Australian Government
Department of Home Affairs

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

Submission by Department of Home Affairs

Response to Office of the Australian Information Commissioner

Introduction

The Department of Home Affairs, including Australian Border Force (the Department) provides the following submission to the Office of the Australian Information Commissioner in response to the discussion paper on the disclosure of public servants' names and contact details through the Freedom of Information (FOI) process.

The Home Affairs portfolio, which includes the Australian Federal Police (AFP), Australian Criminal Intelligence Commission (ACIC), Austrac, Australian Security and Intelligence Organisation (ASIO) and the Department, brings together a number of different agencies and functions with differing security threat profiles, to deliver critical roles in the Government's commitment to a prosperous, secure and united Australia. The portfolio is responsible for a centrally coordinated strategy and policy leadership in relation to domestic and national security arrangements, law enforcement, counter-terrorism, social cohesion, the protection of our sovereignty, integrity of our border and the resilience of our national infrastructure. The Department also delivers services that strengthen the cohesiveness of Australian society through our migration program.

Access to information held by government is fundamental to open, transparent and accountable representative democracy and it is these principles among many, that the Home Affairs portfolio seeks to protect.

Submission

Australia faces a complex and evolving threat environment and the Home Affairs portfolio is at the forefront of the Government's response. Our skilled and committed staff are our greatest resource and the protection of personnel is amongst our paramount concerns.

When considering if public servants' names and contact details should be redacted as part of the FOI request process, the objects of the *Freedom of Information Act 1982* (the FOI Act) and supporting guidelines issued by the Australian Information Commissioner are considerations which must be balanced with the obligations under the *Work Health and Safety Act 2011* (WHS Act). The WHS Act aims to protect workers and other persons against harm to their physical and mental health, safety and welfare through the elimination or minimisation of risks arising in the work place. Meeting the Department's obligations under the WHS Act may be unnecessarily complicated by a disclosure of a worker's name, contact details or other identifying information even where that disclosure is authorised by law. Following the disclosure of identifying information, public scrutiny or criticism of a worker's actions, including through "trolling", harassment or unlawful antisocial behaviour, can lead to physical or mental harm to that worker or others. This may lead to legal and/or compensation claims from those that consider they have been put at risk by the Commonwealth's actions.

With the increasing risk profile of the portfolio responsibilities, alongside the rapid progress of technology, it is essential to acknowledge the risks associated with the ease that information can be accessed, redistributed and manipulated for purposes other than the original intent.

While the portfolio agencies protect their personnel through differing means, the overarching principle is to ensure staff who would not otherwise be subject to unrestricted exposure of their identity as part of their usual duties, are protected from potential repercussions for the lawful work they undertake on behalf of the public.

Given the wide remit of the Home Affairs portfolio in security and law enforcement, it is our submission that there is a demonstrable risk of harm arising from the general release of staff names and contact details.

A practice that involves the redaction of staff names and contact details other than in exceptional circumstances, and which does not otherwise affect the release of documents generally, is not inconsistent or incompatible with the object and spirit of the FOI Act. While accountability is an important part of government administration, the general disclosure of staff names and contact details would not advance the public interest in government transparency or integrity.

Discussion

1. Does your agency have concerns about releasing the names and contact details of staff in response to FOI requests? If so, what are your concerns? Has your agency experienced any specific work health and safety issues as a result of a person's name or contact details being released in response to an FOI request?

In the normal conduct of duties, workers employed across the Home Affairs portfolio have access to privileged, classified, sensitive or other valuable information and may be in positions requiring them to make decisions that may be controversial or at risk of manipulation for personal gain. The release of workers names in connection with such matters may resonate with disgruntled members of the public, activist groups or those with nefarious intent resulting in the risk of staff being exposed to harassment, reprisals, coercion, bribery or blackmail.

The following incidents highlight both the environment that departmental workers are exposed to, the need to protect their identity and the lengths that individuals will go to in locating individual staff.

a) Following the release of a staff member's name into the public, the staff member became the target of hate emails. The harassment escalated with the staff member's name being published on websites, including a partially pixelated photo of the staff member, his address and *google maps* images of his home. As a result, security assessments of his home were undertaken, the staff member, his wife and children were briefed by the AFP and a security system with a back-to-base alarm was installed in their home. Further investigations were conducted in regards to the pixilated photo published on the website, revealing it was a photo of the staff member and his children on a family holiday. The family discovered an unknown person linked to the son's *Instagram* account where the photo had been published. This example demonstrates the efforts some parties will pursue to intimidate, threaten or cause harm to departmental staff and their families and is one of several incidents resulting in the Department installing security systems in staff residences.

b) A staff member's partner found threatening notes in their private residence letterbox. The notes identified that the writer was aware that there were children in the family. The notes included assertions that the writer and their associates considered the staff member was personally responsible for the torturing of individuals in Regional Processing Centres. Security measures were immediately implemented, however, the Department cannot remove any claimed harm suffered by the partner and family who received these notes. The resultant stress to their family had a lasting effect and the staff member felt the need to leave the Department and the APS.

c) A person of interest searched Facebook using the first name and the surname of a cancellation case officer. The search returned the details of five individuals. The person contacted each of the individuals asking them if they worked for the Department. Four out of the five responded 'no', leaving only one probable match. The person of interest then obtained the phone number and address of the officer and showed up at their private residence to argue their visa outcome.

d) Following release of documents under FOI, staff named within these documents were the subject of adverse and threatening comments in the media, social media and by email. In at least one case, there was a serious impact on a staff member's family.

2. Have your agency's views on this issue changed over time? If so, please describe any factors that have affected your agency's approach, including technological, environmental or legal factors.

With the progress of technology, the information world is a vastly different environment to when the FOI Act was drafted in the early 1980s. The ability to collect information and track individuals surpasses anything previously seen in history. The rapid growth of the internet and the proliferation of social media tools, together with powerful and publically available search engines significantly increases the ease with which an individual's privacy can be compromised from relatively little information through a mosaic effect that occurs when seemingly innocuous pieces of information are combined to create a bigger picture. Workers are increasingly reluctant to include personal details in signature blocks on correspondence, as small pieces of information can be assembled like a puzzle to reasonably establish the full details of a worker, as demonstrated in the examples above.

The Department has witnessed the increasing trend of documents released under FOI being shared online, resulting in the names of workers that may be known to an individual client becoming more broadly known to the public, even though they are not easily found on any other publically accessible sources as employees of the Department.

The ease with which information can be published without controls has been witnessed when screen shots from a departmental system released through FOI requests have been routinely shared on an online forum discussing Australian citizenship processing times.

The Department has no ability to control the sharing of workers' details once released under FOI. For example, the Department has concerns about a Facebook discussion group comprising of members who have had their visas cancelled on character grounds. There is no means to prevent such a group sharing information released under FOI or publishing the information on the internet and in example (a) above. The anonymity of social media and keyboard commentators does not lessen the damage to individuals' health and wellbeing from negative and abusive commentary.

Staff have a right to use Social Media in their private lives without feeling the impact of their working arrangements. To reduce risks staff are asked to refrain from identifying as a Department employee. Nonetheless, if their details are published under FOI, it can intrude negatively into their private life, that of their family and friends, affecting their health and wellbeing. This has the potential to damage the reputation of the Department as an employer.

The nature of the portfolio has changed substantially in recent years expanding to become a law enforcement agency. Subsequently, the release of staff names and other identifying information exposes workers to targeting by malicious groups seeking to access information or systems for the purposes of circumventing laws and controls or activists seeking influence. Such gathering of information exposes portfolio employees, their families, friends, and associates to the risk of grooming, making them susceptible to corruption or bribery.

There are several incidents noted and investigated by the Department's Integrity and Professionals Standards Branch, where criminal organisations have attempted to infiltrate the ABF via the corruption of individuals. The naming and publication of ABF officer's details enables easier access to the ABF employees. Organised crime gangs remain active in their attempts to corrupt individuals.

As the portfolio's risk profile increases, so too does the potential for more frequent and severe security incidents. An upward trend in the number of reported security events relating to threats to departmental workers, with 40 reported incidents in 2016-17, 46 in 2017-18 and 70 in 2018-19 evidences the changing and increasing profile of incidents. These incidents include aggressive behaviour towards staff, assault of a staff member, and harassment/intimidation of staff.

The Department has observed in the detention environment, that the likelihood of grooming or threatening behaviour towards staff and service providers has increased. This is as a result of the change in cohort from predominantly Illegal Maritime Arrivals (IMAs) to persons whose visas have been cancelled on character

grounds (following criminal behaviour) under section 501 of the *Migration Act 1958* (the Migration Act). Incidents include the publishing of a female medical provider's (doctor) photo by a detainee in an Immigration Detention Centre. The detainee disagreed with the medication dispensed to him on one particular day. Whilst the medication was correct (following review of the situation), the doctor received considerable vexatious and alarming threats, including from doctors who had never treated or had access to the detainee.

3. Does your agency advise staff, including contractors undertaking functions on behalf of the agency, that names and contact details may be released in response to an FOI request as part of your agency's training and induction programs?

The Department provides FOI awareness training for staff including an overview of the FOI Act and departmental processes. Staff are advised that generally staff names are disclosed if their details are recorded in the normal course of their public service duties.

The Department notes the concerns from the current contracted health services providers in the detention network who are aware staff names may be released and they submit:

> *In addition to being an unreasonable disclosure of personal information, (service provider) remain concerned that public release of (service provider) staff personal information could pose a risk to their physical safety. We have seen previous instances of threats against staff where their information has been placed on publicly available websites. (Service provider) strongly supports continued redaction of its staff's names and contact details in any FOI release.*

Workers are aware that their names may be released increasing concerns for their health and safety. The Department is addressing any impact these concerns may be having on the quality and efficiency of operations including reporting incidents in the detention network due to fear that their details will later be released to the subject of the report, as observed in example (b) above.

4. How do you balance work health and safety considerations with the objects of the FOI Act, which include 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 Department operates under the framework in the WHS Act and *Work Health and Safety Regulations 2011* to ensure the health and safety of workers. To meet these obligations, the Department must ensure, so far as is reasonably practicable, the physical and mental health and safety of workers and others through the elimination or minimisation of risks arising from the work place. The Department is equally committed to meeting its obligations under the FOI Act to provide members of the public with access to information the Department holds.

The Department is of the view that in relation to the majority of FOI requests it receives the names and details of staff are irrelevant. In these cases, including the 90% of requests that are for access to personal files, applicants are advised:

> '*It is the Department's policy to consider irrelevant to the scope of a request the personal details of staff engaged in some roles. This includes their names, direct email addresses and also the mobile and direct work telephone numbers of these staff. This material will be removed under s 22 (1)(a)(ii) of the FOI Act from the documents that form the scope of the request. If you require names and contact details of these staff, please inform us so the decision maker may consider your request (within seven days from the date of this letter). Otherwise we will take it that you agree to that information being excluded from the scope of your request.*'

In cases where the applicant objects to the redaction of the names and contact details or where it is clear that names and details are within the scope of the request, documents are assessed under the provisions of the FOI Act and are released or exempted accordingly.

In considering the balance between WHS obligations and the application of the FOI Act, decision makers evaluate whether there are grounds that a risk may be realised. Decision makers, at first instance, assess whether the disclosure of the information, alone or in conjunction with other material, could reasonably be expected to enable a person to ascertain the identity of an individual or existence of a confidential source and then exemptions are appropriately considered.

The Department recognises that where staff names and details are within the scope of a request, it cannot redact these details by default and the legislation limits the ability to exempt material without qualified grounds. This threshold is quite stringent requiring a demonstrated history of a threat to staff or conducting malevolent criminal acts specifically directed toward departmental staff for an exemption to be considered. When giving consideration to the release or protection of a worker's details, the decision makers must give due consideration to:

- protect the privacy, safety and wellbeing of officers and their families, noting the prevalence of social media and the ability to locate personal information on social media and across the internet;
- the right of staff to hold a social media profile and not to 'hide' in the community;
- ensure that officers are not targeted or groomed by criminal organisations; and
- maintain the Department's investigative and operational integrity.

5. If your agency considers that disclosure of a public servant's name or contact details will negatively impact their health or safety, what evidence do you require before deciding that their name or contact details are exempt from disclosure?

The FOI Guidelines acknowledge that in some circumstances the disclosure of public servants' names may be unreasonable; 6.154 of the FOI Guidelines states that '*an agency needs to identify the special circumstances which exist rather than start from the assumption that such information is exempt*'.

In light of the risks set out above, the Department has identified that special circumstances exist for non-SES staff and contractors working in certain business areas with high risk cohorts and considers that the names and contact details of these staff should be exempted, assuming they in fact relevant in the first place:

- Employees of contracted service providers, i.e. SERCO staff at immigration detention centres, International Health and Medical Services (IHMS), and BUPA
- Australian Border Force officers
- Non-SES staff working within fields such as Visa refusals and cancellations, Intelligence, Investigations, Integrity and Professional Standards, Identity, Status Resolution, and Medical Transfers
- Non-SES staff from business areas that are referring complex/high risk clients for any of the above
- Non-SES staff and Locally Engaged Employees undertaking integrity work offshore
- Locally Engaged Employees undertaking any work at overseas posts

The Department's National Character Consideration Centre (NCCC), conducts assessments which may have a significant effect on someone's life, such as being removed from Australia. As the individuals who are the subject of such assessment often have criminal records or affiliations with organisations such as outlaw motor cycle gangs or terrorist groups, protecting the identity of staff who manage the cancellation and refusal of visas is essential. As such, the Department has implemented a policy with broader protections to not disclose any names associated with this workload, similar to the above, but applies to <u>all</u> staff names and

details, regardless of their business areas. This policy also applies to departmental contractors and agencies consulted in the execution of duties related to section 501 of the Migration Act.

The Department is aware that 3.54 of the FOI Guidelines states '*There is no apparent logical basis for treating the names of SES officials as being within the scope of a request, but other officials as being irrelevant to the request*'. The Department notes that in *The Australian and DIBP* [2017] AICmr62, the Information Commissioner made the case that the names of public servants who are generally expected to engage publically as part of their normal duties are not subject to redaction unless there is a specific or possible risks to personal safety to the officer. As SES are generally expected to be publically listed as part of their normal duties, i.e. in the Government Directory, the redaction of their details would only be considered where there is a real and imminent risk of harm.

The Department submits that the publication of direct contact numbers including mobile numbers has the capacity to:

a) Require the Department to cancel mobile phone numbers that are published to reduce the risk of individuals receiving phone calls and the consequent disruption of operations or security breaches.

b) Phone numbers, mobile or otherwise, may be allocated across a team and do not 'belong' to an individual, making publication irrelevant.

c) Mobile numbers may be the private number of individuals and the Department will become accountable for the reparation if publication creates risk to an individual.

The Department refers to *Coulson v Department of Premier and Cabinet (Review and Regulation)* [2018] VCAT 229 (20 February 2018), and while relevant to Victorian FOI legislation, the Tribunal found that it would be unreasonable to disclose the names, initials, signatures and email addresses of non-executive public servants, in circumstances where they were implementing directions for which they were not the decision-makers. The Department takes a similar view for NCCC staff who are not delegated decision-makers, but who are tasked with informing clients of the outcome of their assessment under character legislation.

6. Do you consider the FOI Guidelines provide enough guidance for agencies when considering these issues?

Despite the progress of technology and changes in the global socio-economic community increasing the risk to workers following the release of their identity, the FOI Act has not evolved to keep pace with these changes, failing to afford workers the protection necessary to allow them to fulfil their duties and live their private life separate to their employment. To address this gap, it is necessary to review the interpretation of the provisions of the legislation and suitably modernise the FOI Guidelines through a global lens that views the impact of information disclosure on individuals' rights to privacy and protection.

The FOI Guidelines are insufficient to resolve the contradiction on the issue of disclosing staff names and contact details. As evidenced by the cases listed below, the Department recommends that the FOI Guidelines need to be updated to provide more guidance to agencies.

In *Bartucciotto and Commissioner for Complaints* [2006] AATA 36 (17 January 2006), the Tribunal considered it would not be unreasonable to disclose the names of staff but that it would be unreasonable to disclose the email addresses of those staff. Once a staff member's name is disclosed it is not difficult to determine their email address or in fact to find a contact number at their work locations or their private address.

The Department notes that in *PO and AFP* [2018] AICmr 72, the Information Commissioner specifically stated that s.22 of the FOI Act requires consideration of the scope of the individual request and should not be applied as a blanket policy. However, in *Price and Attorney General's Department (Freedom of*

Information) [2016] AATA 1044 (20 December 2016), the Tribunal found that disclosing the surnames, signatures, email addresses and user IDs of staff would be contrary to the public interest, noting the potential for harm given the nature of the agency's role. Furthermore, in *Mond v Department of Justice (General)* [2005] VCAT 2817 (22 December 2005), and although relevant to Victorian FOI legislation, the Department notes that the Tribunal found it would not be reasonable to disclose the signatures, hand-written initials or contact telephone numbers of staff who are not usually available to speak to members of the public.

7. In what circumstances do you consider that a public servant's personal information (name and contact details) are irrelevant to the FOI request?

As noted in question 4, for the requests seeking access to personal files (90% of all requests), applicants are advised that personal details of staff are considered irrelevant to the request unless otherwise advised to the contrary.

The Department considers the names and contact details of public servants are irrelevant as such details do not generally promote the objectives of the FOI Act. The Department notes that the increased participation in Government processes and increased scrutiny and discussion of Government activities can often be met without applicants knowing the names and contact details of individual staff members:

- Employees of contracted service providers at immigration detention and regional processing centres
- Australian Border Force officers
- Non-SES staff working within fields such as Visa refusals and cancellations, Intelligence, Investigations, Integrity and Professional Standards, Identity, Status Resolution, Regional Processing and Medical Transfers
- Non-SES staff from business areas that are referring complex/high risk clients for any of the above
- Non-SES staff and Locally Engaged Employees undertaking integrity work offshore
- Locally Engaged Employees undertaking any work at overseas posts
- Workers, service providers and other agencies associated with cases decided by the NCC

8. Where you have withheld the names and contact details of public servants, what impact does deleting this information from documents have on the time it takes to process FOI requests?

When the Department began redacting names and contact details of public servants, the Department experienced a temporary increase to FOI processing times while staff adapted to new processes. As the new practices have become embedded in routine and staff capabilities increase, processing times have decreased.

When implementing this policy the Department has taken steps to mitigate any increase to processing times such as applying s22(1) to redact staff names and notifying applicants of the process up front, removing the need for the decision makers to commit time to preparing lengthy decision notifications.

Where appropriate, the Department encourages staff to use their position numbers (not exempt) rather than names in correspondence and to send emails from group inboxes rather than their individual email address. Such measures not only support protecting workers' identities, they will serve to reduce the impact on FOI staff when assessing documents.