25 October 2018

Review of National Arrangements for the Protection and Management of Identity Information
C/o Home Affairs
4-6 Chan St
BELCONNEN ACT 2613

By email: submissions@homeaffairs.gov.au

Dear Mr Wilkins

As the union representing staff in the Australian Public Service (APS), the Community and Public Sector Union (CPSU) welcomes the opportunity to make a submission to this review of national arrangements for the protection and management of identity information. We are committed to providing a strong voice for our members in key public policy and political debates.

The CPSU has significant concerns that the outsourcing of core public sector work done by the APS risks identity theft and fraud. The CPSU has particular concerns about the proposed privatisation of visa processing. The CPSU is concerned that this emphasis on cost and speed could be at the expense of the safety and security of identity information as the Government is aggressively seeking to outsource functions.

While the Department of Home Affairs’ request for expressions of interest is primarily aimed at outsourcing visa applications and approvals, reports suggest that more functions—including data collection and verification, health and character checks or genuineness assessments—are expected to be added over time. Private operators could be used to administer tests, detect fraud and recommend decisions to grant or refuse visas.1

The overseas experience of outsourcing visa processing shows the risk of identity theft is real. In 2015, the operations of VFS Global, which acts for around 45 governments, were temporarily suspended after a technical glitch allowed visa applicants in Italy to access other people’s private information.2 This was far from the first instance of privacy breaches occurring. In 2007, the British Foreign and Commonwealth Office shut down its online visa application service, also provided by VFS Global, after a security breach was discovered that allowed unprotected information including claimant addresses, dates of birth and passport numbers, to be easily accessible for more than a year.3

---

These private operators such as VFS Global not only receive filled out visa application forms and passports but also collect fingerprints or other biometric data. The experience overseas is that any monitoring of privatised providers is decentralised and there is no guarantee of a consistent level of accountability. The privatisation of visa processing by the Spanish Government to VFS Global led to the handling of personal documents and biometric data being subcontracted out by the provider to India, showing the state could not hold the provider to account.\(^4\)

Former Department of Immigration Deputy Secretary Abul Rizvi has also raised concern about visa integrity if the profit motive is driving decisions by outsourced providers, risking fraudulent visas as Australian visas can be worth a significant sum, especially if work is offshored. It is unclear to what extent outsourced visa providers would be subject to scrutiny by government agencies such as the Ombudsman and the Auditor-General and whether the Freedom of Information Act still be applicable. Other issues include privacy issues given the vast wealth of data about Australians as well as potentially new Australians it would have access to and what data might be sold to offset any costs to meet requirements.\(^5\)

The experience of outsourcing in the Australian Taxation Office and the Department of Human Services (DHS) shows that these privacy risks are a real threat in outsourced providers and not an exaggeration.

While there is limited public reporting on the activities of third party providers, the experience of our members to date supports these concerns. In DHS, where contract call centres are being utilised, APS employees have raised a range of concerns about the training afforded to the workers in the centres, their ability to access systems and properly advance claims. There are circumstances where individuals have not had the knowledge or expertise to properly undertake the work, but they are still accessing and making amendments to client’s personal information. This situation raises real questions about the security of client’s data and the confidence we can have that it is being properly maintained.

There have also been reports of a high turnover of Labour Hire Staff with a member who is involved in training Serco staff reporting inadequate training, high staff turnover and a relaxed approach to hiring. Our members have described training they have done for outsourced workers as “woefully inadequate”. One member, who worked for DHS before working for an outsourced provider, reported receiving 4 months training in-house where when she was working for Probe she had received 2 weeks.

There are questions about the security of these outsourced sites. The CPSU understands staff cannot use mobile phones on site, but they may be able to take in a USB to remove data. Furthermore, systems are not immune to hacking and security clearance system have also been outsourced.

Only by maintaining this core work in-house can the public be confident that the handling of personal and biometric data will not be subcontracted overseas, risking privacy and identity theft, and that the Commonwealth can enforce the level of oversight and accountability the Australian community expects from government services whether it is for visa, social security or tax processing.


The CPSU is happy to provide information on the matters raised in this submission. Please contact our Senior Policy and Research Officer, Osmond Chiu, at osmond.chiu@cpsu.org.au or on 0424 159 463 for further information.

Yours sincerely

Lisa Newman
Deputy National President
Border Protection & International Affairs Team
Community and Public Sector Union