comment and would like to reiterate our focus that any legislation holds in highest regards the digital rights of the citizen and the public sector worker. We look forward to future opportunities that responsible data sharing could bring to build a better public sector workforce and workplaces.

REFERENCES

Australian Government Agencies Privacy Code. Office of the Australian Information Commissioner. 25 July 2019. Available at: https://www.oaic.gov.au/privacy/privacy-for-government-agencies/australian-government-agencies-privacy-code/

Australian Government Public Data Policy Statement 2015 (federal document)
Available at: https://www.pmc.gov.au/public-data/public-data-policy

Australian Privacy Principles Quick Reference. 8 August 2019. Office of the Australian Information Commissioner. Available at:
https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-quick-reference/

Centrelink Compliance Program. Community and Public Sector Union. September 2019. Available at:
https://www.cpsu.org.au/system/files/sub11_cpsu.pdf?fbclid=IwAR37bk7ZIn-DpYjJCdqJ9vAzH8Fy5Oq5hLvfF-W2QceugeBPGSGwsnn6MF0

Data Availability and Use Inquiry 2017 (Productivity Commission)
Available at: https://www.pc.gov.au/inquiries/completed/data-access#report

Data Sharing (Government Sector) Act 2015 (New South Wales)

Data Sharing Code of Practice: Draft Code for Consultation. Information Commissioners Office. 15 July 2019. Available at: https://ico.org.uk/media/about-the-ico/consultations/2615361/data-sharing-code-for-public-consultation.pdf

Digitalisation and Public Services: A Labour Perspective. Public Services International.
Available at: https://pop-umbrella.s3.amazonaws.com/uploads/abbb272d-2710-45eb-b1dc-bf6579eb8a1c_2019%20-%20EN%20Digit%20Summary%20LRGM%20web.pdf

Dingwall, D. et al. Data Breach sees records of 50,000 Australian workers exposed. 2 November 2017.
Available at:
https://www.smh.com.au/public-service/data-breach-sees-records-of-50000-australian-workers-exposed-20171102-gzdef3.html

Health Records Act 2001 (Victoria)

Majority of Australians say online privacy beyond their control (27 November 2017) University of Sydney.
Available at: https://sydney.edu.au/news-opinion/news/2017/11/27/majority-of-australians-say-online-privacy-beyond-their-control.html

New Australian Government Data Sharing and Release Legislation – Issues Paper for Consultation. Department of the Prime Minister and Cabinet. p10.
Available at: https://www.pmc.gov.au/sites/default/files/publications/australian-government-data-sharing-release-legislation_issues-paper.pdf

O'Brien, J. Asylum seekers invited by OAIC to speak about data breach. 25 January 2018. CIO.
Available at: https://www.cio.com.au/article/632576/asylum-seekers-invited-by-oaic-speak-about-data-breach/

Powell, J. PPPs and SDGs : Don't Believe The Hype! Public Services International Research Unit. June 2016.
Available at: https://gala.gre.ac.uk/id/eprint/16843/7/16843%20POWELL_PPPs_and_the_SDGs_2016.pdf

Privacy Act 1988 (Commonwealth of Australia)

Privacy Amendment (Notifiable Data Breaches) Act 2017 (Commonwealth of Australia)

Privacy and Data Protection Act 2014 (Victoria)

Public Sector (Data Sharing) Act 2016 (South Australia)

Privacy and Data Protection Act 2014 (Victoria)

Safety by Design Resources. eSafety Commissioner.
Available at: https://www.esafety.gov.au/esafety-information/safety-by-design

State of Digital Rights. Digital Rights Watch. May 2018.
Available at: https://digitalrightswatch.org.au/wp-content/uploads/2018/05/State-of-Digital-Rights-Web.pdf

THE CONFIDENTIALITY INFORMATION SERIES (1160.0). Australian Bureau of Statistics. August 2017.
Available at:
https://www.abs.gov.au/ausstats/abs@.nsf/Latestproducts/1160.0Main%20Features1Aug%202017?opendocument&tabname=Summary&prodno=1160.0&issue=Aug%202017&num=&view=

*Victorian Data Sharing Act 2017 (*Victoria)

WORK VOICE PAY: Draft New Technology Agreement. UNITE. October 2017.
Available at: https://unitetheunion.org/media/1236/draft-new-technology-agreement-october-2016.pdf

Yosufzai, R. Thousands of Australians hit by private health insurance data breach. SBS News. 17 July 2017.
Available at: https://www.sbs.com.au/news/thousands-of-australians-hit-by-private-health-insurance-data-breach

5 Step Action Plan. Office of the Victorian Information Commissioner. Available at:
https://ovic.vic.gov.au/resource/5-step-action-plan/