

# submission

Privacy NSW submission to the Joint Working Group on National Investigation Powers on behalf of the Leaders Summit on Terrorism and Multijurisdictional Crime

on the Discussion Paper

## **Cross border investigative powers for law enforcement**



privacy**nsw**

*Issue date: May 2003*

**Privacy NSW**  
**Submission on Discussion Paper Cross border investigative powers for law enforcement**

The Discussion Paper deals with four separate law enforcement areas where issues of cross-border jurisdiction arise:

- controlled operations,
- assumed identity,
- protection of witness identity, and
- surveillance devices.

While each of these areas touch on privacy concerns, this submission will pay closer attention to the surveillance proposals. We appreciate that the purpose of the Discussion Paper is to adapt existing jurisdictional provisions to the needs of cross-border investigation and that it is not primarily about the way these existing provisions operate within jurisdictions. The Discussion Paper does however provide an opportunity to reflect on the adequacy of the privacy protection built into existing legislation on the relevant aspect of criminal investigation. Having said this, we would emphasise that our submission focuses on the provisions discussed in the Discussion Paper and does not seek to analyse or critically assess the adequacy of protective measures in the legislation currently applicable in any Australian jurisdiction.

The views expressed are those of the Office of the NSW Privacy Commissioner and should not be taken to reflect the official position of the New South Wales Government.

## **Surveillance**

The Discussion Paper proposes model legislation to cover four kinds of surveillance, listening, optical, tracking and data surveillance devices.

The main thrust of the surveillance proposals is to create a unified system of warrants for authorising the use of different kinds of surveillance devices where these are used in cross-jurisdictional investigations. Legislative coverage of the four kinds of surveillance activity is currently uneven as between jurisdictions. Victoria has adopted reasonably comprehensive surveillance regulation. NSW and other jurisdictions have laws dealing with listening devices and laws restricting access to computers, but leave optical and tracking forms largely unregulated. The proposed legislation may therefore involve some pressure towards greater standardisation as between jurisdictions. The possibility that this pressure will encourage some jurisdictions to enact a unitary system to cover both intra-jurisdictional and inter-jurisdictional surveillance is recognised on page 211 of the Discussion Paper.

In New South Wales the possibility of unitary surveillance legislation was canvassed in the NSW Law Reform Commission *Report No 98 Surveillance: An Interim Report*, and in official responses to the Report. In June 2002 Privacy NSW issued The

*Privacy Commissioner's Position on the Law Reform Commissions Report 98 Surveillance: An Interim Report* (copy attached). This submission supported the basic principle of unitary legislation to cover both overt and covert forms of surveillance but made a number of recommendations in relation to the administration of covert surveillance authorities that would be relevant to your Committee's Reference.

At page 231 the Discussion Paper raises the issue of whether offences to which cross border powers should apply should be limited to those carrying a possible sentence of more than three years or should apply to any offence provided that the authorising officer considers it justifies the issue of a warrant. In support of the latter position it is suggested that experience would lead one to believe the powers would not be sought for minor regulatory offences. It is argued in the Discussion Paper that an "any offence" threshold would enable surveillance devices to be used in relation to environmental and firearms offences and would avoid inconsistencies between jurisdictions as a result of different maximum penalties.

The general trend for law enforcement agencies to adopt more intrusive forms of surveillance-based investigation makes it difficult to use past experience as a guide to future limits on the scope of surveillance. In these circumstances there is value in establishing a threshold in relation to offences. A three year threshold may inevitably be somewhat arbitrary, but serves an important symbolic privacy function in recognising that surveillance, by its very nature, is privacy invasive and that it requires a strong public interest to overcome objections to its use.

The Discussion Paper presents a persuasive argument for having a single form of warrant for the various kinds of inter-jurisdictional surveillance, and this is consistent with the position Privacy NSW adopted on the NSW Law Reform Commission's Surveillance Report. However the benefits of a unitary warrant requirement could be undermined by the suggestion on pages 237-238 that a separate regime might apply to the issue of tracking devices. If a single legal form of warrant is to be used for the different kinds of surveillance activity it would be desirable that the prescribed wording adequately describe the kind of surveillance authorised by it and direct the attention of the judicial officer to any issues associated with this kind of surveillance. For instance clause 9(2) could include consideration of the form of surveillance proposed.

The commentary on clause 7 suggests a relatively permissive process as to who can apply for a warrant, for the purpose of expediting applications by non-Police conduct and anti-corruption agencies. The lack of a precise definition of law-enforcement officer could have a serious net-widening effect in regard to investigative bodies pursuing activities that fall outside the scope of serious crime in other jurisdictions. The term "law enforcement officer" should be more clearly defined in relation to the kinds of offences for which warrants could be issued.

Clause 32 seeks to protect the giving of evidence that would prejudice the effectiveness of law enforcement methodologies or the maintenance of a lawful method of procedure. We need to be careful to ensure that this provision does not promote a level of secrecy that could effectively deny fairness to accused persons or compromise the openness of the trial process. Criminal trials offer one of the few

sources whereby members of the public can gain an insight into the effect of various forms of surveillance. This process provides an essential means of ensuring democratic accountability for the way surveillance powers are used. Therefore methods of surveillance should be disclosed at trial and publicly reportable to the greatest extent possible, consistent with individual safety and the security of the operations themselves.

Once a claim for non-disclosure is made Clause 32(2) places the onus on the presiding officer in a proceeding to be satisfied that disclosure is necessary to ensure a fair trial, to establish the legality of the surveillance or is otherwise in the public interest. It is questionable whether this strikes the appropriate balance. In the nature of such proceedings, a defendant's capacity to argue the issues of fairness and legality may be handicapped at the outset. The presiding officer is likely to have limited guidance on how to apply the public interest test.

In this context, the "reasonable expectation of prejudice" test in paragraphs (1)(d) and (e) could be seen to represent too low a threshold. Having regard to the examples provided in the second set of dot-points in commentary on page 309 a more appropriate test would be one similar to that in paragraph 4(b) in relation to making suppression orders, that is, whether operations or methodologies would be compromised. Law enforcement officers seeking to protect their operations or methodologies could be required to satisfy the court that a disclosure would compromise them.

We are not concerned with. However we consider the scope of paragraphs (d) and (e) need to be qualified to ensure reasonable exposure of the way evidence involving electronic surveillance has been collected. The scope of the public interest test in subclause (2)(c) should be broadened, so that a decision whether to withhold or suppress information does not depend solely on the view formed by a judicial officer based on submissions by police or prosecutors.

Clause 34 requires reasonably comprehensive reporting to the Court that issues a warrant. However this does not flow through to the kind of reports that would allow the public to assess whether an appropriate balance was being struck between privacy and law enforcement. Comprehensive reporting provides an important measure of accountability in circumstances where one cannot expect law enforcement authorities to specifically reveal details of each warrant authorised.

Clause 35 does not require an Annual Report to specify the kinds of surveillance activity to which a warrant should apply, for instance how many warrants are issued for listening devices, tracking devices or other purposes. Without a breakdown of the kind of activities covered by warrants the value of such a report to members of the public who seek to understand the scope of surveillance activity is significantly limited. It is difficult to see that the adoption of a single warrant should prevent the compilation of statistics that will indicate the kind of surveillance activities that have been authorised given that proposed clause 10(d) requires an application for a warrant to specify the kind of surveillance device that it is proposed to use.

The Discussion Paper fails to address the issue of when individuals should be directly informed that a surveillance exercise has been conducted against them or

that information about them is held as a result of a covert surveillance operation. Section 20 of the Listening Devices Act 1984 (NSW) provides an instance of the kind of provision which could be made, although the restricted circumstances in which directions can be made under section 20 make it a less than effective means of scrutinising the way warrants are granted and used. A provision of this nature would give individuals whose privacy has been breached a useful opportunity to assess the appropriateness of the surveillance used without compromising their own privacy.

Part 4.3 of the 1994 *Review of the Long Term Cost Effectiveness of Telecommunications Interception* (Barrett Report) made favourable recommendations in relation to proposals to disclose the fact of surveillance where no critical law enforcement information had been collected. The broader scope of the surveillance regime proposed in this legislation provides a stronger case for such disclosure.

It is not possible for individuals to rely on current privacy or freedom of information legislation to find this out. Section 25 of the NSW Privacy and Personal Information Protection Act excludes the Police and other law enforcement agencies from having to comply with the information protection principles, including relevantly section 13 which otherwise allows a person to gain access to personal information held about them. The law enforcement exemptions in section 37 of the Federal Freedom of Information Act and Schedule 1 of the NSW Freedom of Information Act also effectively prevent access through such legislation.

Proposed clause 30(4)(a)(ii) creates an exception for the prohibition on disclosing information collected through surveillance where the information has entered the public domain. This could amount to a very broad and difficult to define exemption which could seriously undermine the interests in security and privacy, which the section as a whole might be expected to protect. It is difficult to establish convincing evidence as to whether the information has entered the public domain at any particular time. Even if it is proved to have been published legitimately, the manner in which this occurred might still not be consistent with protected interests. If it is necessary to have such an exception it should be more narrowly applied to information that is contained in a publicly available publication.

Clause 30(5)(c) permits the use, communication or publication of protected information for relevant proceedings. Relevant proceedings are defined to include proceedings for the protection of a child or intellectually impaired person or a disciplinary proceeding against a public officer. These amount to very broad exemptions and the justification for them is unclear. It would be appropriate to specify that they should apply to the more serious and difficult to detect offences.

### **Controlled operations**

We would emphasise the importance of clause 17 of the Model Controlled Operation Provisions as a means of ensuring that controlled operations do not entail unnecessary or unregulated incursion on individual privacy in circumstances where the extent of such incursions are already prescribed by law, such as telephone interception, electronic surveillance search and seizure and identification procedures.

For clarity the Model Bill should more clearly define what is meant by laws relating to forensic or identification procedures. Presumably this refers to laws under which individuals are liable to a penalty for failing to identify themselves to authorised officers.

The Discussion Paper indicates that it will be an offence to disclose information about a cross-border controlled operation, however clause 27 may be too broadly expressed. Broadly interpreted this provision could expose individuals to much greater liability than is presumably intended. For example the statement; “He is a cop”, uttered by an innocent bystander in relation to an officer who, unbeknown to the bystander, is participating in a controlled operation would apparently amount to an offence under this provision. It would appear logical to make the offence conditional on the individual’s knowledge that a controlled operation had been authorised.

### **Assumed identities**

The legal authorisation of assumed identities for law enforcement operatives creates a number of privacy concerns.

Firstly authorising law enforcement officers to adopt an assumed identity has the potential to unfairly infringe on the right of individuals to a private life by exposing their actions to the scrutiny of people who claim to be other than they are. Privacy serves an essential purpose in a democratic society in allowing people to form relationships and participate in public life by selectively disclosing or concealing aspects of themselves. Undercover surveillance by State institutions, whether by electronic or human means, can undermine this process. For this reason the process of authorising law enforcement officers to assume a false identity needs to be regulated in the same way as other forms of intrusive surveillance.

Secondly the adoption of an assumed identity has the potential to adversely impact on a third party who may be mistaken for the identity that is assumed. There is no provision in the proposed legislation that would specifically prevent an authorised person assuming the identity of another person. It may well be impracticable to limit the scope of an authority to made up identities. However it seems reasonable to assume that a higher test should be satisfied before an authority to assume another person’s identity is granted, having regard to the grave risks this could have for the person who is impersonated. It is perfectly reasonable to require the authorising agency to consider appropriate safeguards in circumstances where a person’s life could be placed at risk as a consequence of their identity being assumed by a law enforcement officer as part of an undercover operation.

Thirdly the creation of assumed identities represents a potential threat to the integrity of institutions and record systems through which individuals legitimately establish their identity. The proposed legislation makes provision for registrars of births, deaths and marriages to create records and issue certificates which could be characterised as false. While clauses 7 and 8 provide a mechanism for removing an entry, this is dependent on an authorised officer cancelling an authority. There is no absolute requirement to correct registers once the purposes of the operation have

been wound up. Unlike the creation of assumed identities for protected witnesses, the need for an assumed identity for a law enforcement purpose is likely to expire once the operation is completed. There is a case for stronger safeguards to prevent the process of establishing identity for which these registers provide an essential basis from being compromised. Similar considerations apply to the non-mandatory issue of forms of identification by non-Government organisations.

The offence provision in clause 26 is open to similar objections to those referred in relation to clause 27 of the provisions for controlled operations. That is, it is possible for a person who knows the person concerned under their real identity to commit the offence as stated even if they are entirely unaware of the existence of an authority to adopt an assumed identity. Again there is a need to relate the offence to knowledge of an authority.

### **Protection of witness identity**

The provisions under Part 2 are limited to the protection of police operatives giving evidence in criminal proceedings as distinct from civilians seeking protection under a witness protection program. Consequently the privacy interest in ensuring that the identity of protected witnesses is adequately safeguarded needs to be balanced against the protection of accused persons from any unfairness where operatives have obtained evidence through an assumed identity.

In comparison to the kind of concerns raised in relation to clause 27 of the provisions relating to controlled operations and clause 26 of the provisions relating to assumed identities, the protection of the identity of an operative under clause 12 only applies to their identity when giving evidence in court proceedings. There is therefore less of a risk of a person breaching clause 12 unwittingly.

The protection for those on witness protection programs under Part 3 requires a different balancing exercise so far as privacy is concerned. The issue is whether it strikes an appropriate balance between fairness to the accused and the adequate protection of witnesses, having regard to the reasonable expectations of witnesses arising under a witness protection program. My concern relates in particular to the adequacy of the protection provided to witnesses under clause 19 (4) (7) and (8) which allow the court to give leave to disclose the identity of a witness. These provisions do not require the court to take into account any views or evidence which the witness may wish to put in relation to the granting of leave under subclause 4 or in relation to orders made under subclause (8), even though the effect of giving leave may put them at risk. Nor do they explicitly give an affected witness the right to be represented when putting such views.

Clauses 18(2)(c) and 19(9) raise similar concerns as the offence provisions in clause 27 of the provisions relating to controlled operations and clause 26 of the provisions relating to assumed identities. That is, having regard to clause 16(4) the provisions could be used unfairly to penalise a person who is not a party but who is present in the court, is aware of the true identity of the witness but is unaware that he or she is the subject of an assumed identity certificate or an order made by the court under clause 19(8).

## **Conclusion**

In the time available we have not been able to make detailed recommendations on all the privacy issues identified in the draft Model Bill. Rather we have sought to identify the privacy issues that need further attention in subsequent drafting. Please contact John Gaudin of this Office on (02) 92685581 if you wish to discuss any of the issues raised in this submission.