Australian Government

Department of Employment, Skills, Small and Family Business

Submission on the disclosure of staff names and contact details

July 2019

Contents

1. Introduction

The Department of Employment, Skills, Family and Small Business (**the department**) welcomes the opportunity to provide the Office of the Australian Information Commissioner (**OAIC**) with a submission on the Discussion Paper, *Disclosing public servants' names and contact details* (**the Discussion Paper**). The department's submission has been developed with reference to the consultation questions contained in the Discussion Paper.

It is clear that our freedom of information (**FOI**) processing landscape has changed and continues to evolve with technological advancements. Widespread ownership of internet enabled devices such as smart phones, watches, tablets and laptops mean easy and constant access, sharing and publishing of information[1]. Once information is released publicly, the department has little to no control over its subsequent dissemination and use. Additionally, there are many readily available tools to enable a member of the public to easily find, collate and reconstruct personal information using the name and contact details.

The transforming technological environment has influenced the department's approach to the release of staff[2] names and contact details in response to FOI requests. In particular, release of staff names and contact details in this context has the potential to create work, health and safety (**WHS**) risks for staff. While the majority of FOI applicants have no interest in staff names and contact details, there are instances of FOI applicants who are particularly interested in this information, signalling a cause for concern. Technology advancements combined with the large amount of publicly available information, can easily allow a motivated person to misuse staff names and contact details. This has the potential to cause direct harm to staff and negatively impact on the effectiveness and efficiency of the department's operations, intentionally or otherwise. Considering the consequences for staff and the department, the preference of the department would be not to disclose staff names below the SES level, unless directly related to the FOI request and appropriate for release. A reference to staff includes reference to staff of contracted service providers, where relevant.

2. Concerns

The department's main concerns about the release of staff names and contact details include:

- staff safety (section 2.1);
- impact on the department's efficiency (section 2.2);
- online conduct (section 2.3); and
- identity theft (section 2.4).

In the context of the department's operations, these concerns may arise when FOI applicants request documents which:

[1] According to the 2018 Yellow Social Media Report (page 5), on average, people own 3.5 internet enabled devices. We also use the internet more than five times a day. [online]: https://www.yellow.com.au/wp-content/uploads/2018/06/Yellow-Social-Media-Report-2018-Consumer.pdf

[2] A reference to staff includes a reference to staff of contracted employment services providers, where relevant.

- involve ‘frontline’ staff, including the National Customer Service Line (**NCSL**) who handle calls from the public concerning employment programs;
- relate to compliance activities including audit, fraud and staff investigations;
- contain information on matters that are currently in the media and are driven by individuals with particular agendas; and
- involve staff of contracted employment services providers, who operate to deliver employment programs on the department’s behalf.

2.1 Staff safety

The department has an obligation to ensure the WHS of staff. As a service delivery agency, staff – particularly frontline staff – can be subjected to inappropriate or escalating behaviour from clients. This may result in clients making unsolicited calls or visits to departmental offices, often displaying difficult behaviours.

The department considers that the release of staff names and contact details creates an elevated risk to staff safety. The nature of an FOI applicant’s previous interactions with this department (or other departments) may indicate a potential for concern, however, there are not always clear indicators of an impending safety risk to staff. Confidential [redacted]

In a digital age, minimal information can enable a motivated person to further identify staff and misuse staff names and contact details, and sophisticated search engines easily enable tracking of digital footprints. The risks to staff are exacerbated by the speed and ease with which further and potentially more sensitive information about the staff member can be obtained online.

Furthermore, potential WHS risks are compounded in smaller localities and regional locations with low populations, which increase the risk that disclosure of information could lead to easier identification and inappropriate access to, and contact with, staff.

2.2 Impact on the department’s efficiency

Disclosure of full names of staff generally allows official email addresses to be established.

Inefficiency

Members of the public circumventing established communication channels because they have access to a particular staff member’s details can lead to significant inefficiencies for the department, including:

- more time spent by staff reviewing and actioning unsolicited emails and phone calls at the expense of time spent performing their duties; and
- delayed outcomes for the client where the targeted staff member has not actioned emails and voicemails due to absences; a change of roles and responsibilities; or where emails are overlooked, misdirected or undelivered.

The department has established processes and channels for communications with clients to enable the department to efficiently manage resources and maximise productivity. Continuing resource pressures on the department, and the public service more broadly, necessitates an even greater impetus to ensure efficient operations.

Inappropriate contact with staff

The identification of official email addresses increases the likelihood of staff being subjected to inappropriate or obsessive correspondence. Correspondence of this nature has the potential to affect a staff member's mental health, impact performance, lead to extended periods of personal leave and result in workers' compensation claims against the Commonwealth.

Confidential [redacted]

Attracting and retaining skilled staff

As a practical matter, staff and prospective staff will contemplate the risks associated with a work environment. Potential exposure to personalised contact from members of the public with difficult behaviours can be a factor in their employment decisions and potentially affect the ability of the Commonwealth and its service providers to attract and retain staff.

2.3 Online conduct

Considering the widespread ownership of internet enabled devices and the frequency of online communications, the department has further concerns about the potential for a motivated person to pursue staff via online social media platforms and other mechanisms. Inappropriate online conduct could have a negative impact on a staff member, which would be challenging for the staff member and the department to rectify.

While the department is not aware of any specific instances where this has occurred, a recent survey undertaken by the Australia Institute on online harassment and cyberbullying[3] shows there is reason for concern. The Australia Institute reported that:

- 39% of respondents said they had experienced online harassment[4]. Among other things, the harassment included online publication of their personal details to intimidate them (5%), deliberate attempts to damage their work reputation (4%) and inciting others to stalk or threaten the person in real life (3%)[5].
- 8% of respondents reported that they had experienced cyber hate[6]. For the purpose of the survey, cyber hate was defined as 'repeated, sustained threats or attacks on an individual through the use of electronic devices, which result in real-life harm to the target. These harms may be physical and/or psychological. The attacks may be perpetrated by one or more individuals'[7].

[3] The Australia Institute, Trolls and Polls – The economic costs of online harassment and cyberhate. January 2019
[4] Ibid, p. 2.
[5] Ibid, p. 1.
[6] Ibid, p. 7.
[7] Ibid, p. 7.

- 28% of respondents who indicated negative impacts on their wellbeing said the experience caused them to see a doctor, psychologist or other health professional and affected their ability to work[8].

While there are legal avenues available to address such online conduct, the financial (and emotional) cost can be significant.

2.4 Identify theft

The department is concerned about the potential for identity theft if staff names and contact details are disclosed. In particular, where it also includes staff signatures.

Identity theft methods are becoming increasingly creative in how other personal information is obtained using names and contact details of individuals. Often a victim will not become aware that their personal information has been misused until losses are incurred. The impact of identity theft can be damaging, resulting in financial loss, emotional distress and negatively affecting an individual's personal credit rating. Serious cases of identity theft often result in advice for the affected individual to initiate a legal name change, causing further emotional distress.

3. Balancing accountability and transparency of government decision-making against WHS considerations

The department acknowledges that subsection 3(2) of the FOI Act provides that the Parliament intends, by the objects set out in the section, to promote Australia's representative democracy by contributing towards the following:

- increasing public participation in government processes, with a view to promoting better informed decision-making; and
- increasing scrutiny, discussion, comment and review of the government's activities.

The importance of accountability and transparency in government decision making is not significantly improved by the release of low-level staff names and contact details. This is because in most cases, the identity of individual staff is immaterial, and the decision is not reflective of the individual staff member's views, but the views of the department.

While there is some merit to the argument that release of the name of a decision maker will assist an FOI applicant to assert, during a review process, conflict of interest or bias in a decision that affects that applicant, these instances are rare. In the context of decision letters, disclosing the decision maker's title, position, business area and the name of the department should be sufficient to meet accountability and transparency requirements of government decisions. Any public benefit to going further appears to be outweighed by the WHS impact on individual staff's health and safety, and government resources used to protect its staff.

[8] Ibid, p. 9.

4. FOI applicants' interest in staff names and contact details

The department has found that many FOI applicants will expressly exclude third party names and contact details from the scope of their request or when excluded through an exemption, do not challenge the exemption under the FOI legislation.

There are a number of Commonwealth agencies who have adopted the approach of advising FOI applicants that, in accordance with section 22 of the FOI Act, names, position titles and contact details of staff members will be removed, unless advised otherwise. Generally, there have been no objections by FOI applicants to this approach.

The department treats staff names and contact details as irrelevant where it is clear from the request that this information is out of scope or the FOI applicant has excluded this information. This may arise following informal consultation with the FOI applicant to clarify scope or following a formal consultation process under the FOI legislation. The department considers whether 'special circumstances' exist to support an exemption claim under section 47F (personal Information) or section 47E(d) (operations of an agency) of the FOI Act where an FOI applicant is particularly interested in staff names and contact details. Similarly, this approach is taken in circumstances where it has come to the department's attention that an FOI applicant has been violent or aggressive towards contracted service providers or other agencies.

5. The FOI Guidelines

The current FOI Guidelines provide that it would not be unreasonable to disclose public servants' personal information because of their usual duties or responsibilities, unless special circumstances exist. This is because the information would reveal only that the public servant was performing their public duties. Personal information referred to in this part of the FOI Guidelines includes a public servant's name, work email address, position or title, contact details, decisions or opinions.

The FOI Guidelines, in relation to disclosure of public servants' names and contact details during the performance of their usual course of duties or responsibilities, do not take into account technological advances and social platforms, which can result in access to public servants' personal and financial information. This access to personal information and financial information can expose a public servant to harm and detriment. Therefore, the department's preferred position is that it not be required to disclose staff names and contact details below the SES level in response to FOI applications.

However, if this position is not supported by OAIC, then it would be useful if the FOI Guidelines could recognise the WHS risks posed in releasing staff names and contact details, including the inherent difficulty in being able to predict which applicant (or their associate) might misuse those details.

Additionally, the FOI Guidelines should identify factors that the agency may consider when assessing whether the disclosure may be reasonable in those circumstances.

Some relevant factors might include:

- anonymous FOI requests

- the nature of the FOI applicant's previous interaction with the agency
- the style of writing used in the FOI request
- inherent risks associated with the department's functions and operating environment
- the nature of the FOI applicant's online activities
- staff locality
- the views of staff involved.

6. Conclusion

In a digital age, there is a real potential for staff names and contact details, released in response to an FOI request, to be misused. This can have significant consequences for staff, the department and more broadly, other Commonwealth agencies. Accordingly, the department considers it appropriate to adopt a more cautious approach to the release of staff names and contact details.

The department's preferred position is that it not be required to disclose staff names and contact details below the SES level in response to FOI applications in order to appropriately balance its need to protect the health and safety of staff against the need to ensure transparency and accountability.