New South Wales
Council for
Civil Liberties

New South Wales Council for Civil Liberties Inc

149 St Johns Road
Glebe NSW 2037
Australia
Ph 61 2 9660 7582
Fax 61 2 9566 4162

Correspondence to:

PO Box 201
Glebe NSW 2037
Australia

DX 1111 Sydney
Email office@nswccl.org.au
www.nswccl.org.au

Assistant Secretary
Criminal Law Branch
Attorney-General's Department
Robert Garran Offices
National Circuit
BARTON ACT 2600

via e-mail : aml.reform@ag.gov.au

Dear Sir/Madam,

RE: **Comments on the Exposure Draft of the Anti-Money Laundering and Counter-Terrorism Financing Bill 2005**

1. The NSW Council for Civil Liberties ('CCL') thanks the Attorney-General's Department for the opportunity to make this submission.

2. CCL is concerned about the proposed AML/CTF legislation as it introduces an expansive regime for the widespread breach of individual rights, especially the right to privacy, without adequate justification or procedural safeguards. It also represents a denial of government administrative accountability. In doing so, this legislation potentially violates Australia's obligations under international law. Lastly, this regime will undermine the legal system in Australia by requiring lawyers to breach client confidentiality at each stage of their relationship. This submission will outline the relevant principles and international law, followed by a more detailed examination of how specific provisions raise the above concerns.

International obligations

3. The CCL notes that the Financial Action Task Force ('FATF') *recommendations* are provided by an international body under the Convention against Financing of Terrorism. They are not treaty obligations. As such, the FATF recommendations cannot override Australia's actual treaty obligations. The most important of these are the ICCPR, which is partially incorporated in the *Privacy Act 1988*. Other treaties include the International Convention on the Elimination of All Forms of Racial Discrimination, which is incorporated into domestic law by the *Racial Discrimination Act 1975*.

4. The *Privacy Act* and the ICCPR set out the fundamental principle that all human beings are entitled to the basic liberty of privacy and anonymity. The principle is stated in Article 17 of the ICCPR,

   'No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.

   'Everyone has the right to the protection of the law against such interference or attacks.'

5. The National Privacy Principles (NPP) give effect to Article 17 by establishing principles of data quality, access and correction, and limitation and security.

6. While Australia entered a reservation under Article 17 ICCPR for "national security", CCL believes that this reservation should be interpreted strictly. It does not authorise blanket invasion of the rights if individuals, families, and whole communities.

7. CCL also highlights the fact that standards set out in the ICCPR are only minimum standards. The Human Rights Committee has stated that the ICCPR minimum standards does not lower the standards set out in other international human rights treaties. In addition to obligations under the ICCPR and its optional Protocols, Australia has other binding treaty obligations. These include the obligation to eliminate 'all forms of racial discrimination' under CERD, as incorporated by the *Racial Discrimination Act*.

8. The *Racial Discrimination Act* provides:

   'It is unlawful for a person to do any act involving a distinction, exclusion, restriction or preference based on race, colour, descent or national or ethnic origin which has the purpose or effect of nullifying or impairing the recognition, enjoyment or exercise, on an equal footing, of any human right or fundamental freedom in the political, economic, social, cultural or any other field of public life.' (section 9(1))

9. The *Racial Discrimination Act* also provides:

   'a person requires another person to comply with a term, condition or requirement which is not reasonable … [and this] … has the purpose or effect of nullifying or impairing the recognition, enjoyment or exercise, on an equal footing, by persons of the same race, colour, descent or national or ethnic origin as the other person, of any human right or fundamental freedom' (section 9(1A))

   This is held to be a form of racial discrimination.

10. CCL submits the *Racial Discrimination Act* and the *Privacy Act*, as well as other relevant treaties, establishes the framework in which the proposed legislation must be assessed. These earlier international obligations are at least as important, as a matter of principle, constitutionally and internationally, as any FATF recommendations.

11. Together, the *Privacy Act*, the *Racial Discrimination Act*, the HREOC Act and other legislation incorporating international treaties create a framework that recognises minimum international standards of human rights and civil rights and liberties. Most importantly they recognise a minimum entitlement to privacy, and to be free from racial discrimination.

12. CCL recognises the importance for Australia to combat terrorism and the threat of terrorism, and supports properly adapted and proportionate measures towards this end. However it is more important to recognise that the government is required to formulate and implement these policies within the limits of all of the government's international law obligations. It would be anomalous for the Australian government to breach its binding treaty obligations, including its long-standing international human rights obligations, in order to follow non-binding recommendations of an international body.

Consultation

13. CCL welcomes the Attorney-General's public inquiry on the proposed legislation. However CCL notes that the bill was written between March 2004 and December 2005. During these eighteen months, industry groups were consulted through Industry-Government working groups to ensure the proposed measures do not create an unreasonable compliance burden on businesses. However, it seems these consultations were limited to industry groups and legal advisors. Individuals in the community received neither information about the proposed laws, nor any opportunity to engage in similar consultations with the government.

14. In contrast to the access given to industry groups, public interest and human rights bodies were only given the opportunity to comment on the proposed legislation after the draft legislation and some of the rules have been written.

15. The process, as a result, was extremely unbalanced. The government recognised that the policy to combat terrorist financing must be balanced with businesses efficacy; but it seems to have failed to recognise that legislation to combat terrorist financing must uphold minimum international standards of human rights and civil liberties. Businesses that take on surveillance duties on behalf of the government were consulted; during the course of consultation the government made the commitment to minimise the proposed regime's 'red tape' and compliance burden.

16. In contrast, individuals whose financial affairs and personal liberties will be exposed to government and private scrutiny in such an unprecedented way were not informed, much less consulted.

17. CCL is deeply concerned that this process means that in drafting this legislation, the government has not been able to receive any feedback about its likely impact on individuals, nor take into account interests and concerns other than those of business and industry groups. Industry and business concerns about compliance costs are undoubtedly crucial, due to their role in the proposed public-private financial monitoring regime. However the interests of individuals who will be subject to this regime are even more crucial.

18. In the current global environment, there is already widespread concern that fundamental human rights are being eroded in the course of combating 'terrorism'. The Australian government presents itself as a nation that upholds democratic principles of government and civil society in contrast to terrorist regimes. It is important that in fighting terrorism the legislature is vigilant in protecting fundamental rights and does not itself undermine the very values and beliefs it is seeking to protect from external threats. This need to do so is even more pressing in Australia than in other western democracies as Australia lacks a bill of rights by which the courts can test the compatibility of legislation with fundamental rights.

Recommendation 1 The Attorney General establish a consultation process with civil rights and community interest groups and form Community-Government working groups for future projects.

Constitutional Basis and Misleading Title

19. We refer to our observations above on the range of Australia's international law obligations. Again, we emphasise that the assessment of the proposed legislation cannot be done in isolation, instead it must be assessed in light of the framework of international rights and civil liberties that Australia has recognised, some of which are incorporated into domestic law.

20. While the title of the proposed legislation implements FATF recommendations, the details of the monitoring regime established by the legislation goes beyond from this stated purpose in many ways. A number of submissions to the Senate Legal and Constitutional Committee have expressed great concern at the fact that the ambit of this proposed legislation exceeds the FATF recommendations. It exceeds FATF recommendations in the range of services caught in the first and second tranches. It also exceeds FATF recommendations by allowing extraordinary powers to investigate offences other than money laundering and terrorist financing offences. Industry groups have also expressed its concern that this legislation goes far beyond even the system in the UK and USA.

21. The ambit of the legislation blatantly violates the object clause (section 3). Businesses are required to report their suspicions that information provided by a client or prospective client 'may be relevant' to the commissioning of crimes against 'taxation law' (section 39(1)(d)(i)), or any 'law of the Commonwealth or territory' (section 39(1)(d)(ii)). Moreover, under section 99(a) AUSTRAC has the power to allow any 'designated agency' to access information collected 'for the purposes of performing the agency's functions'. The government clearly expects to use this system of State-Industry surveillance to detect non-serious crimes, taxation and other petty fraud. This side-steps the need to pass contentious legislation that targets such crimes directly.

22. Most importantly from the civil libertarian point of view, there is no limit on the uses to which information collected under this legislation could be put. In effect, legislation and regulations supposedly designed to capture and combat serious international crime will routinely capture civil and petty criminal offences or breaches.

23. Agencies such as Centrelink and the Child Support Agency already access AUSTRAC records to capture social security frauds. It is conceivable that other government and non-government 'partner agencies' could access such information. While AUSTRAC currently controls access through memoranda of understanding, and would continue to do so under the proposed legislation, CCL is concerned that the legislation itself imposes no limit on who may access sensitive financial and personal information, nor establish guidelines or criteria to determine who may be granted access.

24. CCL is further concerned that any memoranda of understanding are confidential and not open to external scrutiny. Given the expansive nature of the surveillance regime contained in this legislation (and the proposed "second tranche") it is inappropriate that there are not clear and public limitations on the use of data collected by AUSTRAC. Any difficulties involved in drafting such restrictions are not an adequate justification for allowing unfettered access to this data.

25. This feature of the legislation violates NPP8 and international protocols on collection and use of personal information. Under NPP 8, as under globally accepted standards, the uses for personal information must be stated at the time of collection, or as soon as practicable afterwards. Uses and disclosure of personal information is required to be tied to the purposes stated at the time of collection, or to uses and disclosures necessary for that purpose. These protocols are as significant as the FATF recommendations in setting global standards of regulation and conduct.

26. CCL submits it is not permissible to deviate from these international standards by omitting control mechanisms in the legislation. Administrative discretion should only be exercised within recognised international standards.

27. Such wide discretion and powers also make it questionable whether all parts of this proposed legislation would be supported by the External Affairs power in the Constitution. Instead of the current provisions that require reporting of 'suspicious transaction' that is potentially relevant to the investigation of 'an offence' against the undefined body of domestic civil, criminal, international, and overseas laws, CCL urges the government to adopt a much more strict definition of 'suspicious matters'.

Recommendation 2

The legislation include the following requirement:

"a 'suspicious transaction' is a transaction that is

a) potentially relevant to the investigation of 'an offence' directly related to the financing of terrorism.

b) a transaction may also be suspicious if it is relevant to an 'offence' under an Australian law or a binding international treaty that has a reasonable connection to the financing of terrorism.

28. Similarly, allowing potentially unlimited access to any federal, state or overseas agency, 'for the purposes of performing the agency's functions', clearly takes the ambit of the legislation beyond its title and object clause. The proposed legislation in its current form allows any public or private agency to apply for access to information collection under this legislation, even if the agency's functions has no connection to money laundering or financing of terrorism. Even if it may be argued that social security fraud or income tax evasion could contribute to the financing of terrorism, by being part of the same national and global economic system, it is clear that there are other agencies, whose purpose is to promote international and national security, that would be able to make more effective and targeted use of such data than, for example, the Child Support Agency.

29. This failure to include limitations or accountability mechanism is also a clear violation of established data protection and privacy principles.

Recommendation 3

The legislation include the following limitation on AUSTRAC discretion,

'AUSTRAC may allow a designated agency to access data collected under this legislation if AUSTRAC is satisfied

a) the agency's purpose is reasonably related to preventing the financing of terrorism, and

b) the data will be used for purposes and investigations that are reasonably related to preventing the financing of terrorism.'

30. Alternately, CCL recommends the legislation includes an expanded objects clause that acknowledges the fact that the legislation would exceed FATF recommendations, as well as comparable laws in the UK and USA.

Recommendation 4

Insert an alternate objects clause:

'An Act to:

a) control the financing of terrorism under FATF recommendations;

b) allow the government to routinely record and monitor the financial affairs of all people through private businesses and corporations;

c) allow Australian and overseas agencies to access and use such information for any purposes, including purposes beyond the scope of Australia's international law obligations, and including uses that may violate Australia's other international law obligations.'

Invasion of Privacy

31. We refer to individuals' fundamental civil rights and liberties under ICCPR and national privacy law above. Seen against these basic rights, the legislation's identification requirements (Part 2), reporting requirements (Part 3), and monitoring requirements (Part 4) creates grave concerns.

32. Under these provisions, service providers and their employees are required to report suspicious 'matters'. There is no corresponding requirement in the legislation that employees with such responsibilities are to be trained to a nationally certifiable standard. This creates huge potential for misreporting and over-reporting. Likewise businesses are likely to over-report to avoid penalties and even serious criminal sanctions (s.39(4) for failure to report) under the proposed legislation, particularly as the legislation provides no penalties for wrongful or negligent reporting or misuse of collected information.

33. This imbalance in the reporting requirements and penalty regime creates three main concerns for individual civil liberties.

34. Firstly this proposed regime overrides the anonymity privacy principle. Under the customer identification requirements, individuals will be forced to identify themselves to every service provider, for everyday transactions such as purchasing jewellery, seeking financial planning advice, and buying or selling a house. Under the 'know your customer' requirements, individuals will also be subject to continual monitoring of their financial activities and assessment by their service providers even for the most innocuous transactions, such as a $50 overseas transfer.

35. These requirements violate the ICCPR privacy principle that interference with personal privacy is permissible under very limited circumstances. CCL notes that section 110 makes it a crime to provide a service on the basis of customer anonymity, which directly overrides the NPP 8. Such invasion is exacerbated under the proposed regime, because it will be private businesses that undertake the monitoring, recording, and reporting, effectively transforming the private sector into an extension of Australian security and intelligence agencies. This concerned is addressed below.

36. Secondly, the lack of quality control provisions in the legislation offends against the data quality principle. The information collected is highly likely to be of dubious quality, as each 'suspicious matter' will be the subjective judgment of people who are unlikely to know the relevant laws. The experience in the UK demonstrates that without rigorous quality and quantity control, there will be poor quality over-reporting. This not only violates the data quality principle, which is a basic tenet of the right to privacy, it ironically nullifies the effectiveness of the legislation.

37. The proposed regime also offends against individuals' access and correction rights under privacy laws, as the privacy-exempt suspicious transactions list thus created will be exempt from FOI law. It is uncertain how AUSTRAC will deal with information that appears to be unreliable, but it is submitted that the object of the legislation – prevention of terrorist financing – cannot be met if government or international investigations proceed on unreliable information. CCL notes that these secrecy provisions go beyond any existing regime in Australia, and even beyond the controversial wire-tapping laws in the United States. The CCL urges the government to reconsider the secrecy provisions, and to include a provision allowing ex post facto notice to be given to the affected individuals.

38. In a recent consultation meeting with the Attorney General Department and AUSTRAC, the point was raised that existing requirements of customer notification is inadequate, as many individuals are unaware of the fact that their international fund transfers are already recorded. The degree of customer ignorance about the level of surveillance of their financial activities is likely to increase if all businesses acquire an obligation to monitor and report, but not a corresponding obligation to notify customers that they are being monitored and reported.

39. CCL suggests the legislation impose a clear customer notification requirement for transactions that are not exempt from the privacy laws. In other words, the legislation should, at a minimum, provide a mechanism by which individuals may be warned against financial products or transactions that are likely to generate a 'suspicious transactions' report.

> Recommendation 5
>
> The legislation includes:
>
> a) a notification to customer that businesses and service providers are required to monitor and report their financial activities at the beginning of the 'business relationship';
>
> b) a notification to customers that business and service providers are required to monitor and report their financial activities *each time* the customer undertakes an activity that is likely to be 'suspicious'.

40. CCL also submits that the legislation ought to include provisions that allow individuals to access their AUSTRAC files. Instead of the blanket ban on access to the 'suspicious transactions' list, it is suggested that the onus of proof be placed on AUSTRAC or the Attorney-Generals Department. AUSTRAC or the Attorney General would be required to consider each request on its merits, with a final right of refusal if the information is deemed to be sensitive information and in the interests of national security.

41. Alternately it is suggested that individuals have the right to require an impartial, third-party intermediary to access the individual's files and undertake audit of the 'suspicious matters' reports.

> Recommendation 6
>
> The proposed legislation provides a mechanism whereby individuals may request access to 'suspicious matters' reports filed against them, or request an independent third party to access and audit the 'suspicious matters' reports.

42. CCL is also concerned about the requirement to keep employee records, which are currently exempt from privacy legislation. It is suggested that employee records should become subject to privacy legislation.

43. To ensure that public interest in civil liberties are not eroded by the proposed regime, it is suggested the legislation include provisions that penalizes businesses for wilful or negligent false reporting.

> Recommendation 7
>
> Insert the following clause:
>
> "Business commit an offence against this act if the business:
>
> a) grossly negligent or wilfully false reporting customer and employee information;
>
> b) failure to notify customers at the beginning of their business relationship of the degree of reporting required, and before each transaction that is likely to generate a suspicious transactions report against the customer;

44. Lastly it is suggested a 'good faith' and 'reasonable steps' defence be available to any penalties associated with businesses' failures to comply with their reporting and monitoring obligations. This would bring the Australian legislation in line with UK legislation.

> Recommendation 8
>
> A defence of 'good faith' and 'reasonable steps taken' be available to business who fail to comply with their reporting and monitoring obligations under this proposed legislation.

Potential for Racial Discrimination

45. We refer to our observations on Australia's obligations under the Convention to Eliminate All Forms of Racial Discrimination, incorporated by the *Racial Discrimination Act 1975*.

46. CCL notes with concern the lack of precision in the definition of 'suspicious matters'. In conjunction with the decision to give private businesses and corporations the power to decide which matters and transactions are 'suspicious' and the lack of training or quality control mechanisms, this could become a state-sanction method of racial and other discrimination.

47. The criteria for 'suspicious matters' has been left to the regulations, and a draft criteria under the sample rules include such intangible and hard-to-define matters as manner and circumstances. CCL believes that assessment of suspicious matters made under these criteria is liable to be impression-based and highly subjective. Part 9 (Countermeasures) of the proposed legislation allow the government to prohibit financial transaction to and from residents of particular countries. The combined effect of these provisions could be to encourage unwarranted 'suspicion' against persons of particular ethnic backgrounds or appearances. If so, this may create discrimination against individuals from non English-speaking backgrounds, because their behaviour, language, and lack of familiarity with Australian institutions and laws could lead to false 'suspicions transactions' reports against them.

48. For this reason, CCL recommends that these above provisions be preceded by the statement that assessment and monitoring of 'suspicious matters' should be undertaken, subject to the *Racial Discrimination Act*. It is also suggested individuals be expressly entitled to bring complaints against reporting entities or agencies on the basis of racial discrimination, as well as privacy violation.

Recommendation 9

The Act states that this legislation seeks to recognize and uphold the principles established in the *Racial Discrimination Act 1975*.

Lack of Accountability

49. This legislation raises concerns by drastically reducing the degree to which the government and government agencies will be accountable for Australia's national security and intelligence operations. It does so by 'privatising' the state's intelligence functions to private businesses and service providers.

50. Individuals cannot control corporations and business actions to the degree that government actions may be held accountable under administrative and public law. The proposed legislation may mean that individuals will only have recourse to the Privacy Commissioner or Industry Ombudsman for any redress or information about data collection about them.

51. Express exemptions from FOI and Privacy laws is also a concern. As highlighted above, the lack of penalty provision about misuse or disclosure is exacerbated by the fact that individuals will not be able to use the usual administrative avenues of appeal and redress. In the absence of public accountability, exemption from FOI laws creates another layer of protection for private reporting entities, in addition to any claims of commercial confidence that may prevent businesses from being held accountable for their reporting activities.

52. The outsourcing to corporations also creates concern about who will have access to the stored records of customers and transactions. Individuals in these data will be easily identifiable by their unique customer number. Even if businesses are controlled by existing security requirements, the sheer amount of data that will need to be collected and stored creates the very real prospect that business data may be stolen or misapplied.

53. While some of the above matters may dealt with in the regulations, CCL believes it is crucial to ensure that existing privacy protection will not be sidelined or eroded under the proposed legislation. As such we suggest a provision specifying that if a small business or service provider acquires monitoring and reporting obligations under the proposed legislation, they will also acquire security and privacy obligations under the *Privacy Act*.

54. For this reason, CCL suggests the addition of a penalty provision, that penalises deliberate supply or use of data for commercial purposes.

55. CCL also submits that regulations and guidelines about what constitutes 'suspicious matters' ought not be left to the regulations. These are fundamental to any assessment of the legislation's proportionality and validity. This reinforces our earlier submission that statements of principle or guidelines protecting fundamental civil liberties should be part of the legislation, to minimise the lack of accountability for the actions of private entities.

56. Lastly, to address the basic concern that this legislation 'privatises' administrative functions from the government to the private, commercial sector, CCL suggests provisions in the legislation that makes the government ultimately accountable for any violations of privacy and other democratic rights suffered by individuals. This is critical to ensure that if information is wrongly or negligently reported and used against individuals, there is no uncertainty about who is liable for such misuse and subsequent abuse of individual privacy.

Recommendation 10

The following clauses be included in the proposed legislation:

a) it is an offence under this Act for reporting entities to deliberately supply or use data collected under this Act, for commercial gain, or for purposes other than purposes permitted under section 3 of this Act.

b) the government will be deemed responsible for private reporting entities' breaches, if the government is aware of the breach and fails to stop the breach or prosecute the reporting entity;

c) AUSTRAC and the Attorney General is responsible for ensuring a national level of education and training for businesses and service providers that will have monitoring and reporting responsibilities;

d) AUSTRAC and the government is responsible for agencies that access and use information collected under this Act;

Lawyer-client confidentiality

57. The proposed legislation requires legal practitioners to assess their existing and prospective clients, perform "know your client" duties, and report any suspicious matters to AUSTRAC. These requirements breach the fundamental principle of confidentiality at the basis of the legal system. While other professions may accommodate the onerous reporting and monitoring obligations, the legal profession is founded on the basis that each person has the basic right to legal representation; and they have the basic right for their lawyer to present their strongest case to other parties and to the Court. Clients must be certain that information provided to their solicitors will remain confidential; this ensures that clients have the confidence to disclose their whole case to the solicitors, which ensures the proper functioning of the justice system.

58. Solicitors owe fiduciary duties to their clients, which will be breached if they act in a way contrary to their clients' interests. Legal practitioners are already subject to strict regulations on every aspect of their practice. Legal practitioners cannot advise anyone on how to break the law.

59. If lawyers are required to assess their clients for 'risk' of committing AML/CTF crimes, and form suspicions against their clients, the lawyers will be forced to violate their position as legal advisors, and become akin to an adversarial party. The result will be a head-on collision between lawyers' professional ethics and their obligations under this proposed legislation.

60. Secondly, while the 'first tranche' of the proposed legislation only claims to cover legal practitioners who offer financial services in competition to financial entities, the ambit of the legislation may already cover every aspect of their practice. The CPA's Senate submission highlighted their concern that the definition of 'loan' under section 5 is too broad: it appears to cover any credit facility, including accountants and lawyers who provide services on a deferred-payment system. If so, all lawyers' work will be a 'designated service' under the proposed legislation, unless lawyers demand upfront payment from all clients. This would be so whether the lawyer holds a trust account, or provide innocuous services such as drafting a will.

61. This result requires lawyers to consistently violate people's basic right to have proper legal representation. As financial industry groups have pointed out, accountants and lawyers' clients are likely to have accounts with banks and other government agencies already, and would have satisfied those institutions' customer identification procedures. It would be unnecessarily and arbitrarily invasive for accountants and lawyers to undergo further customer identification. It may

also violate the ICCPR's protection from 'to arbitrary or unlawful interference with [everyone's] privacy … or correspondence'

Recommendation 11
Legal practitioners be exempt from AML/CTF obligations; or the government consults with legal professional bodies to establish procedures that do not violate the fundamental right of client confidentiality and people's right to proper legal representation.

Impact on other laws

62. As noted above, this legislation creates a privacy-exempt suspicious transactions list. This will have much wider and serious ramifications for individuals than can be seen from this proposed legislation alone.

63. For example, individuals are required to undergo security clearances for a large number of government and non-government employment. If the privacy-exempt suspicious transactions list is accessible to government agencies and designated private or international agencies, individuals could be penalised for false information wrongly reported against them.

64. Under proposed Australian Citizenship laws, the Minister for Immigration and Indigenous and Multicultural Affairs would have the discretion to refuse Australian citizenship to anyone who does not prove their identity. If the Minister has discretion to refuse Australian citizenship, it is conceivable that a mistaken or false report about an individual on the AUSTRAC privacy-exempt suspicious transactions list would influence the Minister's exercise of his or her discretion.

65. The list could also affect other migration matters, potentially raising racial discrimination concerns.

Conclusion

66. CCL would be happy to elaborate on any of the above points should the department wish.

67. If the proposed legislation violates these international standards, it ironically undermines the aim of Anti-Terrorism treaties and laws – to maintain and protect a democratic way of life and to uphold fundamental rights and liberties.

Yours faithfully,

Rhonda Luo
Member

Anish Bhasin
Committee Member