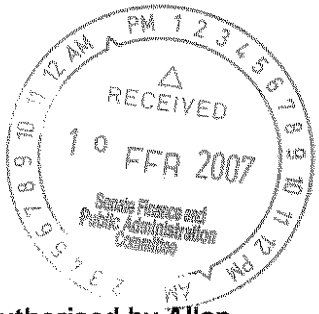
Hughes, Alan

Subject: FW: Senate Estimates
Importance: High



Instruction / Guidelines

National Instruction CG 920227, 'Dealing with clients who are family friends etc', authorised by Allan Ross, Assistant Secretary, which has applied since 28 September 1992.
National Instruction CG920227 relevantly states:
Staff must not handle the cases of persons with whom they have a relationship in a private capacity. This includes family, relatives and friends...

When cases involving a family member, former relatives through a terminated marital relationship, personal friend, [or] close personal acquaintance... become the responsibility of officers, those cases must be given to their supervisor for reassignment to another officer who has no association with the client.

National Instruction CG 930240, 'Browsing information without authority', authorised by Allan Ross, Assistant Secretary, which has applied since 1 December 1993.

National Instruction CG 930240 relevantly states:
It is not part of your job to access records of neighbours, friends, family, acquaintances etc... Because you have been told that it is not part of your job to do so, accessing these records is not authorised and may be an offence...

A person found to have browsed a record should expect a demotion of position, a decrease in salary or dismissal

National Instruction No CL 960007, 'Browsing and Conflict of Interest', authorised by Michael Sassella, First Assistant Secretary, which has applied since 16 January 1996.

National Instruction CL960007 relevantly states:

Departmental officers must always avoid situations in which there is, or may appear to be a conflict of interest. For example, there would be a conflict of interest where the officer has a private relationship with a person whose record is being accessed... Records of friends, relatives and acquaintances... must not be accessed. Officers who access a record where there is, or may be, a conflict of interest, are therefore making an unauthorised access.

Authority for staff to access departmental records is given by the Department, not customers involved. A customer authority is no excuse for an officer to access a record where this instruction advises a conflict of interest may be involved.

Department of Social Security Confidentiality Manual Chapter 2, titled 'Unauthorised Access to Protected Information', which applied from January 1996 to January 2003. This Chapter explains what is meant by 'browsing' and why it creates a conflict of interest, and why accessing information without authorisation is not allowed.

Chapter 2 of the Confidentiality Manual relevantly states:
2.202 Browsing... means accessing a record (computer record or paper file) that the officer has no need to access...

2.301 ... It is important that departmental officers understand that just because they have access to customer records through such means as logon access, this does not mean that all records are available to them. They may only access those records which they are required to access as part of their prescribed duties...

2.312 Departmental officers must always avoid situations in which there is, or may appear to be, a conflict of interests. For example, there would be a conflict of interest where the officer has a personal interest in the person whose record is being accessed. For this reason an officer must not access his or her own customer record. Records of friends, relatives and acquaintances, including work colleagues, should also not be accessed. Officers who access a record where there is, or may be, a conflict of interest are, therefore, making an unauthorised access.

2.321 Departmental officers are given access to the ADP system solely to enable them to do their jobs. It is not provided as a data base for private use.

2.322 Staff members must not access computer records out of personal interest or curiosity. To do so is to browse without authority.

2.323 Some examples of browsing are:

- looking up your own record
- looking up a friend's birth date and/or address to send a greeting card
- looking up a friend's or relative's telephone number which may be unlisted
- looking up friends and relatives to find out what their income or assets might be
- looking up a third party on behalf of a friend or relative
- looking up a friend's or relative's claim in another office to see how it is progressing or to see if it has been correctly assessed...

2.325 Browsing which is not part of an officer's job is unauthorised access. An officer **cannot** be authorised by a customer to access the customer's record when such an access would be contrary to departmental practice.

2.331 To avoid situations where there is, or could be, a conflict of interests between a staff member's duty as a departmental officer and their personal connection with the customer, staff **must not** handle the cases of persons with whom they have a close relationship in a private capacity. This includes family members, friends, close personal acquaintances or persons with whom they are connected through community organisations such as service clubs or sporting associations.

2.332 While it is acceptable for an officer to receive a request from a friend, relative or acquaintance for information or advice about that person's dealings with the Department, the officer **must not** be involved in processing the matter (including accessing the customer's record). When such a situation arises, the officer **must** hand the matter to another officer for action...

2.334 Cases or enquiries involving any of the groups described above should be referred to the staff member's supervisor for possible reassignment to another officer. As only the affected staff member may be aware that a situation involving a conflict of interest has arisen, it is imperative that all staff members remain constantly alert to these situations and advise their supervisor immediately.

2.335 This restriction does not apply to everyone an officer knows as a casual acquaintance. The test is whether the officer's acquaintanceship with the customer could be seen by a third person to be to the customer's advantage in his or her dealings with the Department. It is understood that in small communities, an officer cannot be removed from handling any case where he or she knows the customer personally. In these circumstances, advising the officer's supervisor that a conflict of interests may occur can remove the potential problem. If an officer has any doubts about a situation, they should refer it to their supervisor, Regional manager or Area Privacy Officer for advice...

Centrelink Privacy and Confidentiality Manual Chapter 3, titled 'Storage and Security of Personal/Protected Information', which has applied since January 2003 and has been amended from time to time. This Chapter of the Manual states that a person whose information is held by Centrelink has a right to expect that Centrelink will hold it securely, and will ensure that access to the

information is permitted only for legitimate purposes.

Chapter 3 of the Privacy and Confidentiality Manual relevantly states:
3.061 Being a Centrelink employee does not automatically authorise an individual to access protected information. Employees are given access to Centrelink computer and paper records in order for them to carry out their prescribed duties. Access to protected information is not provided for private use therefore employees must not access computer or paper records of customers or employees out of personal interest or curiosity...

3.063 Some examples of browsing include accessing:

- your own customer record;
- the customer database or Infolink to:
  - obtain a friend's birth date and/or address to send a greeting card;
  - obtain a friend or relative's telephone number which may be unlisted in order to contact them on a social/personal basis etc;
- the records of people reported in the press;
- neighbours records out of curiosity;
- the records of friends and relatives to find out what their income or assets might be;
- a customer record on behalf of a friend or relative;
- a friend's records to see how their claim is progressing or to see if it has been assessed correctly;
- a work colleagues record at his or her request;
- using 'live' records for group training purposes; and
- a customer's record who is the subject of a tip-off if it is not part of the staff member's job to do so.

3.064 Public confidence in the integrity of the public service is vital to the proper operation of government. Where the community perceives a conflict of interest that confidence is jeopardised. A conflict of interest occurs when an employee's personal affairs, financial or other interests conflict with the performance of their official duties...

3.067 There would be as conflict of interest where the employee has a personal interest in the person whose record is being accessed. For this reason an employee must not access and/or process their own customer record or those of family, ex family, friends, close personal acquaintances, neighbours [or] work colleagues without authorisation from their team leader...

3.068 The restriction does not apply to everyone an employee knows as a casual acquaintance. The test is whether the acquaintance with the customer could be seen by a third person to be to the customer's advantage in his or her dealings with Centrelink...

3.071 If circumstances make it unavoidable for an employee to access the record of a friend, relative or acquaintance, the problem of conflict of interest can be overcome by advising his or her team leader/manager of the need **before** accessing the record. With the team leader's permission, the record may then be accessed and/or assessed. A record of this authorisation will need to be kept, possibly in a DOC created by the team leader on the customer record [or] in a secure office register signed by the team leader...

3.072 **A customer cannot authorise an employee** to access their record when such an access would be contrary to Centrelink practice. For example, an employee's mother cannot authorise them to look at her record because Centrelink instructions clearly state that an employee must not access or assess the records of family members....

3.101 A Centrelink employee may inadvertently access the customer record of a family member, friend, close personal acquaintance, neighbour etc. If this happens the employee must immediately speak with their team leader or manager and explain the situation. The team leader or manager must make a note of the 'inadvertent' access in a secure office register...

Centrelink 'Declaration of Confidentiality/Privacy, Security, Fraud Awareness and Conduct

Responsibilities' booklet (previously known as the 'Declaration of Confidentiality/Security and Privacy Responsibilities' booklet or the 'Rules for the Handling of Personal/Protected Information' booklet), which is referred to in this report as the Confidentiality Booklet. The Confidentiality Booklet is provided to employees who undertake training in privacy or information security awareness. The Confidentiality Booklet contains a summary of the 'no-browsing' rules and a Declaration of Confidentiality, which is signed by each employee who receives the Confidentiality Booklet.

The Confidentiality Booklet relevantly states:
Access to personal information is on a 'need to know' basis in order for you to perform your duties. It is not provided for your personal use. You do not have to disclose the information to someone else, just looking at a customer or employee's record when you are not authorised is an offence under various legislation Centrelink administers. This is commonly known as **browsing**.

You are not authorised to access and/or process your own customer record or those of family, friends or other people where there may be, or may be perceived to be, a **conflict of interest**. This also includes people with whom you may have had or are having a dispute.

While it is acceptable for you to receive a request from a friend, relative or acquaintance for information or advice about the person's dealings with Centrelink, you should not be involved in processing the matter including accessing the customer's or Centrelink employee's record. **A customer (including a colleague who is a customer) cannot authorise you to access their record** where such access would be contrary to Centrelink practice. For example, your mother cannot authorise you to look at her record because Centrelink instructions clearly state that you cannot access or assess the records of family members.

There are severe penalties for employees who breach the confidentiality provisions. These include penalties under various legislation (including the *Crimes Act 1914*) of up to two years imprisonment. Ongoing and non-ongoing employees may also face sanctions under the *Public Service Act 1999* which may attract disciplinary measures such as fines, demotions or dismissal.

Chief Executive Instruction 20, 'Unauthorised Access/ Centrelink Employees as Centrelink Customers', which has applied since 2 December 2005. This Instruction clearly articulates Centrelink's rules regarding unauthorised access of ISIS, Centrelink employees as Centrelink customers and access to employee records.

Chief Executive Instruction 20 relevantly states:
Centrelink officials must not access the...ISIS records of themselves; family members; relatives, including in-laws; their neighbours; their friends, including emergency contacts; their close personal acquaintances; their work colleagues; or any other customers' records where there is no legitimate business reason...

The above instruction was reissued on 18 December 2005, renamed and is still current. It is 'Unauthorised access to Centrelink Customer Records and the Personnel Records of Centrelink Officials'. A new CEI was also issued - CEI21 'Centrelink Officials Interacting With Centrelink as Customers.'

Legislation

section 1312A of the *Social Security Act 1991*, which applied from 24 December 1992 to 20 March 2000 and was amended from time to time. Effectively, this provision made it an offence for a person to intentionally access protected information in Centrelink records if the person was not authorised to obtain that information and knew that the information was protected information.

section 1312B of the *Social Security Act 1991*, which applied from 24 December 1992 to 20March 2000 and was amended from time to time. Effectively, this provision made it an offence for a person to intentionally use, record or disclose protected information in Centrelink records if the person knew that the information was protected information.

subsection 203(1) of the *Social Security (Administration) Act 1999*, which has applied since 20 March 2000 and has been amended from time to time. Effectively, this provision makes it an offence for a person to intentionally access protected information in Centrelink records if the person is not authorised to obtain that

information and knows that the information is protected information.

subsection 204(1) of the *Social Security (Administration) Act 1999*, which has applied since 20 March 2000 and has been amended from time to time. Effectively, this provision makes it an offence for an unauthorised person to intentionally use, record or disclose protected information in Centrelink records if the person knows that the information is protected information.