AFP
AUSTRALIAN FEDERAL POLICE

GPO Box 401 Canberra City ACT 2601
Telephone 02 6131 5804 Facsimile 02 6132 6079
Email peter.whowell@afp.gov.au
www.afp.gov.au
ABN 17 864 931 143

13 January 2014

Executive Director
Australian Law Reform Commission
GPO Box 3708
Sydney NSW 2001

By email: brigit.morris@alrc.gov.au

Dear Professor McDonald,

Inquiry on Serious Invasions of Privacy in the Digital Era

Please find attached the AFP's submission in response to the Issues Paper on Serious Invasions of Privacy in the Digital Era. I apologise for the delay in providing the AFP's formal response to the Inquiry.

The AFP has no objection to the publication of its submission on the ALRC's website.

If you require further assistance in this matter, please do not hesitate to contact me.

Yours sincerely

Peter Whowell
Manager
Government Relations

AFP
AUSTRALIAN FEDERAL POLICE

Issues Paper on

Serious Invasions of Privacy

in the Digital Era

Submission by the

Australian Federal Police

13 January 2014

Introduction

The Australian Federal Police (AFP) welcomes the opportunity to make a submission in relation to the Australian Law Reform Commission's (ALRC) Issues Paper on Serious Invasions of Privacy in the Digital Era (Issues Paper).

2. On 12 June 2013, the then Attorney General of Australia, Mark Dreyfus QC MP, asked the ALRC to conduct an Inquiry into ways in which the law might prevent and redress serious invasions of privacy in the digital era.

3. The terms of reference for the Inquiry outline what the ALRC have been asked to consider.

4. The AFP's submission responds to the following questions:

    - Question 1 – What guiding principles would best inform the ALRC's approach to the Inquiry and, in particular, the design of a statutory cause of action for serious invasion of privacy? What values and interests should be balanced with the protection of privacy?

    - Question 3 – What specific types of activities should the ALRC ensure are not unduly restricted by a statutory cause of action for serious invasion of privacy?

    - Question 6 - What should the test be for the actionability of a serious invasion of privacy? For example, should an invasion be actionable only where there exists a 'reasonable expectation of privacy'? What, if any, additional test should there be to establish a serious invasion of privacy?

    - Question 7 – How should competing public interests be taken into account in a statutory cause of action? For example, should the Act provide that:

        - competing public interests must be considered when determining whether there has been a serious invasion of privacy; or

        - public interest is a defence to the statutory cause of action?

    - Question 12 – In any defence to cause of action that the conduct was authorised or required by law incidental to exercise a lawful right of defence of person or property, should there be a requirement that the act or conduct was proportionate, or necessary and reasonable.

    - Question 15 – What, if any, activities or types of activities should be exempt from a statutory cause of action for serious invasion of privacy?

- Question 27 – In what other ways might current laws and regulatory frameworks be amended or strengthened to better prevent or redress serious invasions of privacy?

Overall the AFP's position is that law enforcement agencies are already subject to an extensive authorisation and accountability framework in relation to how they manage, collect and store personal information, particularly where the information is obtained through an intrusive means and should therefore be exempt from any cause of action. The existing framework contains mechanisms to protect individuals through the use of external oversighting bodies and civil and criminal penalties. Any new requirements which impact on the effectiveness of the current regime should be avoided and if amendments are required, these should be made within the existing regime. That being said, the AFP is of the view that the current controls are adequately robust.

Question 1 – What guiding principles would best inform the ALRC's approach to the Inquiry and, in particular, the design of a statutory cause of action for serious invasion of privacy? What values and interests should be balanced with the protection of privacy?

5. The AFP believes that the key issues to consider in response to this question are:

    - The mechanisms contained in the current framework, which sufficiently balance an individual's right to privacy by considering whether the proposed intrusion is reasonable in all the circumstances;
    - The robustness of the current regime, which is achieved through the oversight provided by external bodies and protections contained with the relevant legislation that authorises the intrusion;
    - The enhancements that will be made to privacy protections with the introduction of the Australian Privacy Principles (APPs);
    - The need for individual's to take ownership of their own privacy; and
    - The benefits of privacy education.

6. The AFP considers the mechanisms that currently govern the collection of personal information by the use of intrusive means already achieve a balance between the individual's rights to privacy and whether the proposed intrusion is reasonable. By way of example, the process for obtaining a telephone interception warrant under the *Telecommunications (Interception and Access) Act 1979* (TIA Act) includes an independent assessment of a number of factors by a Judge or Member of the Administrative Appeals Tribunal (AAT) before a warrant is issued. These factors are set out in section 46 of the TIA Act and include:

- how much the privacy of any person or persons would be likely to be interfered with by intercepting under a warrant communications made to or from the service to be intercepted; and
- the gravity of the conduct constituting the offence or offences being investigated; and
- how much the information obtained from the proposed interception would be likely to assist in connection with the investigation by the agency of the offence or offences; and
- to what extent methods of investigating the offence or offences that do not involve intercepting communications have been used by, or are available to, the agency; and
- how much the use of such methods would be likely to assist in connection with the investigation by the agency of the offence or offences; and
- how much the use of such methods would be likely to prejudice the investigation by the agency of the offence or offences, whether because of delay or for any other reason.

The AFP submits that this process adequately considers the extent that an individual's privacy is interfered with and determines whether the proposed interference is reasonable in the circumstances.

7. The AFP strongly supports the need to balance an individual's right to privacy with other values and interests. The AFP considers that the following factors as suggested by the ALRC must take precedent over an individual's right to privacy:
    - The proper administration of government and matters affecting the public or members of the public;
    - National security and safety;
    - The prevention and detection of criminal and fraudulent activity; and
    - The protection of vulnerable individuals within the community.

8. It is essential that any statutory cause of action does not impede the ability of law enforcement agencies to continue to appropriately exercise, or provide support for, legitimate law enforcement, intelligence and related functions. Moreover investigative and covert techniques that intrude on the privacy of individuals are already subject to strict legislative controls that prohibit misuse of personal information and oversighting regimes. Therefore, in the AFP's opinion, an additional layer of protection is unnecessary.

9. In addition to the above factors, the AFP submits that the following matters have already been sanctioned by legislation and should therefore override an individual's right to privacy in the proposed cause of action and be exempted from its scope:

- an action or activity that is authorised or required by an existing law;
- an action or activity that is sanctioned by an order of a court or tribunal; and
- an action or activity that is already regulated by existing legislative restrictions to guard against the improper use of personal information.

This submission is expanded at paragraph 18 below.

10. The AFP also considers that the ALRC needs to recognise the differences between public sector agencies and private sector organisations when formulating any statutory cause of action. Public sector agencies are already subject to multiple layers of scrutiny and independent oversight in relation to all aspects of their activities, including in relation to the collection, use and storage of information. Both sectors are required to comply with different legislative regimes and these differences need to be recognised. Although, in the privacy space both sectors will shortly be bound by the one set of APPs. This argument is expanded at paragraph 14 in relation to the external bodies that oversight the AFP.

11. Further, in relation to the incoming APPs, there may be merit in the ALRC delaying its consideration of the creation of a statutory cause of action until such time as the APPs have become fully embedded. Given that the APPs expand the existing privacy regime to further regulate how personal information is dealt with, it may be pre-emptive to address any gaps in this area, until such time as the impact of the new regime is fully understood. The ALRC would then be in a better position to identify any remaining gaps and address these.

12. Another factor that the ALRC needs to balance when designing any statutory cause of action is that individuals need to accept some responsibility for their actions and ensure that they take steps to protect their own privacy. In the digital era individuals now make the decision to live part of their lives online in an information rich and difficult to regulate environment. Individuals need to fully understand the potential consequences of disclosing personal information in this environment. While there will always be some individuals within our society who lack the capacity to protect their privacy, it is important for individuals to have the opportunity to make informed decisions about their privacy. To this end, educating people regarding technical literacy is essential so that they have an understanding of the data they are creating and potentially disclosing. The AFP believes that both government and industry should play a role in this education process. The AFP currently contributes to this process by participating in programs such as Think u

Know. This program raises awareness amongst Australian children, parents and teachers of safety issues on the Internet.

Question 3 – What specific activities should the ALRC ensure are not unduly restricted by a statutory cause of action for serious invasions of privacy?

13. The AFP believes that law enforcement agencies already operate in an environment where the use of personal information is strictly controlled and should not be further restricted by the development of a statutory cause of action. The AFP regularly needs to balance an individual's privacy against being able to effectively protect society from criminals to enforce the criminal law. The specific activities that the AFP believe should not be unduly restricted by the cause of action are ones that are:

    - already sufficiently regulated; and
    - agency mandated activities.

14. The AFP considers that law enforcement agencies are already heavily regulated. In the AFP's case, it is subject to the following accountability framework:

    Internal

    - AFP Values and Code of Conduct; and
    - Part V of the AFP Act – which sets out the Professional Standards Regime, this also includes oversight by the Commonwealth Ombudsman.

    External

    - Oversight by Australian Commission for Law Enforcement Integrity in relation to corruption matters;
    - Oversight by Parliament, through the Senate Estimates process and examination of Annual Report by the Parliamentary Joint Committee on Law Enforcement, as well as specific inquiries by Parliamentary Committees;
    - Australian National Audit Office for assurance activities;
    - Oversight by the Ombudsman relating to the use of covert information gathering powers for controlled operations, telecommunications interception and access to stored communications and surveillance devices;
    - Certain counter terrorism legislation is reviewed by the Independent National Security Legislation Monitor;

- The Courts and the AAT in relation to warrant and authorisation applications; and
- The Courts in relation to prosecution actions.

15. Law enforcement agencies are required, in accordance with their governing legislation, to undertake certain activities. In the AFP's case this is contained in section 8 of the *Australian Federal Police Act 1979* (AFP Act) and includes:

    - The prevention of crime and the protection of persons from injury and death, and property from damage, whether arising from criminal acts or otherwise in relation to the Australian Capital Territory, the laws and property of the Commonwealth.

    - Safeguarding the Commonwealth interests

    - Assisting and cooperating with Australian or foreign:

        (i) law enforcement agencies;

        (ii) intelligence or security agencies; or

        (iii) government regulatory agencies.

16. The AFP is also required to comply with any directions issued by the Minister. The current Ministerial direction sets out the priorities for the AFP including:

    - Countering the threat of terrorism to the safety and security of Australians and Australian interests, inside and outside Australia, including through countering violent extremism;

    - Supporting the implementation of the Commonwealth Organised Crime Strategic Framework and preventing, deterring, disrupting and investigating serious and organised criminal activities impacting on the interests of the Australian community;

    - Safeguarding the economic interests of the nation from criminal activities such as serious fraud, money laundering, corruption, intellectual property crime and technology enabled crime;

    - Contributing effectively to Australia's border management and security, particularly protecting Australia from people smuggling, including prevention, deterrence and disruption;

    - Contributing effectively to the Government's international law enforcement interests including matters involving cooperation to combat transnational organised crime, responses to emergencies, law and order capacity building missions, and participation in

internationally mandated peace operations;

- Countering the threat of cyber-crime including through achieving and maintaining a technological edge over criminals;

- Leading and managing the law enforcement and crime prevention aspects of aviation security;

- Ensuring that specific individuals, establishments and events, identified by the Australian Government as being at risk, are protected;

- Implementing the relevant recommendations of the Federal Audit of Police Capabilities *New Realities: National Policing in the 21st Century*, particularly achieving a revised program structure and consolidation of most of the core, lapsing and terminating funding into base funding; and enhancing core investigative capabilities;

- Contributing actively to broader government programs or initiatives where their successful implementation requires the engagement of law enforcement capabilities;

- Where possible identifying emerging criminal threats to the national interest and, for issues in which the AFP have operational expertise, advising on appropriate approaches, to counter such threats.

Undertaking these activities will inevitably involve interfering with an individual's privacy on occasions. Where this does occur every effort is made to respect an individual's privacy by ensuring the information that is obtained is properly protected and dealt with whilst in the possession of the AFP. Indeed, the various Acts contain provisions which set out how the information can be used by law enforcement agencies and how it must be protected. This argument is expanded below commencing at paragraph 20.

17. Additionally, the oversight of the Commonwealth Ombudsman and the requirement that activities under the TIA Act are reported to the Attorney General provide additional layers of protection to assure the community that the AFP and other interception agencies use their powers under the TIA Act appropriately.

18. The AFP submits that any actions or activities that are currently:

- authorised or required by an existing law;
- sanctioned by an order of a court or tribunal;

- an action or activity that is already regulated by existing legislative restrictions to guard against the improper use of personal information; or
- the subject of an international agreement or obligation

should not be unduly restricted by the creation of a cause of action. Actions or activities of these type have their own specific regimes that must be complied with before the particular action or activity is considered to be sanctioned by law. Any perceived limitations in those regimes should be addressed in those regimes, not in a statutory cause of action.

19. Section 180F of the TIA Act is an example of a law that incorporates privacy protection as part of the authorisation process before sanctioning access to telecommunications data. The assessment considers whether the interference with the privacy of any person is justifiable having regard to the likely relevance and usefulness of the information that is expected to be obtained and the reason why the information is sought.

20. Further, regimes such as the TIA Act, the *Surveillance Devices Act 2004* (SD Act) and the *Crimes Act 1914* in relation to search warrants and controlled operations, have safeguards and prohibitions in place to ensure that information obtained through the use of an intrusive method is carefully managed. By way of example, section 46 of the SD Act provides that any information obtained from the use of a surveillance device under a warrant, an emergency authorisation or a tracking device authorisation is to be kept in a secure place with access restricted to only those people who are entitled to deal with it.

21. Similarly, the TIA Act imposes strict prohibitions on how intercepted information (refer to Chapter 2, Part 2-6) and stored information (refer to Chapter 4, Division 6) must be dealt with. If those prohibitions are breached criminal or civil charges may be pursued.

22. The AFP considers that these additional safeguards and prohibitions further negate the need for law enforcement agencies to be subject to restrictions relating to a statutory cause of action for serious invasions of privacy.

23. Further protection is achieved by reporting regimes contained within the various pieces of legislation. For example, the SD Act contains specific provisions (see section 49 and 50) on reporting and record keeping requirements that must be complied with after an application for a warrant has been granted. This includes an inspection regime by the Commonwealth Ombudsman, with a report being provided to Parliament on the outcome of that inspection.

24. The TIA Act also contains reporting and record keeping requirements in relation to accessing stored communications. This includes a report being provided to the Minister that is tabled before Parliament. (Refer to Chapter 4, Part 4-2)

25. An additional layer of accountability is achieved through the imposition of penalties where legislative requirements are not complied with. By way of example, section 45 of the SD Act imposes penalties for failing to deal appropriately with sensitive information in accordance with the provisions of the SD Act.

26. As outlined in paragraph 21, the TIA Act also contains civil and criminal penalties if the information is misused. (see Chapter 3, Part 3-7 for intercepted information and section 182 for stored communications).

27. There are also existing mechanisms in place whereby an individual may seek compensation if they suffer loss or injury from the use of a surveillance device. Compensation is available under the SD Act:

- where the use of that device is prohibited by the laws of the State of the Territory in which the use occurs; and
- the surveillance is not in accordance with the SD Act.

If these criteria are met, the Commonwealth is liable to pay compensation to the individual for the loss or injury.

28. Therefore, noting the internal and external accountability frameworks with which the AFP must comply, including specific legislative regimes which contain penalties for misusing the information, the AFP submits that a further layer of privacy protection is unnecessary.

Question 6 - What should the test be for the actionability of a serious invasion of privacy? For example, should an invasion be actionable only where there exists a 'reasonable expectation of privacy'? What, if any, additional test should there be to establish a serious invasion of privacy?

29. The AFP believes that the test for the actionability of a serious invasion of privacy should include whether the act or activity that constitutes the invasion of privacy is:

- authorised or required by an existing law;
- sanctioned by an order of a court or tribunal; or
- an action that is already regulated by existing legislative restrictions to guard against the improper use of personal information; or

- the subject of an international agreement or obligation.

30. Further, the ALRC should give consideration as to whether it is appropriate for individuals who are committing or attempting to commit criminal offences to have a reasonable expectation of privacy or whether this expectation should be displaced by the criminal activity. Particularly, where the personal information is obtained by law enforcement agencies under an existing law and is required for the purpose of a criminal investigation.

Question 7 – How should competing public interests be taken into account in a statutory cause of action? For example, should the Act provide that:

- **competing public interests must be considered when determining whether there has been a serious invasion of privacy; or**
- **public interest is a defence to the statutory cause of action?**

31. As outlined in the response to question 3, the AFP considers that the public interest must be considered when determining whether there has been a serious invasion of privacy. In certain circumstances, the AFP would argue that the public interest outweighs an individual's right to privacy. These circumstances include:

    - the proper administration of government and matters affecting the public or members of the public;
    - National security and safety;
    - the prevention and detection of criminal and fraudulent activity;
    - the protection of vulnerable individuals within the community;
    - an action or activity that is authorised or required by an existing law; and
    - an action or activity that is sanctioned by an order of a court or tribunal.

32. The AFP's response to whether the public interest should be a defence to a statutory cause of action is outlined below.

Question 12 – In any defence to statutory cause of action that the conduct was authorised or required by law or incidental to exercise a lawful right of defence of persons or property, should there be a requirement that the act or conduct was proportionate, necessary or reasonable?

33. The AFP submits that there is no need for the additional requirement that an act or conduct was proportionate, necessary or reasonable when the act is

authorised, regulated or required by law. As outlined above, the actions that are authorised or required by law have their own specific thresholds that must be complied with before the action or activity will be permitted. For example, in the case of an application for an telephone interception warrant a Judge or AAT member is required to satisfy themselves that in addition to determining whether the facts satisfy the legislative threshold that the action or conduct is proportionate, necessary and reasonable.

Question 15 – Exemptions

34. As outlined above, the AFP believes that law enforcement agencies are already heavily regulated and subject to appropriate independent oversight. Therefore, if a statutory cause of action is created it is recommended that these agencies should be exempt from its operation.

35. A particular concern for the AFP is that if it is not exempt from a statutory cause of action that the legitimate performance of its law enforcement functions will be compromised. The concern relates to the potential for a statutory cause of action for serious invasions of privacy to:

- a reduce or impact upon the AFP's legitimate use of developing technologies for investigative purposes;
- enable individuals to find out whether they are the subject of covert operations;
- expose sensitive operational capabilities in legal proceedings; and
- enable litigants to launch collateral challenges against the AFP during prosecutions, thereby diverting resources to defending actions against the lawful exercise of legitimate law enforcement powers.

36. The AFP is mandated in the Ministerial Direction to

> *Counter the threat of cyber-crime including through achieving and maintaining a technological edge over criminals*

However, depending upon how the statutory cause of action is framed it may impact or reduce the AFP's ability to legitimately use emerging technologies to meet this objective.

37. The concern in relation to points 2 -3 above, is that in the course of defending legal proceedings information could be released that would enable an individual to determine if they are the subject of covert surveillance or reveal details of sensitive operational capabilities. Responding to legal proceedings also has the potential to divert substantial resources away from the AFP's role of fighting crime to instead defending the lawful exercise of law

enforcement powers. It is for these reasons that the AFP submits that a law enforcement defence is not sufficient to prevent any statutory cause of action from unduly interfering with law enforcement.

38. The AFP believes that either a specific exemption is required or exemptions based on the *Privacy Act 1988* are required to prevent the statutory cause of action from unduly interfering with law enforcement. For example, the exemptions in Australian Privacy Principle 6 and 8 or a permitted general situation could be applied to the operation of the statutory cause of action.

Question 27 – In what other ways might current laws and regulatory frameworks be amended or strengthened to better prevent or redress serious invasions of privacy?

39. The ALRC have asked the AFP to consider whether the divergence in the scope of state surveillance laws has any impact on the AFP's functions. As the AFP mainly relies on the Commonwealth law to perform its functions, the divergence in the state surveillance laws has not had a significant impact upon the AFP's ability to undertake its functions.

40. The ALRC have also asked whether the difference between interception as opposed to accessing stored communications in the TIA Act creates any difficulties for the AFP. The requirements to obtain a warrant for both activities are similar in that an application must be made to a Judge or AAT Member, who needs to be satisfied of certain matters (outlined at paragraph 6) before they can grant the application. In that sense the differences between the two activities creates no issues for the AFP.

41. Further, in June 2013 the Parliamentary Joint Committee on Intelligence and Security released its report into its Inquiry into Potential Reforms of Australia's National Security Legislation. This review included an assessment of the existing telecommunications interception regime. For the purposes of this Inquiry this included consideration of the need to strengthen the safeguards and privacy protections currently in place. The AFP therefore considers that it would be an unnecessary duplication of work for the ALRC to include this issue in its current review.