Chapter 7

PRIVACY AND CIVIL LIBERTIES ISSUES

Introduction

7.1 The FTR Act contains a number of features that are of concern to civil liberties groups. These were summarised by the Privacy Commissioner as follows:

- the legislation sanctions information gathering techniques which apply to the community at large, or to a significant section of the community, and which involve routine monitoring of certain activity;
- the legislation contains a very wide definition of the social objectives of the initiative - typically encompassing loosely defined law enforcement, revenue protection or efficiency goals;
- the legislation is justified on the basis of a public interest accompanied by estimates of large anticipated financial savings;
- there is no significant consideration of alternatives (particularly more focused or targeted options);
- the legislation requires secrecy of operation, especially as regards individuals affected;
- the information collected under the Act is circulated relatively widely amongst a significant number of Commonwealth and State agencies, and a wide range of officers within those agencies;
- the Act reposes significant administrative discretion as to the circulation of information with the head of the agency;
- there is a suggestion that external accountability mechanisms, such as the Ombudsman and the Privacy Commissioner, furnish adequate protection of the individual interests affected; and
- the legislation gradually expands to new areas.[1]

7.2 Parliament has procedures in place to ensure that legislation coming before it is scrutinised carefully, both as to the substantive policy

---

[1] Submission No. 41, (Privacy Commissioner) p. 1.

contained in the bill and also as to general compliance with accepted norms protective of the rights of individuals. For example, all bills introduced into the Senate are examined by the Senate Standing Committee for Scrutiny of Bills. This is a multi-party committee which looks at whether the bill:

- trespasses unduly on personal rights and liberties;
- makes rights, liberties or obligations unduly dependent on insufficiently defined administrative powers, or on non-reviewable decisions;
- inappropriately delegates legislative powers; or
- insufficiently subjects the exercise of legislative power to parliamentary scrutiny.[2]

7.3 These procedures themselves are an indication of the importance which Parliament attaches to ensuring that the rights of individuals are limited only after the most thorough scrutiny, and with the clear approval of Parliament. Thus it is important to ensure that intrusive powers are conferred in express language and are not disguised in empowering provisions of too much generality. It is for this reason that the Committee has concluded, as discussed in chapter 3 above, that AUSTRAC must take care to ensure that its actions are clearly within the terms of its statutory charter. In cases of doubt, AUSTRAC should seek a suitable amendment to the legislation.

7.4 The legislation does restrict rights that people would otherwise have under the law. It does this in seeking to cutrail and detect the commission of major crime.

7.5 The question as to where the balance between the need to maintain a free and democratic society and the need to ensure crime is prevented and punished is a difficult one.

7.6 However, it must be said that the processes of AUSTRAC should not be aimed at detecting minor crime, for example, lesser offences against the Social Security Act.

---

[2] Senate Standing Order 24(1)(a).

7.7 These areas of concern were examined during the Committee's inquiry.

AUSTRAC's Functions

7.8 In bilateral projects the role of AUSTRAC was explained as follows:

- by using known criminal target information (*provided by the lead law enforcement agency*) specific related reports are identified and analysis conducted;
- from examination of data for relevant geographic areas, AUSTRAC will prepare profiles of cash flows as indicated by its holdings;
- an initial report is made to the lead agency and this may result in further analysis, effectively repeating the cycle;
- records from banks and other cash dealers may be requested either by AUSTRAC or the lead agency depending on the circumstances;
- similar data might be requested from those cash carriers that are exempt from reporting;
- AUSTRAC may use its (civil) audit powers to go into cash dealers in appropriate cases ....; and
- the identified relevant financial data held is integrated into the law enforcement operation.

This process is not a rigid one, it is changing as experience grows.[3] (Emphasis added.)

7.9 While it may be that AUSTRAC has exceeded its charter by participating in NCA task forces, as noted in Chapter 3, AUSTRAC has been very conscious of civil liberties issues. The Director of AUSTRAC, Mr Coad, satisfied the Committee that it had these issues well in mind.

[3] Submission No. 13, (AUSTRAC) p. 104.

Investigations and Intelligence Gathering

7.10 In considering the criticisms that AUSTRAC has exceeded its statutory functions, it is essential to keep in mind the difference in character between the investigations carried out by policing bodies such as the National Crimes Authority, the Australian Securities Commission and the Australian Taxation Office, and an intelligence gathering entity such as AUSTRAC.

7.11 Policing bodies have the ability to obtain information from people by compulsion or in circumstances which may cause them to make statements unfair to themselves.

7.12 A police interview can be a daunting affair even if carried out on a voluntary basis. Questioning by compliance officers of the Immigration Department can be quite frightening to someone suspected of breaching the relevant Act no matter how polite they might be. People subject to these sorts of investigations may provide evidence which is flawed and disadvantageous to them.

7.13 AUSTRAC does not engage in these sorts of enquiries. It deals with material which, though supplied by the force of law, is created without compulsion and in the absence of state authority. Thus the risk of it being tainted to the disadvantage of the supplier is markedly reduced.

AUSTRAC and the IPPs

7.14 As set out in paragraphs 3.17-3.26 it is essential that AUSTRAC always acts within the legislation which underpins it.

7.15 It is fundamental to the effective operation of civil rights that Parliament determines what powers law enforcement bodies will have and the framework within which they may be exercised.

7.16 The operations of AUSTRAC and the discretion of the Director to allow access to information held by AUSTRAC are subject to the

Information Privacy Principles (IPPs) under the *Privacy Act 1988*. AUSTRAC detailed its compliance with the relevant IPPs as follows[4]:

The Privacy Principles	How AUSTRAC Complies
Principle 1 - Ensuring collection of information is lawful and fair	
Agencies must not collect personal information unless: (i) it is collected for a lawful purpose directly related to a function or act of the agency; and (ii) the means of collection are lawful and fair.	*Financial Transaction Reports Act 1988.*
Principle 2 - Informing people why information is collected.	
Agencies must ensure that people from whom they solicit personal information are generally aware, before collection, or as soon as practical thereafter, of: (i) the purpose of collection; (ii) and legal authority for the collection; and (iii) third parties to which the collecting agency discloses such information as a usual practice.	Advertisements in press, brochures Guidelines Media interviews Airport signs - in various languages Advice from financial institutions to their clients. International currency report forms have their purpose clearly stated on them.

[4] AUSTRAC Security and Privacy Manual section 5.2, draft document tabled at the Committee hearing on 10 June 1993 (Evidence, Mr Coad, p. 192).

Principle 3 - Ensuring personal information collected is of good quality and not too intrusive.	
Where an agency solicits personal information (whether from the person that information is about or otherwise), it must take reasonable steps to ensure (i) that the information is relevant to the purpose of collection, up-to-date, complete, and (ii) that its collection does not unreasonably intrude upon the person's personal affairs.l	AUSTRAC is not able to fully control the quality of the data which financial institutions gather and subsequently report. Guidelines are issued, there is a statutory requirement to report and AUSTRAC carries out audits of financial institutions. When the reports are lodged AUSTRAC takes the following steps to ensure quality information. Quality Control Unit functions • cleansing • checking suspect transaction reports twice after data entry • suspension/return of non-cash transactions for correction • with electronic data delivery systems the ability to return data for correction.
Principle 4 - Ensuring proper security of personal information	
An agency must protect personal information against misuse by reasonable security safeguards, including doing everything within its power to ensure that authorised recipients of the information do not misuse it.	Physical personal and data security procedures. Section 27 - statutory restriction on access Memoranda of Understanding required from agencies accessing FTR information. Logging access. Recording summary and other types of report details.

Principle 5 - Allowing people to know what personal information is collected and why.	
Any person has a right to know whether an agency holds any personal information (whether on him or her or not) and if so: (a) its nature; (b) the main purpose for which it is used; (c) the classes of persons about whom it is kept; (d) the period for which each type of record is kept; (e) the persons who are entitled to have access to it; and under what conditions; and (f) how to obtain access to it. Each agency must maintain an inspectable register of this information, and inform the Privacy Commissioner annually of its contents.	As for Principle 2 (ie) advertisements, guidelines, brochures, media interviews, airport signs, advice from banks etc to their clients and Responding to general enquiries from public. Publishing outline on AUSTRAC holdings in the agency Privacy Digest. FOI Statement provided to anyone who asks for information - FOI requests are processed in accordance with the guidelines set out in the FOI Statement.
Principle 6 - Allowing people access to their own records.	
A person has a right of access to personal information held by an agency subject to exceptions provided in the *Freedom of Information Act 1982* of any other law.	AUSTRAC provides information in response to FOI requests.

Principle 7 - Ensuring that personal information stored is of good quality, including allowing people to obtain corrections where it is not.	
Agency must make corrections, deletions and additions to personal information to ensure that it is: (i) accurate; and (ii) relevant, up-to-date, complete and not misleading (given the purpose of collection and related purposes), subject to exceptions provided in the *Freedom of Information Act 1982* or any other law. Agencies are required to add a reasonable statement by a person to that person's record on request.	Quality Control Unit (QCU) functions. Where AUSTRAC becomes aware that poor quality data has been sent to it then steps are taken to correct it. At the same time poor quality data may be suspended to eliminate access to it. To ensure that suspect reports are accurately reflected in database and QCU checks them twice after data entry. With electronic data delivery systems poor quality data can more easily be returned for correction.
Principle 8 - Ensuring that personal information is of good quality before use.	
Agencies must take reasonable steps to ensure that personal information is accurate, up-to-date and complete (given the purpose of collection and related purposes) before using it.	See Privacy Principle 3 & 7. AUSTRAC suspends poor quality data if necessary to ensure that clients cannot use it. Data processed manually is carefully vetted to ensure highest possible quality of data.
Principle 9 - Ensuring the personal information is relevant before use.	
Agencies may only use personal information for purposes to which it is relevant.	AUSTRAC has responsibility for ensuring that the information released to its clients is for an appropriate purpose - also see Privacy Principle 4. AUSTRAC staff are made aware of the importance of the need to ensure that, as far as they can, they are convinced that the information supplied to clients is consistent with the stated purpose it was requested for and consistent with the MOU.

Principle 10 - Limiting the use of personal information to the purposes for which it was collected.	
Agencies may not use personal information for purposes other than for which it was collected, except: (a) with the consent of the person; (b) to prevent a serious and imminent threat to a person's life or health; (c) as required or authorised by law; (d) where reasonably necessary for the enforcement of criminal or revenue laws; or (e) for a directly related purpose. In the case of exception (d), but not otherwise the use must be logged.	AUSTRAC must ensure that information is not given to clients unless directly relevant to work and in accordance with conditions set out in FTR Act and MOUs.
Principle 11 - Preventing the disclosure of personal information outside the agency.	
Agencies may not disclose to anyone else personal information, with the same exceptions as in Principle 10(a)-(d), plus an additional exception where the subject of the information is reasonably likely to be aware of the practice of disclosure (or reasonably likely to have been made aware under Principle 2). The recipient of information under one of these exceptions may only use it for the purpose for which it was disclosed	This provides for release of information but it is also why releases of information must be carefully considered and recorded.

AUSTRAC Security Procedures

7.17 AUSTRAC impressed the Committee with its consciousness of the need to secure the sensitive information which is provided to it. For

example AUSTRAC adheres to a range of security procedures designed to protect this information. The range of security procedures is as follows:

- **Physical security.** The AUSTRAC head office at Chatswood, Sydney is a secure building. For example, guards are located on its floors at key risk times; external doors are fitted with card access facilities and are subject to a security monitoring system; staff are issued with photo ID cards; and sensitive areas, such as the computer facility, have digital combination locks and passive infra red detectors.

- **Personnel security.** Every person working within AUSTRAC premises (whether employees, contractors or otherwise) is security cleared.

- **Data security.** Data is protected from corruption and misuse. The security measures include a requirement that all internal access be controlled through the issue of log-on and protected passwords; all PCs linked to the system have the floppy media drive disabled; clear desk rules are applied; and all secure waste is either shredded on the premises or contracted out to a security waste firm for pulping and recycling.[5]

7.18 All information received by AUSTRAC, whether received by electronic means or via paper reporting, is treated as confidential.

7.19 In April 1991 the Privacy Commissioner conducted a privacy audit of AUSTRAC, focusing on suspect transaction reports. The auditors concluded that AUSTRAC had a moderately high level of inherent risk. However, this finding 'was modified by the assessment that there also existed a high level of security in place and a strong security culture exhibited' within AUSTRAC.[6]

Access to FTR Information

7.20 The FTR Act states that the Commissioner of Taxation and ATO officers are entitled to access to FTR data, and that other specified agencies can access the data at the discretion of the Director of

---

[5] Submission No. 13, (AUSTRAC) pp. 180-183.

[6] *Privacy Act 1988* Section 27(1)(h) - Cash Transaction Reports Agency - Suspect Transaction Reports - Audit Report - Information Privacy Principles 4-11. Document tabled by Mr Coad on 10 June 1993. (Evidence, Mr Coad, p. 192.)

AUSTRAC.[7] Apart from the ATO, the other agencies which may have access to FTR information are the AFP, NCA, ASC, State and Territory police forces, NSW Crime Commission, NSW ICAC and the Queensland CJC.

7.21 Online access to the AUSTRAC database is set at six levels, as follows:

Level 0	No access
Level 1	Indicator of a report - name and address response with a message that the report is restricted.
Level 2	Abridged details of a report - transaction summary - date, report type, amount, transaction type, postcode of cash dealer, BSB number (bank branch identification code), account number, report number.
Level 3	Access to significant cash transaction report, international currency report and abridged suspect transaction report. Full details from a suspect report are available only when AUSTRAC has specifically referred the suspect report to that agency.
Level 4	AUSTRAC access only - to all reports other than suspect transaction report specials (see level 5).
Level 5	AUSTRAC access only - to a special database on reports including suspect transaction report specials. These include suspect reports concerning law enforcement personnel which may be subject to internal affairs investigations.[8]

7.22 The number of officers (excluding AUSTRAC) having access to the database at levels 1,2 and 3 is as follows[9]:

---

[7] FTR Act Section 27. Also see the discussion later in this chapter under the heading 'Should ATO have statutory right of access to FTR data?'

[8] Submission No. 13, (AUSTRAC) p. 63.

[9] AUSTRAC - Updated Statistics. Document tabled by Director AUSTRAC on 8 June 1993. (Evidence, Mr Coad, pp. 6-7.)

Table 7.1 Officers Having Access to Database

Access Level	Agency	Suspect Reports	Significant Cash Reports
Indicator of a report (Level 1)	ATO	277	–
	State law enforcement agencies (LEAs)	–	–
	Commonwealth law enforcement agencies	39	–
Abridged report (Level 2)	ATO	185	–
	State LEAs	59	–
	Commonwealth LEAs	194	–
Full report (Level 3)	ATO	234[10]	696
	State LEAs	25	84[11]
	Commonwealth LEAs	78	311

7.23 AUSTRAC provided data on the number of searches, and the type of searches, made of the database between 1 July 1992 and 31 December 1992. Those details are as follows[12]:

[10] Full report of a suspect transaction is available only to an agency when AUSTRAC has specifically referred the report to that Agency.

[11] State law enforcement agencies have access only to significant cash transaction reports reported in their home state.

[12] Submission No. 12, (AUSTRAC) p. 60.

Table 7.2 AUSTRAC Data on Searches

	AUSTRAC	Total AUSTRAC clients	ATO	Federal Agencies	State Agencies
System Access					
Number of log ons	5,746	11,931	6,516	4,349	1,066
Average number per work day	45	93	51	34	8
Searches:					
By name	38,894	64,293	32,775	25,871	5,647
Other	51,039	30,649	15,154	12,510	2,985
Total	89,933	94,942	47,929	38,381	8,632
Average number of searches per log on:	15.7	8	7.4	8.8	8.1
Information Retrieved (000's)					
Name searches	649	673	343	275	55
Other searches	46	26	14	11	1
Total	695	699	357	286	56

Number of ATO Officers with Access to FTR Data

7.24 The Australian National Audit Office (ANAO) carried out a security audit of AUSTRAC, including issues relevant to data security. Amongst other things, the audit recommended that persons who had not logged on to the AUSTRAC database for a considerable period should lose

their access privilege to do so. As a result, AUSTRAC followed the practice of deleting persons who had not logged on for six months or more. So far as ATO are concerned this resulted in the removal of access privileges from almost 28 per cent of the ATO officers with access to the AUSTRAC database:

Table 7.3 Number of Officers With Online Access to AUSTRAC Data

User Agency	June 1991	June 1992	June 1993
ATO	550	966	696
Commonwealth Law Enforcement Agencies	223	360	311
State Law Enforcement Agencies	135	117	84
AUSTRAC	51	68	64
TOTAL	959	1511	1155

(The June 1993 figure follows the culling referred to above.)[13]

7.25 These figures suggest that ATO has not used the AUSTRAC data to the extent originally anticipated and that access privileges were granted more widely than was in fact necessary.

7.26 During public hearings the following exchange took place on this point:

> **Senator O'CHEE** - The number of on-line users at the ATO has been culled quite substantially. Do you have any information as to the basis of that culling?
>
> **Mr Coad** - Yes. It was culled by us. In our submission we say that, at the outset, we judge the on-line access to law enforcement on our assessments. That will be debated a little more in Melbourne, because some will say that we have gone too

[13] Submission No. 13, (AUSTRAC) pp. 61 and 185-186, and document entitled AUSTRAC Updated Statistics tabled by Mr Coad during the Committee's public hearings on 8 June 1993.

far. Basically, the on-line access to law enforcement is to the key intelligence areas of the police forces.

As far as the Tax Office is concerned, AUSTRAC does not have any final say as to the access because the Act permits any tax officer to have access to the database. In practice, I signed an agreement with Mr Boucher, the then commissioner, that would circumscribe that access in light of the privacy principles, but the actual degree of access was very much left to the Tax Office. Since it was enthusiastic to try it, probably in the early days it was given wider scope than what the utility of it would later produce. There are many primary audit areas and whatnot where the data would be unlikely to produce any information that was relevant to it.

When we were audited last year by the Australian National Audit Office, it made a suggestion to us that we should consider culling the database. We adopted that suggestion; we cull it every six months. The Taxation Office's figures fell significantly. I think that was largely because we overdid it in the first instance.

Senator O'CHEE - I think you are right. Many of the officers who do the primary investigation in the ATO would probably not really get much utility from the information that is provided. A cynical person could say that they probably would not have the skills to utilise it either. But it still concerns me that we have 696 ATO people as at June 1993 who are on-line users of AUSTRAC data yet we only have 311 people in the Commonwealth law enforcement agencies and 84 people in State law enforcement agencies.

Senator KEMP - Do you want more?

Senator O'CHEE - It seems that we have many people who perhaps are not getting a lot of utility out of it.[14]

Should ATO have Statutory Right of Access to FTR Data?

7.27 The FTR Act provides that the Commissioner of Taxation and ATO officers are *entitled* to access to the data and that law enforcement agencies (including Customs) can access the data only at the discretion of the Director of AUSTRAC. This distinction in terms of the basis for access to FTR data between the revenue agency and law enforcement agency would seem to have resulted in access that is too indiscriminate, bearing in mind the privacy sensitive nature of the data in question. Also, the

[14] Evidence (Mr Coad) pp. 55-56.

substantial culling of users carried out in 1993 suggests that wide access is unnecessary for ATO purposes. AUSTRAC conceded this point in its submission where it is remarked that 'in the first instance, the granting of online access (particularly to the Australian Taxation Office) may have been too wide. The culling of users, consistent with the Australian National Audit Office's recommendations ... appears to have wound back the online access to what may be more permanent levels.'[15]

7.28 It is desirable that access to FTR data should be closely guarded. Obviously, it should not be accessible by any person who does not have a genuine need to do so. In the case of ATO it seems that access has been too generous and should be limited.

Recommendation 7: The Committee recommends that the FTR Act be amended so that ATO no longer has a *right* of access to FTR data but has access to FTR data on the same basis as law enforcement agencies, that is, on the basis of a Memorandum of Understanding entered into with the Director, AUSTRAC.

Civil Liberties Representation on Advisory Committees

7.29 The VCCL pointed out that there was limited external scrutiny of AUSTRAC through the auditing function of the Privacy Commissioner and the Australian National Audit Office. However VCCL argued that privacy interests could be safeguarded through allowing for civil liberties representation on key advisory committees.

7.30 The Attorney-General established a Ministerial Advisory Committee on the Financial Transaction Reports Act in 1991. That Committee is chaired by the Secretary of Attorney-General's Department, and includes representation by the ABA, AAPBS, CUSCAL, the finance sector unions as well as AUSTRAC. The other key advisory committee is AUSTRAC's own liaison committee. AUSTRAC has a liaison committee which liaises with cash dealers, and another which liaises with law

[15] Submission No. 13, (AUSTRAC) p. 53.

enforcement and revenue agencies. The Director of AUSTRAC has raised with VCCL the possibility of a separate civil liberties committee.[16]

7.31 There is considerable merit in having civil liberties representation on key advisory committees. There should be a civil liberties representative on the Ministerial Advisory Committee on the FTR Act, and also on one of AUSTRAC's advisory committees (or on a separate civil liberties committee established by the Director of AUSTRAC).

7.32 The Director of AUSTRAC indicated during evidence to the Committee his support for this proposal:

> In relation to the civil liberties advisory group, I agree that we should have such a body. I would hope that the representatives on that body would not see us as 'big brother', and that we would be able to make a positive contribution to it. I will seek to set up such a group on the advice of the Privacy Commissioner.[17]

Recommendation 8: The Committee recommends that a civil liberties representative be appointed to the Ministerial Advisory Committee on the FTR Act.

Recommendation 9: The Committee recommends that the advice of the Privacy Commissioner be sought by the Director of AUSTRAC whether to appoint a civil liberties representative either to an existing AUSTRAC advisory committee, or to establish a separate advisory committee on privacy and civil liberties issues.

Deletion of Data

7.33 The FTR Act makes no provision for the deletion of old or spent FTR information from the AUSTRAC database. Indeed, paragraph 38(1)(b) of the Act requires the Director of AUSTRAC 'to collect, *retain*, compile, analyse and disseminate FTR information'. (Emphasis added.) The retention of large, and growing, volumes of quite sensitive personal financial data is a matter of obvious concern to civil liberties groups.

[16] Submission No. 12, (VCCL) p. 51.

[17] Evidence (Mr Coad) p. 210.

7.34 Interestingly, the problem of volume of data also appears to be a matter of concern for AUSTRAC itself. Attorney-General's Department noted in its submission that in 1992 'the Director [of AUSTRAC] sought guidance on whether some records concerning transactions worth less than $10,000 could be destroyed after 3 months' retention in order to facilitate analysis of the residual information.'[18] The Department commented that 'permanent retention of information considered to be of no use may ultimately hamper use of that part of the retained information which is possibly relevant to criminal activity or tax evasion, thus undermining objectives such as facilitating administration of the laws of the Commonwealth and maximising use of FTR information for taxation purposes.'[19]

7.35 The Department took the view that the Director could delete the information but only if prior approval had been obtained from Australian Archives, because the information constituted 'Commonwealth records' within the meaning of the *Archives Act 1983*. This difficulty could be overcome by specific provision in the FTR Act or Regulations empowering the Director of AUSTRAC to authorise deletion of FTR information from the database because the Archives Act does not apply where destruction of Commonwealth records is allowed by a law.

Recommendation 10: The Committee recommends that the FTR Act be amended to give the Director of AUSTRAC power to authorise the deletion of FTR information from the AUSTRAC database in appropriate circumstances.

[18] Submission No. 35, (Attorney-General's Department) p. 150.

[19] ibid p. 151.