

30 July, 2010

Committee Secretary
Senate Standing Committee on Environment, Communications and the Arts
PO Box 6100
Parliament House
Canberra ACT 2600
Australia

Email: eca.sen@aph.gov.au

Dear Secretary

Senate Inquiry into:
The adequacy of privacy protections for Australians online

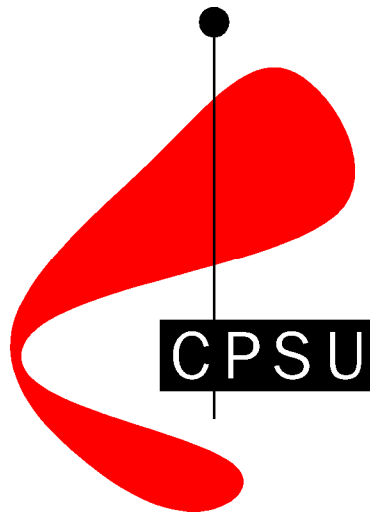
Please find attached a submission from the Community and Public Sector Union (PSU Group) to the Senate Inquiry into *The adequacy of protections for the privacy of Australians online*.

The contact person for this submission is Rhiannon Carter, Research Officer, ph (02) 8204 5709.

Yours sincerely

A handwritten signature in black ink, appearing to read 'Kristin van Barneveld', written in a cursive style.

Dr Kristin van Barneveld
CPSU Deputy Secretary



CPSU (PSU Group) submission to the:

**Senate Inquiry into:
The adequacy of privacy
protections for
Australians online**

July 2010

Senate Inquiry into: The adequacy of privacy protections for Australians online

Background

The Community and Public Sector Union (CPSU) is an active and progressive union committed to the promotion of a modern efficient and responsive public sector that delivers quality services and quality jobs. We represent around 60,000 members in the Australian Public Service (APS), ACT Public Service, NT Public Service, ABC and the CSIRO. We also have members in Telstra, commercial television and the telecommunications industry.

Overview

The CPSU welcomes the Senate Inquiry into *The adequacy of protections for the privacy of Australians online*. The CPSU submission specifically addresses the term of reference '(c) data collection activities of government agencies' taking into account both data collection and data management. As technology improves and government agencies seek to deliver more services online, the need to collect and store personal information is increasing. If Australians are providing sensitive information to agencies there must be mechanisms in place to ensure that data collection processes are transparent and that citizens are clearly informed about why their personal information is being collected and how it will be used.

However, protecting the privacy of Australians is not just limited to the collection of the data, it also encompasses how data is used and managed. With improvements in technology and a shift towards a greater online service delivery capacity across the APS, it is essential that systems and procedures are in place to ensure that privacy is protected. While at the same time APS staff should be given the level of access and information necessary to ensure the delivery of high quality services and programs.

Current Protections

Currently the public sector and public sector employees are subject to some of the complex interactions between privacy legislation and procedures in the country.

APS employees are bound by the *Privacy Act 1988*, the *Freedom of Information Act 1982*, the *Public Service Act 1999*, the *Data-Matching Program (Assistance and Tax) Act 1990* and their specific agency enactment (if any) which could contain provisions relating to the release of information (ie secrecy provisions). For example the agency enactment for the Child Support Agency (CSA) has specific secrecy provisions which make it a criminal offence to use or disclose certain information. This means staff in CSA may face up to a years imprisonment for using or disclosing

certain information in certain circumstances¹, whereas staff in another agency who use or disclose similar information may not be considered to have committed an offence.

In addition, APS employees are also subject to the policies and procedures of their agency and as employees are obliged to follow lawful and reasonable directions, such as any agency privacy policy. This represents another level of regulation for employees to adhere to in their work. Further, Regulation 2.1 of the *Public Service Regulations* 1999 imposes a restriction upon APS employees from disclosure of information an employee obtains in connection with their employment if it is '*reasonably foreseeable that the disclosure could be prejudicial to the effective working of government. . .*'.

Therefore if an employee does not follow the above mention laws or a fails to follow the relevant agency privacy policy they may be subject to disciplinary action under the APS Code of Conduct in s13 of the Public Service Act 1999. Section 15 of the Act provides a range of sanctions that can be imposed on an employee who is found to have breached the Code ranging from a reprimand to termination of employment.

The ultimate consequence of this complex regulatory framework is that depending upon the agency in which an employee works the disclosure or use of certain information could result in a breach of the Code of Conduct or the commission of a criminal offence.

Further to this the Australian Law Reform Commission (ALRC) recently released the report of their inquiry into the *Secrecy Laws and Open Government in Australia*. The purpose of the inquiry was to investigate the:

...options for ensuring a consistent approach across government to the protection of Commonwealth information, balanced against the need to maintain an open and accountable government by providing appropriate access to information².

The inquiry also considered how secrecy provisions interacted with civil restraints such as the *Public Service Act* and Regulations and the increased need to share information within government and also with the private sector to promote an open and accessible government.

While the focus of the review and the subsequent recommendations were on the release of Government information, the underlying theme of the recommendations was the need for consistency and the rationalisation of secrecy provisions across government which is relevant to this review. The outcomes of the ALRC inquiry and reform process have implications for this inquiry and the CPSU strongly suggests that this inquiry consider the recommendations of the ALRC Report in their findings.

The current legislative and agency policies and procedures in place in the APS adequately ensure that the information collected by government agencies is subject to a range of security measures. What is not adequate is the availability of education and training for employees on their responsibilities, and nor is there consistency in the application of these policies/procedures across the APS. With increased data sharing between agencies, including reforms in Human Service delivery, protocols surrounding privacy and the protection/sharing of information is an area requiring urgent clarification.

¹ http://www.austlii.edu.au/au/legis/cth/consol_act/csaca1988427/s16aa.html

² <http://www.alrc.gov.au/inquiries/title/alrc112/5.ExecutiveSummary.pdf>

This submission draws on feedback from CPSU members to highlight some of the concerns with the current privacy protections.

Summary of Recommendations:

1. *That there is a consistent APS wide policy on open and transparent data collection.*
2. *That information on agency data collection activities is made publicly available.*
3. *That government continues to support the ongoing implementation of the Gershon Reforms.*
4. *Agencies are to be provided the necessary time, funding, support and resources to improve their ICT capability and secure their online data collection and management systems.*
5. *Increased data sharing capabilities be properly supported by government.*
6. *Consultation is to occur with staff and their union about current protections that are unnecessary restrictive and/or ineffective and before any changes are made.*
7. *A single consistent privacy policy is to be developed across the APS to promote data sharing.*
8. *Any reforms to data sharing arrangements and protections must be adequately resourced.*
9. *Guidelines for those working with the automated response systems are to be improved in consultation with employees and their union.*
10. *Possible mechanisms that could be added to procedures or ICT systems to reduce instances of inadvertent access are to be investigated.*
11. *Education and training must be consistent across the APS and agencies are to receive funding to administer the training to staff.*
12. *Protection of privacy is best ensured when work is conducted by APS employees who are subject to the APS Code of Conduct. Where work is outsourced, contract workers are to be subject to the same requirements as APS employees.*

Data Collection

Data Collection is a key part of delivering efficient and effective services, however to ensure that the privacy of all Australians is protected, data must be collected in a transparent and secure way. This requires the government to adequately fund agencies to have the requisite ICT capability enabling the collection and storage of data securely. It also requires a consistent approach to data collection and sharing across the APS as a whole, so that all Australians are aware why their information is being collected and how it will be used.

Transparency

Greater online service delivery capability is a major recommendation of the Blueprint for the Reform of Australian Government Administration (the Blueprint for Reform) and is being implemented to varying degrees across the APS. In order to facilitate online service delivery, government agencies are increasing the amount of information they are collecting from the public to enable data matching and sharing across agencies.

This data sharing will simplify citizen interaction with government. However it is essential that if agencies are going to be sharing data, then using it for multiple purposes, that there is transparency about what data is being collected, why it is being collected and how it is to be stored and shared.

To guarantee that privacy is protected there must be an impetus for agencies to be open and transparent about their data collection and data management activities. In this area, the APS would benefit from a consistent, service wide policy that includes mechanisms such as disclaimers on all forms that collect information, obtains permissions for data sharing and by making information on data collection activities publicly available. In addition there needs to be provision of adequate time, resourcing and funding provided to agencies to implement systems and procedures that help them meet their privacy obligations.

Recommendation: That there is a consistent APS wide policy on open and transparent data collection.

Recommendation: That information on agency data collection activities is made publicly available.

Data Collection Capability

Government data collection occurs in a number of different ways, including on paper, over the phone, in person and online. All of this information is then stored electronically and some is made available online through automated tools, for example the pre-populating capability of the Australian Taxation Office (ATO) *e-tax* program forms. This capability partially completes an individual tax return electronically with information such as personal details and government payments³.

Being able to collect and use data in services such as *e-tax* is critical to making government services more accessible to the community. However to ensure that the personal information of Australians remains private and secure in this process, agencies need to have the capability in their ICT systems to collect, store and share this information securely.

Limited ICT capability in some agencies is an issue that CPSU members have raised in a number of different forums. Improving the capability and effectiveness of agency ICT systems is required to ensure that personal information remains protected as the online activities of agencies increase.

The Gershon Report into the Australian Government's Use of ICT supports this view and provides a detailed analysis of the problems facing ICT systems across the APS. Gershon outlined how the current approach to decentralised procurement and ICT

³ <http://www.ato.gov.au/individuals/content.asp?doc=/content/58871.htm&page=2&H2>

governance did not result in high quality outcomes. To address this Gershon recommended a greater level of centralisation for government ICT, nominating a common security network as one of the candidates for centralisation⁴.

Continuing to implement the Gershon recommendations and providing the funding, support and resources to agencies to improve their ICT capabilities is fundamental to ensuring that the privacy of Australians is not compromised in data collection and data sharing.

Recommendation: *That government continues to support the ongoing implementation of the Gershon Reforms.*

Recommendation: *Agencies are to be provided the necessary time, funding, support and resources to improve their ICT capability and secure their online data collection and management systems.*

Data Management

In addition to the data collection activities of government agencies, data management activities are essential to ensuring the privacy of Australians online.

Data management refers to how personal and sensitive data is used and stored once it has been collected and entered into ICT systems by an agency. As the APS moves toward a more integrated approach to service delivery and data management, protecting the privacy of Australians will become a more complex task.

Data Sharing

The Blueprint for Reform recommended increasing the ability for agencies to share information: this information could include addresses, job details or social security payments.

Data sharing has the potential to improve the quality, efficiency and effectiveness of government service delivery. Streamlining the ways agencies can share information will make interacting with the government simpler. However an important balance must be reached - the privacy of individuals must be protected while ensuring APS staff have the flexibility to be able to share and use the information necessary to deliver quality services.

CPSU members described a number positives associated with increasing the ability of agencies to share information:

- It will make performing a range of tasks and jobs easier if personal details can be updated more readily. Currently there is no provision for the automatic update of personal details such as addresses across the public sector. Employees are forced either to wait for individuals to inform each agency or go through what can be an often complicated process of requesting information from other agencies.
- It lessens the burden on the public. Individuals can give one agency information and it can then be shared across the public sector, without the individual having to repeat the process a number of times.

⁴ <http://www.finance.gov.au/publications/ict-review/index.html>

- Greater ability to collect and share data has the potential to save the government money as it allows agencies such as Centrelink to identify instances of overpayment or incorrect payment and changes in circumstances quicker and more easily.
- It has the potential to save the government money and make the work of staff easier. For example greater sharing of income information and work details could potentially reduce child support payment avoidance and related debt collection activities by supplying CSA staff with relevant information in a timely manner.
- Information sharing enables more efficient data mining, which in turn can lead to the more effective use of statistical information. This would bring significant benefits in trend analysis, leading to the more effective development of evidence-based social policy and the more efficient development of tailored service offers to individual citizens.

However there are also a number of concerns with increased data sharing, regarding the protection of the privacy of Australians.

- If the individual does not initially give approval for their information to be shared and used by another agency for another purpose, this has the potential, in certain circumstances to be a breach of privacy.
- The inconsistency between agency policies is a major issue as the protections that are in place in one agency may not be in place in another. This places employees in a difficult and confusing position since what is acceptable in one agency may not be in another, with the corresponding potential to compromise security
- There are significant security and privacy implications for transferring information between agencies. Agencies need to have the resources to ensure their ICT system can adequately protect data. Conversely, there are also risks with having a single database of information - it leaves the information vulnerable loss, damage, misuse or theft.
 - Storing the information centrally could give staff access to information that they do not need to perform their duties, which could potentially compromise privacy.
- In some cases, the current policies are restrictive and difficult to work with, as the protocols for requesting information from other agencies within the APS are strict and time consuming. Any recommendation to further restrict information sharing will affect ability of staff to deliver high quality services to the public, as restrictive protocols are time consuming and require more resources.

The APS is increasingly moving to integrated service delivery that makes accessing government services easier and more efficient for the Australian public. This integrated approach will require a greater level of data sharing and increased ICT capability for online data collection and management. This has privacy implications and requires a consistent APS wide approach that protects individual privacy while allowing staff to do their jobs in the most effective and efficient way possible.

Recommendation: Increased data sharing capabilities be properly supported by government.

Recommendation: Consultation is to occur with staff and their union about current protections that are unnecessary restrictive and/or ineffective and before any changes are made.

Recommendation: A single consistent privacy policy is to be developed across the APS to promote data sharing.

Recommendation: Any reforms to data sharing arrangements and protections must be adequately resourced.

Protections for Staff

The data collection and management activities of government agencies not only have implications for the Australian public, they can also have significant implications for APS employees.

As outlined above, APS employees are already held to a high standard in terms of protecting the privacy of Australians and are subject to numerous legislative and procedural constraints. This inquiry needs to ensure that its recommendations do not further increase the burden on staff and impede their ability to deliver high quality services to the Australian public.

Currently the onus is on staff to avoid breaching privacy regulations or if they inadvertently breach privacy to report the circumstances. There is little in the way of systemic protections to ensure that breaches cannot occur. Placing this level of responsibility on individual staff can be a burden and can also expose staff to serious consequences if any breach occurs, even if it is inadvertent.

One example of where inadvertent access can have significant consequences for staff is in Centrelink where the privacy policies and protections are some of the most rigorous in the APS. The automated response system used in Centrelink Call Centres immediately accesses a client record as they are transferred to an operator. This is designed to promote efficiency and effectiveness allowing staff to view client details as soon as they answer the call. However the employee has no control over who is in their call queue or what record the computer system will open, leaving the employee open to inadvertently access the record of someone who they know, or who in some other way they may be deemed to have a conflict of interest with.

If this inadvertent access occurs, the onus is again on the employee to report the breach, however this can be further complicated if the employee is unaware that there is a conflict of interest. For example, clients living in the same street or apartment building are considered to be a conflict of interest, however if the employee has not had reason to review the address of the client they may not know if they have breached the Centrelink protocols.

To ensure compliance with this policy, there are regular audits of employee access. If an employee is found to have accessed a record that is deemed a conflict of interest and not reported, they are exposed to the range of sanctions outlined in the APS Code of Conduct, including termination of employment.

If more information is to be stored online and electronically available to staff and the public, there needs to be a review into the way inadvertent breaches of policy are dealt with. Continuing to punish staff for instances of inadvertent access that they

have no control over is inefficient and does nothing to protect the privacy of Australians online.

Recommendation: *Guidelines for those working with the automated response systems are to be improved in consultation with employees and their union.*

Recommendation: *Possible mechanisms that could be added to procedures or ICT systems to reduce instances of inadvertent access are to be investigated.*

Education and Training

In order to protect the privacy of Australians online, effective and consistent education and training of staff in the principles of privacy and information sharing must occur. The complex nature of privacy legislation, supporting agency policies and their interaction with the work of APS employees requires more than a basic understanding of privacy requirements. Currently there is no APS wide approach to education and training of employees about their privacy obligations and responsibilities.

The feedback received by the CPSU about this issue was that some agencies, for example the ATO, have education and training programs that are thorough and help staff understand their responsibilities. However other agencies do not have the same level of education and training, so receiving information and guidance on dealing with privacy protections can be minimal and ad hoc.

Recommendation: *That education and training be consistent across the APS and that agencies receive funding to administer the training to staff.*

Recommendation: *Education and training must be consistent across the APS and agencies are to receive funding to administer the training to staff.*

Third Parties

Agencies such as the ATO, make use of contract workers at specific times. While it has been recommended by the Gershon Review that this practice be reduced within ICT, it is still common in other areas of the APS. There are privacy risks with the use of contractors in agencies, and contract staff are not subject to the APS Code of Conduct, therefore not subject to the same privacy obligations and consequences as APS employees.

If agencies are committed to protecting the personal information of Australians, they need to ensure that giving contractors access to potential sensitive data does not jeopardise privacy.

The same requirements should apply to third party organisations who collect information and deliver services of behalf of the government. Again, the workers in these organisations are not APS employees and do not have the same obligations as APS employees. To ensure the protection of Australians privacy there need to be adequate checks and balances included in contracts with providers, while compliance with these mechanisms needs to be monitored and reported on.

Recommendation: *Protection of privacy is best ensured when work is conducted by APS employees who are subject to the APS Code of Conduct. Where work is outsourced, contract workers are to be subject to the same requirements as APS employees.*

Conclusion

Protecting the privacy of Australians online with specific reference to the data collection activities of government agencies is fundamentally about striking a balance. A fair balance between ensuring there are adequate security mechanisms in place to protect personal data and ensuring that APS employees have the access to data that allows them to do their job and deliver high quality services to the Australian public.

This balance can be achieved by developing a consistent APS wide approach to data collection and management, ensuring that agencies have the necessary time, funding, support and resources to have the ICT capability to protect and share data, providing clear and consistent education and training for all APS staff, consulting with staff and their union about current ineffective privacy restrictions and ensuring that data collection and management is conducted by APS employees.

The privacy of all Australians is important, as is having a responsive, flexible, open and high quality public sector. Consulting with staff and their union about ways to protect privacy and ensuring that adequate funding and resources are made available to agencies is the key to making an integrated online public sector work for staff and for all Australians.