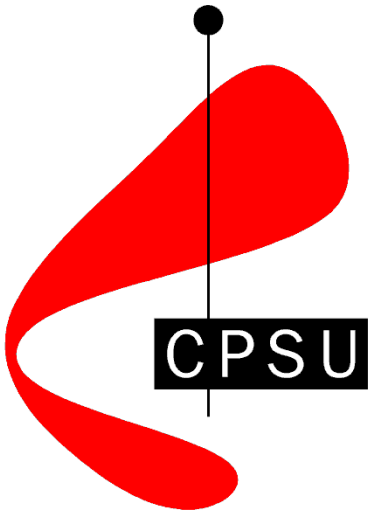

CPSU (PSU Group)

Disclosure of public servants' names and contact details – Discussion paper

August 2019

Summary of the CPSU view

The current FOI Guidelines provide, at Part 6, that:

> "W*here public servants' personal information is included in a document because of their usual duties or responsibilities, it would not be unreasonable to disclose unless special circumstances existed. This is because the information would reveal only that the public servant was performing their public duties."*

The CPSU reads this section of the guidelines as establishing a general disposition towards the release of public servant names and details except where special circumstances exist.

The CPSU submits that both the general disposition, and the understanding of what would constitute special circumstances, needs to be reconsidered in light of a number of factors including:

- the changing information access landscape and social media platforms;
- online abuse and media shaming as a work health and safety risk; and
- concerns about client aggression.

The CPSU submits that tighter guidelines about the release of public servant names and contact details would not hamper the proper functioning and intent of the FOI regime.

The CPSU notes that the object of the FOI Act is not about holding individual public servants up to scrutiny and making them individually accountable to the public.

Currently, in a range of agencies such as Child Support or those involved in intelligence, investigations, compliance or criminal work, staff are not identified due to safety or operational reasons. We would be concerned about any move towards reducing the protections already in place and widely used across the public service.

1. Purpose of the FOI Act

The object of the FOI Act is not about holding individual public servants up to scrutiny and making them individually accountable to the public. Mechanisms dealing with the obligations and accountability of public servants are already provided for in the *Public Service Act 1999* and the *Public Service Regulations 1999*.

The objects of the FOI Act are to promote Australia's representative democracy by allowing the public to be better informed and better participate in government processes. It does this by requiring agencies to publish information and by providing access to documents on request. The CPSU argues that these objects can be met without necessarily releasing the names or contact details of officers in most positions across the APS.

The Act is also designed to increase scrutiny, discussion and review of Government processes *as a whole* in order to make the Government more accountable in its operations and ensure that information held by the government is managed for public purposes as a public resource. The CPSU seeks further clarification from the OAIC as to how the inclusion of the personal information of individual public servants increases scrutiny, discussion and review of Government processes as a whole.

Further evidence of the principle that individual public servants should not be individually accountable to the public can be found in the Legal Services Directions 2017.[1] Appendix E of the Directions provide that Government employees will generally be indemnified for costs and damages in relation to any civil or criminal suit that arises from the employee acting reasonably and responsibly in the course of their duties.

2. Information access landscape and social media

The CPSU believes that the FOI Guidelines need to be reconsidered in light of an information access landscape where there is a growing amount of personal information available online, and a greatly increased search online capacity – in particular that provided by social media platforms.

Public servants will have personal social media accounts and the various accumulated online data and references that are part and parcel of modern life. There is also the de facto expectation on many employees that they will participate in platforms such as LinkedIn, used by the APS to advertise vacancies, which list educational and employment histories, and professional and personal networks.

The issue that arises is that the release of a public servants names, and more so their name and contact details, can provide an FOI applicant with the ability to conduct social media and online searches which could produce access to personal information about the public servant that was not held by the Department or if it was would never be released under the FOI provisions.

The amount of information online, and the access to powerful search tools, makes it far easier than ever before for private interests to compile dossiers of information on individuals from various sources, including their personal life, and put that information to uses that extend beyond the purposes of the FOI Act.

The recent case of the Adani mining companies attempted use of FOI to obtain the names of public sector scientists is an example of the risks public servants face and which must be considered by FOI guidelines. It was reported in the media that Adani's legal advisors prepared an "attack dog strategy" to 'wage war", suggesting that Adani "not settle for government departments dragging out decisions — use the legal system to pressure decisionmakers".[2]

The law firm advised their client that "social media is a tool to use against activists and decisionmakers", and to "Look for evidence of bias and use it to show the court system is being used for political activism."

If that strategy had been put into practice against the public sector scientists, those officers could have been subject to intensive online searches to establish a list of colleagues, friends, family, acquaintances and then each of those similarly investigated to find material that could be used in court, the media, online and elsewhere to seek to discredit the professional judgment, competence and integrity of the officers concerned.

---

[1] Australian Government (2018, 1 July). Legal Services Directions 2017. Federal Register of Legislation. Retrieved from https://www.legislation.gov.au/Details/F2018C00409

[2] Josh Robertson (2019, 19 February). Adani's new law firm put forward 'trained attack dog' strategy for waging legal 'war'. ABC News. Retrieved from https://www.abc.net.au/news/2019-02-19/adani-law-firm-put-forward-trained-attack-dog-strategy/10821470

Attempting to discredit the work or standing of a public servant is not a new tactic for persons by aggrieved by a decision, or those with commercial, political or personal motivations. There are FOI exemptions available and Departments and agencies have generally established practices around protecting sensitive work and the officers who perform that work. Adani was rightly denied access to the information it sought.

What is new is the extent of the risk. The risk arises in any number of cases - where government policy or public service work is highly controversial or subject to heated and polarised political campaigning, or where there are aggrieved citizens, or those pursuing commercial or other motives. Therefore, the risk should now be considered to extend beyond the officers and work types that have traditionally been protected from identification.

3. Online abuse and media shaming as a work health and safety risk

The disclosures of names and contact details need to balance privacy, health and safety with transparency and accountability.

And that balance needs to take into consideration the notable change in the tone and content of political and public discourse. Personal attacks, doxxing, trolling, and aggression are on the rise.

The work of public servants, for example, in the ABC and climate science and policy, is subject to concerted hostile media and political campaigns. This creates the concerns for workers that they may find themselves the subject of very adverse media reporting or online campaigning – or worse.

CPSU members in a number of Departments and agencies, in particular, where there is some degree of public controversy around government policy and/or the work of the agency, report to the CPSU that they hold concerns about being identified online by various campaigns and then subject to abuse, invasions of privacy or other threats.

Employers have a duty of care to protect the health and safety of employees. The duty extends to assessing and managing the risks of exposing employees to abuse, public attack or invasions of privacy. The administration of FOI requests should form part of that risk assessment and management.

However, it is not clear to the CPSU that the current guidelines are adequate for that purpose.

While the guidelines deal with an officer's physical safety being endangered, and exemptions are available under 37(1)(c), there appears to be no reference to the type of risks described above.

This is also a problem at an agency level where attention is paid to physical safety risks but insufficient attention to other risks. The *ATO's Practice Statement*[3] *on releasing employee names* is a case in point.[3] It states that:

> '*You may claim an exemption if the disclosure of information would endanger the life or physical safety of an officer".*

The statement then provides sound advice on when the exemption should be applied:

[3] Australian Taxation Office (2018, 6 July). Practice Statement Law Administration. Retrieved from https://www.ato.gov.au/law/view/document?locid=%27PSR/PS20056/NAT/ATO%27#LawTimeLine

"You do not need to wait for each individual to suffer actual threats of harm from the applicant. It is sufficient to exempt names if there has been:

- *a threat of harm to others working in a similar way*
- *a threat of harm to others after a disclosure of similar information*
- *if there is a real possibility that harm is a consequence of disclosure judging from the attributes of the person making the request (for example, if they have a history of violent or threatening behaviour)."*

However, the statement then says the *"the threat of verbal abuse is not sufficient" and is silent on the types of risks described above.*

The ATO Practice Statement may be an accurate statement of the FOI law but it not consistent with work health and safety requirements, and out of touch with the emerging risks of online abuse and media shaming.

The CPSU therefore suggests that stronger and clearer guidance could be given around the risks of public attacks, abuse and privacy invasion – and perhaps that could include access to exemptions under 47E and 47F.

4. Personal safety

Currently, in a range of agencies such as Child Support or those involved in intelligence, investigations, compliance or criminal work, staff are not identified due to safety reasons.

There are also risks in other agencies, including in the Courts. Client aggression in Centrelink workplaces has been a well documented problem, and there are new concerns for CPSU members in DHS where the screen capture of client information creates a new category of document obtainable under FOI and which contains the name and details of the officer.

Elsewhere, security at the ABC has been increased, and CPSU science members report that they too now have to give consideration to their personal security.

We would therefore be greatly concerned about any move towards reducing the protections already in place and widely used across the public service.

- End.