Victorian Government Submission – *Reform of Australia's electronic surveillance framework discussion paper*

Introduction

Victoria welcomes the opportunity to respond to the Department of Home Affairs' *Reform of Australia's electronic surveillance framework discussion paper* (the discussion paper). This submission aims to assist the Department of Home Affairs by presenting key matters to consider as it develops a new, modernised electronic surveillance legislative framework. The views expressed do not constitute a statement of settled Victorian Government policy on matters of Commonwealth responsibility.

Victoria strongly advocates for sustained engagement with states and territories through the development of any proposed legislative reform of electronic surveillance arrangements, noting that changes to Commonwealth legislation may require subsequent legislative reform at a state level.

The proposed reforms are likely to impact Victorian law enforcement and integrity bodies who currently rely on, or have an interest in, the relevant Commonwealth surveillance legislation. The Victorian Government entities that have contributed to the contents of this submission include:

- The Department of Justice and Community Safety (DJCS);
- The Department of Premier and Cabinet (DPC);
- Victoria Police;
- the Office of the Public Interest Monitor (PIM); and
- the Office of Public Prosecutions (OPP).

Several independent Victorian Government bodies may contribute with their own individual submissions. These may not necessarily present agreed Victorian Government policy positions.

This submission commences by offering some general comments on issues arising from the discussion paper, before providing answers to the specific questions posed by the Department of Home Affairs.

General Comments

The need for a modernised framework

Victorian recognises the need to modernise the current framework governing electronic surveillance in Australia, noting that the current legal framework is complex, inconsistent and creates uncertainty about the activities that can be undertaken. Victoria supports, in-principle, the Commonwealth's effort to develop a single, consolidated legislative framework, provided Victoria continues to be appropriately consulted.

Notably, a significant concern for Victoria Police is the rapid rise in, and more sophisticated use of, technology to commit crime in recent years. It is imperative that the new legislation equips law enforcement agencies (LEAs) with the necessary tools to prevent and respond to crime both now and in the future. New legislation must be proportionate to the threat faced and adaptable enough to keep pace with the technological advancements and the changing threat environment.

The new framework should allow LEAs interoperability between jurisdictions, by recognising their respective authorities to access data. Improved information-sharing arrangements between intelligence agencies such as the Australian Security Intelligence Organisation (ASIO) and LEAs would also facilitate disruption and intervention strategies.

Clarity on implications for state legislation

Victoria would need to carefully consider whether any changes to the Commonwealth framework would require consequential amendments to the *Surveillance Devices Act 1999* (SD Act Vic) and how it would impact on Victorian oversight and integrity bodies. Victoria requests ongoing consultation (including on any subsequent exposure draft legislation) on any potential impacts and interactions with the existing legislation, policies, procedures in each state and territory.

Victoria requests that the Commonwealth clarify whether it anticipates requesting states and territories to amend, replace or override existing legislation to facilitate the new framework to ensure consistency between jurisdictions. Again, states and territories will need adequate time to consider the implications of any settled legislative proposals from the Commonwealth. More detail on the Commonwealth's inter-jurisdictional analysis and preferred reform approach would be useful to support Victoria assessing the impacts of proposed Commonwealth reforms on Victorian surveillance device laws.

Systemic review of police oversight

Work relevant to the proposed Commonwealth reforms is currently being undertaken in Victoria. The Victorian Government is currently conducting a systemic review of police oversight, addressing recommendation 61 of the Royal Commission into the Management of Police Informants (Royal Commission) and building on the work of the Parliament of Victoria's 2018 IBAC Committee *Inquiry into the external oversight of police corruption and misconduct in Victoria.*

The Royal Commission identified that the current system of oversight of Victoria Police's coercive and intrusive powers, including electronic surveillance powers, is fragmented and inconsistent in approach, reflecting the lack of a cohesive principles-based framework for system design. The Royal Commission recommended that the Victorian Government undertake a principle-based review of the institutional and legal structures for the oversight of these police powers in Victoria to bring greater coherence to the police oversight system.

The Royal Commission also identified five key principles for designing an outcome-focused police oversight system, applying these principles to its proposed human source management oversight framework. These principles are:

- necessity and proportionality

- accountability
- effectiveness
- safety and sensitivity
- consistency.

The systemic review is considering how the application of these principles to existing compliance, monitoring, and reporting obligations could result in a more outcomes-focused, principles-based, and meaningful form of oversight, including in relation to use of electronic surveillance by law enforcement agencies. The Victorian Government expects to introduce legislation to reform Victoria's police oversight system in 2022. Victoria will keep the Commonwealth updated on these developments.

Human rights considerations

In Victoria, public authorities (such as government departments and agencies) are required to act consistently with the human rights in the *Charter of Human Rights and Responsibilities Act 2006* (the Charter). Surveillance powers may engage or impact human rights, and several the proposed reforms in the discussion paper have the potential to broaden the privacy impacts of surveillance activities, for example:

- consolidation so that a single warrant could cover a broad range of activities;
- significantly expanded definition of 'communication';
- inclusion of surveillance powers in relation to third parties and 'groups';
- sharing of information between government entities; and
- reduced authorisation requirements in time critical situations.

In addition, Victorian Government agencies must ensure personal information is managed in accordance with the *Privacy and Data Protection Act 2014*, and health information is managed in accordance with the *Health Records Act 2001*.

Overall, Victoria notes that careful consideration around privacy and human rights concerns will be required as the new framework is developed, noting that these considerations may outweigh the benefits of harmonisation for some jurisdictions and stakeholders.

Part 1: Who can access information under the new framework?

1. Do the existing prohibitions and offences against unlawful access to information and data adequately protect privacy in the modern day?

a) If so, which aspects are working well?

b) If not, which aspects are not working well and how could the new prohibition and/or offences be crafted to ensure that information and data is adequately protected?

Victoria recognises the importance of striking an appropriate balance between the use of and access to information and data and the protection of a person's or organisation's privacy. As

noted above, when exercising (or deciding to exercise), powers under the framework, Victorian agencies will be required to act compatibly with and consider the rights in the Charter. This includes a right not to have an individual's privacy, family, home, or correspondence interfered with.

In developing a new framework, Victoria supports the Commonwealth carefully assessing the appropriateness of existing prohibitions. If a new framework is implemented, existing prohibitions and offences against unlawful access should continue to be regularly and independently reviewed to ensure their adequacy.

Notably, Victoria Police considers that the current protections and protocols are effective in achieving a balance between use and access to information and privacy and that the standard of proof required to lawfully intercept information and data and the high threshold for the serious offences under investigation, provide further protection.

Victoria Police suggests consideration could be given to the issue of organised crime groups increasingly being trained in and utilising highly specialised Technical Surveillance Counter Surveillance (TSCM) equipment to 'sweep' for lawfully issued surveillance devices. They note that while there is legislation that prohibits persons from using certain types of surveillance devices, the same individuals can search for these devices without any apparent impediments or regulation.

Victoria notes that the discussion paper contemplates the possibility of enacting a Commonwealth prohibition on the unlawful use of surveillance devices to create consistency across all jurisdictions. If the Commonwealth was to contemplate enacting legislation to replace state and territory surveillance devices laws, the PIM has highlighted several matters of concern or for further consideration:

- If the Commonwealth were to legislate to replace state and territory laws in this area, it is highly likely the power to issue warrants would be vested in the Administrative Appeals Tribunal (AAT) – as is currently the case with telephone intercept warrants (the Federal Circuit Court has concurrent jurisdiction, but it is rarely exercised). Currently, all applications for surveillance device warrants are considered by Judges of the Supreme Court. The Magistrates' Court is empowered to issue tracking device warrants, but during the COVID-19 pandemic the Supreme Court has exercised that function as well.
- In the PIM's view, it is appropriate that the Supreme Court continues to consider applications for surveillance device warrants because of the highly intrusive nature of optical and listening devices installed in private homes. For example, sometimes the residence in which the devices are installed is occupied not only by the suspected offender but by others, including children, who have no involvement at all in the suspected offending. Applications made in these circumstances give rise to challenging privacy issues. The Supreme Court judges who consider surveillance device warrant applications are, mostly, experienced criminal trial judges with long criminal law experience.
- There is currently a system of mutual recognition of surveillance device warrants between most jurisdictions: see SD Act Vic Part 4A 'Recognition of Corresponding

Warrants and Authorisations'. This permits cross-border use of surveillance device warrants. Consequently, difficulties that may previously have been experienced in in cross-border use of devices no longer arise.

2. Do the existing prohibitions and offences against unlawful access to information and data adequately allow the pursuit of other objectives of societal benefit, eg. cyber security of networks, online safety, scam protection/reduction?

Victoria supports efforts to ensure the new legislation is drafted in a way that will capture future technological advances. Victoria Police notes that the current limitations on who can access information can impact on capability around cyber security of networks, online safety, and scam protection/reduction. This reflects that the legislation has not kept pace with advancing technology; for example, private entities 'owning' personal data through messaging platforms and having the ability to access communications.

3. Are there any additional agencies you consider should have powers to access particular information and data to perform their functions? If so, which agencies, and why?

Victoria supports reinstating Corrections Victoria's (CV) access to telecommunications data, in support of the security of prisons and related facilities, noting that such access would need to be balanced by applications requiring compelling justification for access to this data. Intelligence received through this access is an important tool in supporting the security of Victoria's prisons.

Prior to reform in 2015, any authority or body with functions involving enforcing the criminal law, enforcing a law, imposing a pecuniary penalty or a law protecting the public revenue was deemed to be an enforcement agency under the *Telecommunications (Interception and Access) Act 1979* (Cth) (TIA Act). This included CV and enabled access to telecommunications data for security purposes. Amendments made in 2015 reduced the list of enforcement agencies to a small number of Australian, state and territory law enforcement and anti-corruption agencies that did not include corrections services.

Correctional facilities house people who have an ongoing interest in the commission of serious criminal offences, for financial, ideological, or personal gain. Many individuals and criminal organisations are technically proficient and have very quickly adapted to exploit developments in communication technology.

Having law enforcement status would enable CV to identify users of mobile phone services to identify actors in the community supporting serious criminal activity being organised from prisons. This would include:

- preventing illicit drugs and contraband entering prisons
- preventing organised acts of violence aimed at people in the community and within prisons
- preventing serious cases of corruption
- preventing prisoners organising acts of terrorism or radicalisation from within prison.

Prior to the removal of corrections services from the legislation, CV was able to access critical information to support investigations. If further detail is required, specific examples

can be provided about how this information has successfully disrupted criminal activity in Victorian prisons.

CV frequently identifies numbers linked to offenders in prison who are actively involved in serious and organised crime, gangs, or terrorism. Integrated Public Number Database check (IPND) and Customer Call Record (CCR) enquires provide CV with the ability to identify:

- key actors involved in offending;
- staff misconduct; and
- size and scope of organised/coordinated offending (in the community and prison).

This allows preparation of internal plans to prevent offences or make a case to law enforcement to commence a criminal investigation. Without the ability to make these checks, the offences may continue.

CV plays a critical role in the detection, investigation, and prosecution of serious crime and corruption under State and Commonwealth legislation. Enforcement agency status would enable CV to collect telecommunications data where the commission of an offence or other illegal activity by use of a telecommunications device is suspected by a prisoner. The ability of CV to access telecommunications data is critical to ensuring that CV can continue to exercise the full range of its security-related functions in detecting, investigating, and prosecuting crimes, and ensuring the safety of both the correctional system and the community at large.

Separately, Victoria Police is supportive of access to particular data and information by the Australian Transaction Reports and Analysis Centre (AUSTRAC) and Australian Taxation Office (ATO) as this would benefit the community in terms of pursuing, locating, and restraining proceeds of crime.

Victoria also notes that if federal independent corruption commission is created, then consideration should be given to adding this entity to the list of agencies granted access to information and data.

4. Do you agree with the proposed considerations for determining whether additional agencies should be permitted to access peoples' information and data? Are there any additional considerations that have not been outlined above?

The proposed considerations appear appropriate to determine whether additional agencies require access to information and data to enable them to effectively perform their functions.

Part 2: What information can be accessed?

5. Are there other kinds of information that should be captured by the new definition of 'communication'? If so, what are they?

The definition of 'communication' has significant consequences and as such, must be carefully considered to ensure sufficient clarity and to assess privacy considerations. Victoria is supportive of efforts to develop a new term and/or definition that reflects the broad range of data and information that can be transmitted electronically, to ensure that available legal

protections and powers are adequately understood. This could encompass media such as machine to machine communications, augmented and virtual reality and Bluetooth.

A person can have a device in their possession, but the communication is stored elsewhere such as the 'cloud' or some other site. From the perspective of Victoria Police, it is important that this 'communication' is captured in the definition so that warrants are enforceable and enable the retrieval of the 'communication' using the device in LEAs' possession. Victoria Police also considers that the concept of communication could be usefully updated to clarify the distinction between active communication (ie. making a phone call) versus passive communication (ie. on the network).

6. Are there other key concepts in the existing framework that require updating to improve clarity? If so, what are they?

Victoria considers that the definitions for key concepts in the current framework including 'data', 'device' and 'tracking device' should be reviewed and future-proofed where possible.

7. How could the framework best account for emerging technologies, such as artificial intelligence and information derived from quantum computing?

Victoria notes the intention to ensure the full range of information and data transmitted electronically is protected from unauthorised access and that the Commonwealth will consider how to best capture emerging technologies such as artificial intelligence and quantum computing. Victoria supports the Commonwealth's further consideration of these issues, noting that the use of these technologies by LEAs requires careful consideration.

For example, consideration must be given to how intelligence agencies and LEAs would access and understand the way a machine/artificial intelligence responds to external users and what underpins the responses communicated (eg. the coding and biases), to ensure an investigation or prosecution is not undermined. Further, it should be recognised that entities owning such information will likely wish to keep that information commercial-in-confidence and may be reluctant to share it with LEAs.

8. What kinds of information should be defined as 'content' information? What kinds of information should be defined as 'non-content' information? Is there a quantity at which non-content information becomes content information and what kinds of information would this apply to?

Victoria supports the legislation making a distinction between 'content' and 'non-content' information. Careful definition of what information falls within these categories is required, given the different thresholds applied to access. We agree that it is also worthwhile considering the application of different authorisation levels to different categories of 'non-content' data (as is the practice in the UK).

Victoria Police suggests 'content' information should include the actual information that is transferred, and that 'non-content' information should include the metadata associated with that transfer of information, such as the network information.

9. Would adopting a definition of 'content' similar to the UK be appropriate, or have any other countries adopted definitions which achieve the desired outcome?

The UK definition of 'content of a communication' may be workable, however, there are interplays with certain types of data which mean that, depending on the context, the data could be content or non-content information. For example, if health data on a device is being used passively in the background (such as when the application is tracking the number of steps a person takes throughout their day) this would be deemed non-content information. However, if a person actively engages this data to, for example, plan a run and monitor their step count on the application during and/or after this run, then this would become content information.

10. Are there benefits to distinguishing between different kinds of non-content information? Are there particular kinds of non-content information that are more or less sensitive than others?

Victoria Police suggests that basic non-content data (such as call charge records (CCR)) could be accessible and have a lower sensitivity than, for example, international mobile subscriber identity (IMSI) or General Packet Radio Service (GPRS) data. The sensitivity of the content is proportional to the degree to which a person's privacy is impacted by accessing the information.

11. Should the distinction between 'live' and 'stored' communications be maintained in the new framework?

Victoria agrees that there is less significance in distinguishing between 'live' and 'stored' information than there may once have been. It is generally accepted that accessing stored communications is no less intrusive than that of intercepting live communications.

Victoria agrees with the statement (at p. 27 of the discussion paper) that the distinction between 'live' and 'stored' communications is 'less significant than it may once have been. Many conversations once held over the phone are now conducted by text messaging or other communications applications. As the way in which people communicate has shifted significantly, this distinction has little current relevance or use'.

This conclusion is borne out by the individual experiences of the PIMs in their former roles at the Australian Criminal Intelligence Commission, the Office of Police Integrity and IBAC, as well as in their current roles. Information of a private and personal nature (including photographs and videos) is now much more likely to be transmitted in communications that are 'stored' (eg. SMS messages, emails, or voicemails).

A solution may be to standardise the definitions and provide one set of eligibility criteria for access. If the potential future state outlined in the consultation paper is realised, then this would appear to be a reasonable solution and would simplify the legislation.

Victoria notes that the PIM has no function in relation to applications by Victorian law enforcement agencies for access to stored communications. If there is to be any harmonisation between interception warrants and access to stored communication, Victoria would support consideration of the PIM having a role in applications to stored communications, noting that this may have resourcing implications which the Victorian Government would also need to consider.

12. Do each of these kinds of information involve the same intrusion into privacy? Or should the impact of each be considered differently?

Currently, Victoria Police treats intercepted material and stored communications similarly in terms of the impacts on privacy. Victoria Police considers this is appropriate as, in its view, the nature of the communication and the expectation of privacy is the same.

13. What type of Australian communications providers should have obligations to protect and retain information, and comply with warrants, authorisations and assistance orders under the new framework?

Victoria notes, in agreement with the paper, that there is currently a lack of clarity around the definition of 'carriage service provider' in existing legislation which will require the Commonwealth to consult closely with affected entities.

Victoria Police suggests the Commonwealth consider whether telecommunications service providers operating under licence in Australia, on-sellers of telecommunication services, internet service providers, social media providers, infrastructure owners, and hardware providers, should all have obligations to protect and retain information and comply with the new regulatory framework. Victoria notes that close consultation by the Commonwealth with industry will be required as this issue is considered. Further, expanding obligations to retain information could have significant privacy impacts.

It is also important to note the increasing role industry plays in working with the state in collecting electronic surveillance information and the need for protection of access, for example, through lawful access portals.

14. What are your thoughts on the above proposed approach? In particular, how do you think the information captured by surveillance and tracking devices could be explained or defined?

Nil further response.

Part 3: How can information be accessed?

15. How could the current warrant framework be simplified to reflect the functional equivalency of many of the existing warrants while ensuring appropriate privacy protections are maintained?

In principle, Victoria supports the proposal to move to a simpler and more outcomes-based warrant framework which places greater emphasis on the privacy impact associated with obtaining access to that information and the offences or threats being investigated, rather than the surveillance/interception method an agency uses to obtain the information. Victoria notes that the current framework results in additional administration and process burden for Victoria Police. Issues of proportionality and authorisation must be included in determining new criteria.

Most people have at least three personal electronic devices on average, with homes estimated to have 37 connected devices in 2022 with the Internet of Things becoming mainstream. From the perspective of Victoria Police, a single 'catch all' warrant or authorisation that permits the interception of certain types of information without limiting the methods used (and that can be added to without the need to return to the issuing authority),

would significantly improve investigation efficiency and enhance community safety outcomes. This approach would ideally permit the capture of relevant communications related to a person (target), object (vehicle), location (address), or event (meeting).

A single warrant/authorisation would also assist agencies to counter measures presently undertaken by criminals to evade telecommunications interception in a timelier manner than previously available and improve the effectiveness of the surveillance regime. There have been many occasions where a service warrant has been obtained and subsequent information has revealed other services and/or devices. This has required a further warrant application process, which is time consuming, resource intensive and has the potential to lose evidence that would have been captured during the time taken to obtain another warrant.

The PIM has raised several concerns about any proposal to permit 'catch-all' warrants to be issued - that is, warrants naming an individual and leaving it to the law enforcement agency to determine the how, when, where and form of electronic surveillance. The PIM's concern in this regard can be explained by reference to section 46A of the TIA Act. Section 46A permits the issue of a 'named person' warrant, ie. a warrant naming a person rather than specifying a particular telecommunications service. A section 46A warrant permits the law enforcement agency to intercept telecommunications from devices the named person is using or likely to use. This is to be contrasted with a section 46 warrant, which is limited to a specific telecommunications service. There are particular dangers to privacy in the use of section 46A warrants, because once a warrant is issued, it is left to the law enforcement agency rather than to the AAT to determine which devices are to be intercepted. An example of the privacy issues to which this can give rise is where a suspect occasionally uses the telephone of his/her partner, parent, sibling, or friend. If the law enforcement agency intercepts such services, the privacy of the partner, parent, sibling, or friend – who may be totally uninvolved in and ignorant of the suspected offending – is infringed.

If 'catch all' warrants were to be permitted, it would be left entirely to the law enforcement agency to determine, in every case, where devices would be installed (eg. in a private home occupied not only by the suspect but by others (including children) who may have no involvement in the suspected activity). The PIM notes that this gives rise to very significant privacy concerns.

The equivalent of a 'named person' warrant can be obtained under the SD Act Vic, permitting the law enforcement agency to install a surveillance device at any location where relevant activity involving the suspect may be occurring. Currently, the use of such warrants is the exception rather than the rule and applications for these warrants are subjected to particular scrutiny. The Supreme Court will very closely and carefully scrutinise any application to install an optical device in a private home. Only in the rarest cases would a warrant be issued permitting the installation of an optical device in a bedroom, for example. The PIM suggests that any proposed 'catch-all' warrant be subject to similar safeguards ensuring their use is necessary and proportionate.

Victoria notes that in terms of protecting privacy, the issuing authority has the option to impose conditions or restrictions on a warrant. There is also the ability to revoke a warrant when the grounds for the warrant no longer exist, the requirement that intercepted material must be destroyed where it is no longer required for a permitted purpose, record keeping

requirements and the independent oversight of the conduct of agencies in carrying out interceptions. In the case of Victoria Police, both the Victorian Inspectorate and the Commonwealth Ombudsman have powers in this regard.

16. What other options could be pursued to simplify the warrant framework for agencies and oversight bodies, while also enabling the framework to withstand rapid technological change?

Victoria Police supports a principles-based, rather than prescriptive approach, to the legislation to ensure it is adaptable enough to keep pace with the rapid advances in technology and the dynamic and changing threat environment. Victoria Police considers that warrant applications and provision should be able to be conducted via electronic means.

Part 4: When will information be accessed?

17. Is it appropriate to harmonise legislative thresholds (as outlined above) for covert access to private communications, content data and surveillance information where existing warrants are functionally equivalent?

Victoria recognises the merit in harmonising inconsistent thresholds, which would simplify and streamline processes for LEAs and improve operational efficiencies. Victoria recognises that LEAs (including Victoria Police) will wish to ensure that any reforms made to achieve consistency should not erode existing police powers or raise authorisation thresholds.

Victoria considers that a harmonised threshold is appropriate if the warrants/authorisation to which it applies involves a substantially similar level of intrusion into privacy, under Victorian law. The starting position should be the existing higher threshold of offences punishable by at least seven years' imprisonment. Any lowering of the threshold, and corresponding rebalancing of the competing interests of facilitating law enforcement and protecting individuals' privacy, should be carefully justified.

In Victoria, the Supreme Court is required to consider the gravity of the suspected offence in considering a warrant application. The PIM notes that while the definition of 'serious offence' in the TIA Act is unwieldy, replacing the definition with the simple requirement that the AAT consider offence seriousness will do little to 'harmonise' thresholds, because the notion of offence seriousness is so broad it is, largely, subjective. Some would contend, for example, that any offence that involves significant distress to a victim should be regarded as a 'serious offence'.

If it is decided to reduce the complexity of the present definition, the PIM's view is that the legislation should nevertheless make clear that warrants are to be issued only in cases involving a high degree of criminality. This should especially be so in applications for group warrants because of the increased risk that such warrants would significantly infringe the privacy of group members who have committed no offence. In other words, the greater the risk of privacy compromise, the higher should be the offence threshold.

Victoria Police notes that the current definition of 'serious offence' in the TIA Act is long (seven pages), complex and outdated as it excludes offences which Victoria Police considers should be included. There are offences Victoria Police routinely investigates that are either not listed in the definition or only become 'serious offences' if they meet the stringent

condition of involving planning and organisation and the use of sophisticated methods and techniques.

There have been many investigations conducted by Victoria Police over the years that have not been able to utilise telecommunications interception as an investigative tool due to the restrictive criteria. Examples include teams of serial burglars netting expensive items or vast quantities of property that could not have their communications intercepted as the techniques used to enter the premises could not be classified as 'sophisticated.' Firearms dealing and extortion are other crimes in which investigators have been unable to utilise telecommunications interception due to the restrictive criteria.

Victoria Police is also concerned that by raising the threshold for surveillance devices and stored communications to a requirement that an offence is punishable by imprisonment for a period, or a maximum period, of at least five years that these investigative techniques will no longer be available for offences such as family violence, weapons or firearm offending which have lower offence penalties. Victoria Police requests consideration is given to these types of offences being exempted from the five-year threshold.

Further, Victoria Police does not support the proposed requirement that the exercise of these powers in respect of the person is likely to substantially assist the agency in the investigation of the offence. The use of the qualifying term 'substantially' raises the current threshold in the TIA Act for both stored communications and telephone interception, which provides that the issuing authority must have regard to 'how much the use of such methods would be likely to assist in connection with the investigation by the agency of the serious contravention/offence or offences'.

Section 14 of the *Surveillance Devices Act 2004* (Cth) (SD Act Cth) utilises the wording 'the use of a surveillance device is necessary in the course of that investigation for the purpose of enabling evidence to be obtained of the commission of the relevant offences or the identity or location of the offenders'.

Victoria Police is concerned that the inclusion of the word "substantially" provides an additional threshold that is not present in the current legislation and would diminish LEA's current capabilities. Any perceived risk of agencies requesting to use all powers available to them regardless of whether those powers are necessary or proportionate can be mitigated by the issuing authority adhering to criteria in the TIA Act and SD Act Vic. In Victoria, there is the additional safeguard of the PIM for telephone intercept and surveillance device applications.

Victoria notes that the Commonwealth is considering a proposed new threshold for ASIO surveillance warrants. Victoria notes that the proposed threshold ('reasonable grounds to suspect that the person is engaged in, or is likely to engage in, activities relevant to security' (p. 40)), is very broad and requires further consideration to avoid unintended consequences.

18. Are there any other changes that should be made to the framework for accessing this type of data?

Victoria Police's position on question 17 (stated above) remains relevant for this question.

The Victorian Office of Public Prosecutions suggests that the Commonwealth Government may wish to consider including post-sentence detention order proceedings for serious sexual

and serious violent offenders and confiscation proceedings in the list of 'crime-related proceedings' where surveillance information can be given in evidence, without first being adduced in criminal proceedings.

19. What are your views on the proposed thresholds in relation to access to information about a person's location or movements?

Victoria agrees in principle that tracking information may have less impact on privacy than other surveillance information particularly where an individual can be tracked/monitored without a warrant during physical surveillance, although in combination with other methods of investigations and surveillance, the impingement on privacy will often be substantial. In Victoria, a surveillance device warrant must be obtained to attach a tracking device to a vehicle.

Victoria supports the current approach under the TIA Act and considers that LEAs should not be required to obtain a warrant to undertake electronic surveillance activities by accessing prospective information for the purpose of monitoring or tracking a service.

From the perspective of Victoria Police, electronic location tracking/monitoring does not impact on an individual's privacy any more than physical surveillance and it also assists law enforcement officers to deploy equipment more quickly and reduce risk during operations, such as the danger of members of the public being injured or killed during high-speed driving, safety of law enforcement officers during deployments and potential for an investigation becoming exposed due to close surveillance. On this basis Victoria Police supports tracking information being regulated separately from other surveillance information.

In the PIM's view, electronic tracking may require more limitation and oversight than physical surveillance. Physical surveillance is naturally limited by the police resources it requires. It is easier and cheaper to attach a tracking device to a vehicle than for police officers to physically follow it. In the PIM's view, the relative ease of electronic tracking means that a warrant system limiting the use of tracking to where it is necessary and proportionate, should be considered.

Victoria Police also notes that currently, the TIA Act only allows historic information (eg. call records) to be applied for in relation to any missing persons. There is no ability to utilise prospective information such as a 'Location Based Search' (LBS)/triangulation of mobile phone towers to ascertain the location of a mobile phone unless a crime is suspected such as a kidnapping, homicide. Victoria Police considers that the ability to access such data assists with the search for vulnerable missing persons in a timely manner. Victoria notes that this proposal would need to be subject to close consultation with affected groups and stakeholders, and that any new powers should only be used where necessary and proportionate.

20. What are your views on the proposed framework requiring warrants and authorisations to be targeted at a person in the first instance (with exceptions for objects and premises where required)?

Victoria Police supports this approach on the basis that the current system of named person warrants is appropriate and remains the best tool to obtain evidence and provide operational

agility during investigations, however, would strongly support retaining the ability to apply for object or premises-based warrants in applicable circumstances.

As highlighted in the discussion paper on page 47, there are occasions when a suspect's identity is unknown (for example, an unidentified person receives a controlled delivery of drugs) or a third party is targeted to obtain evidence to support a warrant for the intended target (for example, to access communications between a third party and a member of an organised crime syndicate). Similarly, an unknown person may be utilising certain objects or premises to carry out the offending (for example, a drug manufacturer whose identity is not known at the time but is utilising certain equipment or a premises to carry out the activity). In these situations, it remains important to be able to obtain warrants.

The deployment of equipment under these warrants is intelligence-led and specifically focussed. In the experience of Victoria Police there is simply no option of employing a 'scatter-gun' approach in these circumstances as due to limited staff and equipment resources, they only target the premises or objects which will yield the most evidence or intelligence. In these circumstances, Victoria Police requires the ability to target groups and locations of interest, rather than base a warrant around an identified person of interest.

21. Is the proposed additional warrant threshold for third parties appropriate?

Victoria notes that the thresholds for third party provisions in the current framework between LEAs and ASIO are inconsistent and that the Commonwealth Government is considering standardising these thresholds and ensuring they are sufficiently confined to balance the intrusiveness of these provisions. It is noted that the new framework may require agencies to satisfy an additional threshold; for example, agencies may need to satisfy the issuing authority that, in addition to the test for an ordinary warrant, obtaining information directly under a warrant would be impractical or ineffective.

Victoria considers that the starting position should be the existing threshold of 'exhausted all other practicable methods'. Any lowering of that threshold should be justified by reference to evidence of the impact of the existing threshold on criminal investigations.

Victoria Police is supportive of the proposed additional warrant threshold as a starting point (again, with any lowering of that threshold justified by reference to evidence of the impact of the existing threshold on criminal investigations). Victoria Police notes that while rare, the ability to be able to place third parties under surveillance or location tracking could be justified in certain exceptional circumstances, particularly in the pre-crime context such as in preventing terrorist attacks.

22. Is the proposed additional threshold for group warrants appropriate?

Victoria notes that under the current framework, there are limited instances in which LEAs can obtain warrants targeting groups.

Victoria agrees generally that higher thresholds are appropriate for group warrants given to ensure proportionality given their potentially more intrusive nature.

Victoria Police supports the proposal that the Commonwealth will consider introducing dedicated group warrant regimes for both LEAs and ASIO that will apply across all warrant types. Victoria Police considers that if the group can be treated as an entity or their platform

treated as an event that can be the subject of a warrant to capture all relevant communications, this would make the application process more efficient.

23. What are your views on the above proposed approach? And are there any other matters that should be considered by an issuing authority when considering necessity and proportionality?

Nil further response.

24. Should magistrates, judges and/or AAT members continue to issue warrants for law enforcement agencies seeking access to this information?

Victoria supports the retention of magistrate, judge and/or AAT oversight.

Victoria notes that not all members and senior members of the AAT are lawyers. The issue of a warrant significantly interferes with an individual's human rights, in particular, the right to freedom from arbitrary, unlawful, and unreasonable interference with privacy. Victoria suggests that only members of the AAT that are lawyers should be eligible to be nominated to issue warrants.

25. What are your thoughts on the proposed principles-based, tiered approach to use and disclosure?

Victoria supports in-principle simplifying the current provisions, including by replacing them with principles-based rules. The new framework should restrict the use and disclosure of information and could include a principle-based approach. Flexibility and discretion are required in some circumstances to support law enforcement objectives, which are not always facilitated by an inflexible prescriptive rules-based approach.

There are potential benefits of a principle-based disclosure, though such an approach may give rise to privacy and other rights-concerns (by permitting disclosure to a wider range of agencies) and necessitate addition safeguards. The suggested primary and secondary purposes (p. 57) outlined the discussion paper are potentially very broad. Victoria requests more detail on the proposed protections that would accompany such an approach.

Further, Victorian notes that if telecommunications inception currently identifies that a child is at risk of harm from its parents, this information cannot be communicated to child protection agencies. The SD Act Vic enables disclosure of protected information in circumstances where there are reasonable grounds to believe it is necessary to help prevent or reduce the risk of serious violence to a person or substantial damage to property. Victoria requests that the Commonwealth consider adopting a similar provision in the new framework.

26. When should agencies be required to destroy information obtained under a warrant?

Victoria considers it is reasonable to expect that information should be destroyed when it is no longer required for a specified purpose. However, Victoria notes that the 'specified purpose' is often unclear at the time, and that such information can be of benefit for LEAs in future investigations.

For example, information obtained by electronic surveillance can be crucial for intelligence gathering in terms of revealing ideology, associations in Victoria and other states and

territories, criminal/security related capabilities, use of code/language, likes/dislikes, motivations in criminal and security related exploits, movements, and patterns of life.

Accordingly, it would be of assistance to LEA's investigative functions for there to be some provision for the retention of electronic surveillance information for intelligence purposes for a specified period following the capture of that information, which would need to be subject to appropriate privacy legislation.

As highlighted in the discussion paper, there is an inconsistency in the current destruction requirements between telephone intercept warrants and stored communications warrants whereby the requirement for stored communications is that both the original and copies must be destroyed. While it is reasonable to expect that original recordings should be destroyed when there is no longer a permitted purpose to retain, permitting LEAs to retain copies of the recordings would enable them to utilise this information if required for investigations in the future (for example, where the OPP applies for a retrial after an acquittal (double jeopardy) under the *Criminal Procedure Act 2009* which can potentially occur many years later).

Further, Victoria notes that surveillance device legislation currently differs from telecommunications interception legislation in that information derived from surveillance device warrants must be destroyed after five years unless it is certified that a prosecution is likely to commence. Victoria Police, in particular, does not support the uniform adoption of this approach. Victoria Police has records dating back many years on 'cold' cases for serious offences such as murder, armed robbery and other offences involving loss of life or serious personal injury. These cases are revisited and reinvestigated, often well after a five-year period. Any future prosecution will be jeopardised if information from the interception was destroyed after five years because a prosecution was not likely to commence at that point in time. Victoria Police believes that copies of information should also be kept on archived briefs of evidence to enable any future use in cases where an accused is granted a retrial sometimes many years later.

Victoria agrees that if agencies were able to retain surveillance information, it would be necessary to consider strengthening other safeguards to maintain the overall proportionality of the scheme. The breadth of 'specified purposes' for which agencies may retain surveillance information will bear on other aspects of the electronic surveillance framework, such as application thresholds, oversight mechanisms and information sharing rules.

27. What are your thoughts on the proposed approach to emergency authorisations?

Victoria supports a consistent approach to emergency authorisations. Oral applications by agencies are infrequent, and the relevant provisions are being used appropriately.

Victoria considers that the proposal to allow an agency head to authorise surveillance in time-sensitive cases requires additional information to justify the need for changes. Victoria notes the courts, the AAT and duty PIM are available 24/7 for urgent applications. Such applications can be made orally, and technology exists for the warrants to be sent electronically to the relevant decision maker to enable the addition of an electronic signature. Any proposed change would need to be balanced to ensure these arrangements would be used by exception only.

Victorian LEAs have experienced significant delays in applying for an interception warrant in urgent situations. Section 40(2) of the TIA Act enables an application for a warrant to be made by telephone in urgent circumstances. The current interception warrant application process creates significant time delays which can be detrimental in urgent situations. Due to the content required in such a warrant, in terms of satisfying the various oversight bodies, it can take up to five hours to prepare the relevant documentation and have it authorised by the relevant parties. From the perspective of Victoria Police, it would be ideal for the legislation to allow the interception of telecommunications without a warrant in urgent situations.

Victoria invites the Commonwealth to continue to consider options to improve the oral application process. Victoria considers it appropriate that:

- after obtaining a time-sensitive authorisation in an order application, agencies by required to make a written application; and
- the issuing authority have power to invalidate the time-sensitive authorisation and make directions as to the use of any information obtained under the invalidated authorisation.

Victoria invites the Commonwealth to consider Part 4, Division 3 of the SD Act Vic which could be used as a model for any proposed legislative reforms. The SD Act Vic includes safeguards such as a requirement to apply to a Supreme Court judge for approval of the exercise of powers under the emergency authorisation within two business days of the giving of such authorisation.

The PIM considers that if a change is made to allow emergency warrants to be issued on internal agency authorisation alone, the incidence of such issue may become more frequent, although the proposal to limit internal authorisations to the circumstances listed on page 60 of the discussion paper may ameliorate this.

Part 5: Safeguards and oversight

28. Are there any additional safeguards that should be considered in the new framework?

Victoria emphasises that state legislation requires LEAs to notify the PIM of a relevant application which includes an application for a surveillance device warrant and a telecommunications interception warrant. The PIM attends and is involved in hearings to 'test the content and sufficiency of the information relied on and the circumstances of the application'.[1]

Other safeguards include:

- the ability for the issuing authority to impose conditions or restrictions;
- the requirement to revoke a warrant when the grounds for the warrant no longer exist;
- the requirement for intercepted material to be destroyed where it is no longer required for a permitted purpose; and

[1] Section 14 *Public Interest Monitor Act 2011.*

- extensive record keeping requirements.

Were the Commonwealth minded to implement 'technology neutral' legislation, appropriate safeguards should be included in the legislation, such as provision requiring regular review and sunset clauses. Victoria reiterates the benefits of these safeguards. Victoria also notes that the Australian Law Reform Commission's report on *Serious Invasions of Privacy in the Digital Era* discussed the need for careful framing of legislative provisions if a tech-neutral approach was to be adopted to mitigate risks with this approach (including those raised by the Australian Privacy Foundation).

Victoria notes that the protection of contact tracing information and data collected via QR code check-ins for public health purposes of COVID-19 contact tracking is of particular interest and public concern. It may be necessary to consider how this specific type of information may be affected by any reforms, to ensure that the approach is consistent with measures by states and territories legislatures who seek to protect this information from broader use.

29. Is there a need for statutory protections for legally privileged information (and possibly other sensitive information, such as health information)?

Victoria acknowledges the importance of legal professional privilege and journalistic privilege. The Commonwealth may wish to strengthen these protections through codification. Sensitive information from industry, including anything commercial-in-confidence, will need to be considered and protected through consultation. Victoria encourages consultation with individual sectors to shape these protections.

30. What are the expectations of the public and industry in relation to oversight of these powers, and how can a new oversight framework be designed to meet those expectations?

Victoria notes that careful consideration must be given to what is meant by 'robust oversight'. Safeguards and oversight can take several forms, including:

- statutory criteria, including thresholds for the issue of warrants;
- scrutiny of applications by the relevant issuing authority;
- active (real time) monitoring and advocacy, such as is provided by a PIM;
- ex post facto reporting to the federal Attorney General (in the case of warrants under the TIA Act) and to the issuing court (under the SD Act Vic);
- storage and dissemination controls;
- record keeping obligations; and
- ex post facto compliance checking, such as is undertaken by Victorian Inspectorate or the Commonwealth Ombudsman.

In the PIM's view, the only meaningful controls on the appropriateness and proportionality of warrants are statutory criteria, are the first three points above.

Victoria notes that there is a PIM in Queensland (in addition to that in Victoria) and that there is a public official in NSW who has an active monitoring role that does not include advocacy. There are no PIMs in any other states or territories or at the Commonwealth level.

A PIM function – as a 'contradictor' – adds significantly to the integrity of the warrant application process. Indeed, the mere existence of a PIM, such as in Victoria, enhances the quality and proportionality of warrant applications. Law enforcement agencies know their applications will be scrutinised not only by the issuing authority but by a monitor empowered to ask questions and, if appropriate, advocate against the issue of the warrant.

Further, Victoria is of the view that in general a necessary and proportionate test should apply to the issuing of warrants under the new framework.

31. What, if any, changes are required to the scope, role and powers of the Commonwealth Ombudsman to ensure effective oversight of law enforcement agencies' use of powers in the new framework?

Victoria considers it is important that the State of Victoria maintains oversight of Victorian Government agencies. In short, it is vital that the oversight role of state agencies is not diminished.

Victoria acknowledges that under a reformed electronic surveillance framework, where provisions are identical across the Commonwealth and state jurisdictions, it would be most efficient for the Commonwealth Ombudsman to inspect the records of state police forces. However, to remove inspection functions from state oversight bodies would represent an unfortunate diminishment of their powers. Victoria suggests further consultation be undertaken as to how oversight can be best deconflicted.

As a state-based agency, oversight of Victoria Police's use of electronic surveillance powers are divided between the Commonwealth Ombudsman and the Victorian Inspectorate. The Commonwealth Ombudsman has oversight of telecommunications interception powers (telecommunications data, stored communications and industry assistance under the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth) (TOLA)), and surveillance powers under the SD Act Cth. The Victorian Inspectorate has oversight of telecommunications interception powers under the *Telecommunications (Interception) (State Provisions) Act 1988* (Vic) (the TI Act Vic), and of surveillance powers under the SD Act Vic. Law enforcement agencies obtaining Victorian warrants are also required to report to the issuing Court on the use and effectiveness of such warrants.

Both conduct regular and thorough inspections and report on the results of these inspections. Victoria Police has an in depth understanding of the requirements of each oversight body and established processes in line with recommendations and agreements with both, and believes that, as a result, compliance standards are high. In the opinion of Victoria Police, it is doubtful that moving to a single oversight body will promote more efficient oversight and minimise any gaps. In the short term, it will create issues for Victoria Police as the Commonwealth Ombudsman may have differing views and requirements leading to process changes and investigator confusion.

In relation to oversight, the PIM highlights two points:

- Currently, there appear to be inconsistencies between the PIM's role under the TIA Act and the TI Act Vic:
  - both Acts enable the PIM to make submissions regarding the matters referred to in ss 46(2)(a) to (f) and 46A(2)(a) to (f) of the TIA Act. Section 44A of the TIA Act also permits the PIM to make submissions in relation to ss 46(5)(a) to (f) and 46A(2B)(a) to (f) of that Act, but there is no corresponding reference in the TI Act Vic.
  - the TI Act Vic, but not the TIA Act, permits the PIM to make submissions about the appropriateness of issuing the warrant. It is submitted that either under the existing regime or in any harmonised test, the PIM should be permitted to make submissions as to the appropriateness of the warrant application as a whole, rather than the particular considerations specified in paragraphs (a) to (f) of the sections listed above.

  If two electronic surveillance methods are considered to be similarly intrusive, Victoria supports the PIM's involvement being consistent for both methods.
- There is a disconnect between agency roles and the secrecy provisions in the TIA Act that should be reviewed. Section 17(2) of the *Public Interest Monitor Act 2011* (Vic) provides an exception to the duty of confidentiality, where the disclosure is by a PIM or a person assisting the PIM in the performance of their function. However, this exception does not override section 63 of the TIA Act. This can result in a situation where a PIM cannot discuss with another PIM, for the purposes of performing their function, a TI application that contains within it lawfully intercepted information. This issue usually arises where an agency seeks a further warrant in relation to a service and includes lawfully intercepted information from the previous or current interception of that service to justify a further issue. It is submitted such disclosure between PIMs should be a permitted under the TIA Act.

32. How could the new framework streamline the existing record-keeping and reporting obligations to ensure effective and meaningful oversight?

Victoria notes that current record keeping obligations on LEAs are extensive. Victoria Police ensures that appropriate records are kept and necessary reporting requirements fulfilled to comply with current legislation, which is necessary for oversight purposes and good governance. However, a more streamlined and flexible approach to the preparation and maintenance of records that both reduces the administrative burden and enhances the ability of oversight on LEAs would be welcomed.

It may be that a tailored approach to recordkeeping requirements would take account of the different systems used by agencies and reduce the obligation on an oversight body to inspect records that are of limited use to it in performing its oversight functions. However, Victoria consider it is important that some records are mandatory and specified in the framework, with potentially other sets of records able to be modified or discretionary as determined through a consultation process.

33. Are there any additional reporting or record-keeping requirements should agencies have to improve transparency, accountability and oversight?

Victoria notes that if a 'hybrid' or 'single' warrant regime is introduced, it is important that agencies be obliged to keep records that clearly identify which powers have been exercised under the warrant.

The PIM notes that knowing what occurred in the execution phase of a warrant and to whom the product of the warrant has been disseminated can provide valuable general guidance as to whether agencies are using warrants for the purpose originally stated. To better inform the PIM's work in relation to warrants issued to Victorian law enforcement authorities under the TIA Act, it would be of advantage to the PIMs to be provided with copies of the effectiveness reports given to the Commonwealth Attorney-General under sections 94 and 94B of that Act.

Part 6: Working together: Industry and Government

34. How workable is the current framework for providers, including the ability to comply with Government requests?

Nil response.

35. How could the new framework reduce the burden on industry while also ensuring agencies are able to effectively execute warrants to obtain electronic surveillance information?

The implementation of the TOLA and the prospective Clarifying Lawful Oversea Use of Data (CLOUD) Act Agreement (the CLOUD Act Agreement) between Australia and the United States of America will support any amendments around the definition of communication and will enable industry to provide data with more legal comfort.

There is data held by industry that would be useful for LEAs as part of a wider investigation with respect to communications. The TOLA and the CLOUD Act Agreement should assist in accessing this material, but the future legislative framework needs to address metadata held within networks and devices and carefully consider relevant privacy impacts.

Currently, Victoria Police spends a significant amount of money on fees charged by telecommunication providers, for the provision of information. These fees are not currently regulated and the cost for provision of information varies significantly between service providers. Due to budgetary constraints, Victoria Police limits these requests for information. Under the current legislative scheme, fees can only be set on a cost recovery basis. However, Victoria Police considers the current charges are excessive and exceed legitimate cost recovery. The excessive fees are also evidenced by the fact these records are already maintained business records and the effort to provide the information is minimal. There would be considerable benefit in scheduling appropriate fees for the provision of information from telecommunication providers. Victoria recognises that this approach would require close consultation with industry.

36. How could the new framework be designed to ensure that agencies and industry are able to work together in a more streamlined way?

LEAs would benefit from the inclusion of prescribed timeframes for the provision of information from agencies/providers.

Consideration could be given to whether data retention periods and access methods amongst service providers should be standardised.

Part 7: Interaction with existing and recent legislation and reviews

37. Do you have views on how the framework could best implement the recommendations of these reviews? In particular:

a) What data generated by 'Internet of Things' and other devices should or should not be retained by providers?

b) Are there additional records that agencies should be required to keep or matters that agencies should be required to report on in relation to data retention and to warrants obtained in relation to journalists or media organisations? How can any new reporting requirements be balanced against the need to ensure sensitive law enforcement or security investigations and capabilities are not compromised or revealed?

c) Is it appropriate that the Public Interest Advocate framework is expanded only in relation to journalists and media organisations?

d) What would be the impact on reducing the number of officers who may be designated as 'authorised officers' for the purposes of authorising the disclosure of telecommunications data?

In response to question 37(d), Victoria Police notes there is a high threshold (inspector or above) for its authorised officers and suggests this an appropriate rank to hold the delegation. Every request for telecommunications data must be approved by an authorised officer. Due to the very large number of telecommunications data requests undertaken by Victoria Police each year, decreasing access to authorised officers would cause several issues. Firstly, it would place the burden on fewer officers, perhaps at different work locations that do not have an appreciation/understanding of the investigation and the tools necessary to solve crime. It would also lead to delays in accessing the required information. Further, soon, all authorised officers in Victoria Police will be required to undergo further training to ensure they have a complete understanding of their privacy considerations before authorising a request.