

Submissions are public documents

* required fields

Unless you state otherwise submissions are treated as public documents. However, you can ask that your submission be made anonymous or confidential. Please choose one of the following options: *



My submission can be quoted or sourced in publications, kept at the commission for people to look at and uploaded to the commission website (public).



My submission can be quoted or sourced in publications, kept at the commission for people to look at and uploaded to the commission website but I do not want my name to be disclosed (anonymous).



My submission can be looked at by researchers but I do not want it to be quoted or sourced in publications, made available to the public or uploaded to the website (confidential).

Your Contact Details

Surname: Christie

Given Names: Louise Mary

Company: ART Security Pty Ltd

Position: Director

Street: PO Box 494

Suburb: Hawthorn

State: Victoria

Postcode: 3122

Email:

Telephone:

Other Positions:-

Organisation: Victorian Security Advisory Council

Positions: Electronic Security Committee – Vice Chairman

Alarm Response Subcommittee – Vice Chairman

Training Committee – Member

Organisation: ASIAL – Australian Security Industry Association Limited

Position: Victorian Working Group - Member

General Questions

Do surveillance practices in Victorian public places concern you?

As surveillance is becoming more common place and the equipment is becoming more 'intrusive' it is essential that some guidelines and regulations are established both for the training of practitioners and the type/quality of hardware and software that can (and should) be used, for conducting this activity.

These regulations must establish guidelines for use of surveillance practices that encompass such issues of legitimacy of purpose and necessary extent of surveillance. Such guidelines would be of great assistance to all practitioners of surveillance whether in public places or non public places as the current status quo is quite vague on such issues. However, guidelines will only be relevant if accompanied by a requirement to comply with that registration or licensing and have consequences for non compliance.

Public places must remain accessible to the majority of the public particularly those places which do not require an 'invitation' to access. No one should be prevented from, or feel intimidated to be, in a public place or have any fear that being in a public place under surveillance may have unwanted consequences. If this were to occur it is agreed that the nature of public places would alter which would have negative consequences for our society. Feeling safe and being comfortable to be in public places which are surveyed is particularly relevant when information is being recorded and stored. Thus the need for both very specific and publically displayed signage showing who is doing the surveillance, for what purpose, the extent of the surveillance, what is being recorded/stored and what is happening to the information.

Fears of being surveyed in public places may range from unwanted recognition to issues which could verge on harassment. With the advent of the internet information can end up permanently in the public domain which the person surveyed has no information about or control over. I do not believe that by being in a public place or by not having specific information (such as name, address, etc.) regarding the people occupying public places means that the information recorded is public information and can be treated as such.

Also there is a right for individuals to have some privacy where they would normally expect same, change rooms, toilets, etc., even within public places that are surveyed and the surveillance is transparent.

Covert surveillance must be confined for use in very specific circumstances by specifically allowed groups. This may be for purposes of preventing major threats to public safety (eg terrorism/crime prevention) and the groups using such practices must be confined to properly qualified and/or licensed groups. In certain situations the very fact that the group is a part of a major public service (for example, police/army intelligence) may automatically qualify them to conduct covert surveillance.

All surveillance practices should be forced to use video analytics so that specific disturbances/identifications can be made without the need to generally and continuously survey public places and the individuals contained therein by a human operator. After all, it is a well known fact backed by much research, that the efficiency of people conducting surveillance by the 'looking at screens' continuously practice is almost negligible. There is also the issue of playing 'where's Wally' with operators being known to jump to conclusions and make assumptions which can have detrimental consequences for the individuals being surveyed or cause the unnecessary use of public service facilities to attend to apparent, but not confirmed, breaches of public safety.

It is also widely accepted that the quality of surveillance equipment and software in general leaves a lot to be desired which can add to the 'where's Wally' dilemma. Even the operators themselves are not confident with this new technology and distrust it.

With regard to surveying places for the purposes of alarm monitoring (which may or may not be relevant to public place surveillance) alerts for attendance should only be made when used in combination with an alert from a properly installed and reliable electronic security system.

As a final comment the placement and frequency of placement of surveillance devices should not contribute to altering the nature of public places particularly from an aesthetic point of view. Any regulations and guidelines should take this into account. Currently the situation in London is such that cameras appear on every street corner to the multiple often of four. That has certainly altered the nature of many public places.

Do some practices cause you greater concern than others, for example, covert CCTV?

Covert surveillance or any surveillance that is not accompanied by video analytics or an electronic security system – whichever is appropriate for the purpose (see above).

What changes could be made to better regulate surveillance practices?

Developing a regulatory framework is complex but essential. There are many factors to be considered in making this recommendation such as registration, licensing, compliance, ability to conduct compliance checks, consequences for non compliance, extent of regulation, format of regulation, which body is most appropriate to be the regulator, cost of regulation, who bears the cost of regulation, harmonization of regulation on a national scale, etc. It is appreciated that the Commission has tried to encompass most of these factors in this Consultation Paper 7 except for the very great costs which will be involved both in establishment and ongoing application of the regulatory process. One of these essential costs is the resourcing of the regulator to be able to efficiently and effectively carry out the required tasks particularly in regard to processing of applications, complaints and compliance.

If the experience of the security industry with its own regulatory system is anything to go by what usually ends up happening is the regulator is under resourced with applications taking a long time and the compliance process being non existent. This penalizes then only the ethical operators which comply with the regulations and does nothing to improve the non ethical operators who do not comply anyway. Regulation only creates an unnecessary overhead if not accompanied by an effective compliance mechanism.

It is recognized, however, that a punitive approach should only be applied when major breaches of compliance occur. Under these circumstances it would then be assumed that the breach falls within the gambit of one of the existing State or Federal Laws and would be handled by an appropriate body such as the police. This would then involved punitive consequences which would not be imposed by a regulator.

It is also essential in establishing any regulatory system that it be co-regulatory with the stakeholders who supply the service. This is probably best achieved through the Associations which represent these industry stakeholders.

A review of the Victorian Surveillance Laws is essential and perhaps a review of the National Privacy Laws for, when lack of compliance verges into major offences against public privacy, there should be

significant consequences for the perpetrator which should be dealt with under our existing judicial system. Currently it appears there are significant gaps in the three main Acts that regulate surveillance in public places in Victoria. This is clearly displayed in such issues as the definition of consent and participant monitoring.

The general public often may be unaware of the consequences of consenting to or participating in surveillance either directly or by implication. These consequences should be clearly available and a public awareness campaign needs to be launched to educate the public not only to these consequences but also to their right to and avenues of complaint.

Reform option questions

Principles to guide public place surveillance

1. Do you agree with the draft principles proposed by the commission to guide policy making about public place surveillance?

For overt surveillance yes, however, there does not appear to be any reference to covert surveillance in these draft principles. Also the 'notice' provisions are not extensive enough.

2. Should the once-off or intermittent use of surveillance practices by individuals be regulated?

This would certainly be an ideal situation. However, it would seem very difficult to establish and impose. It would certainly require all devices capable of surveillance to be categorized so that it is clearly understood by the public what is covered by regulation and what is not. Certainly the once-off use of any device would be impossible to regulate and the extent of 'intermittent' use needs to be more clearly defined so that it is clear what extent of surveillance falls under the regulations or, more importantly, should fall under the regulations.

It is obvious at present that certain acceptable practices are being exploited and we must guard against over regulation. Greater clarification of current and proposed laws that cover privacy and surveillance is certainly required to avoid this exploitation. This is certainly where the concept of 'lawful excuse' of 'for unlawful purpose' must apply. It would seem ridiculous that a body such as the police would have to gain warrants to conduct surveillance which is essential to protect public safety.

Specific functions of the regulator

3. i. Do you agree with the proposal that an independent regulator should have responsibility for monitoring the use of public place surveillance in Victoria?

The options for reform contained in 6.60 are commendable in principle and should apply both to overt and covert practices of surveillance.

To establish a proper and effective regulatory system it is essential to appoint an appropriate independent regulator not only to monitor public place surveillance but one that has the resources and power to implement a compliance program. The security industry has vast experience of an extensive regulatory system which has little, and certainly no, effective compliance strategy. The Licensing Services Division of Victoria Police does not have the resources, both physical and financial, to conduct such a compliance program even though it has the power to do so. Consequently the entire regulatory

process is ineffective in raising professional standards amongst those practitioners who require regulation. It has literally only served to produce revenue for the State Government and raise overheads for those ethical practitioners who were already providing a professional service.

One of the most powerful compliance tools is public awareness and the competitive edge gained by company's who provide a service which is excellent – competition.

ii. Who should perform this role?

This is a difficult question. The proposal for the Victorian Privacy Commissioner to undertake this role seems feasible on the surface as long as the following conditions are met:

- i. its knowledge of surveillance equipment, techniques and practices are current and kept current
- ii. it is properly resourced, physically and financially, so that it can effectively and efficiently carry out its regulatory duties particularly with regard to processing applications for registration/licensing, conducting an effective compliance strategy and dealing with complaint
- iii. industry stakeholders, most likely though industry Associations, are involved with the VPC in both the establishment, revision and conducting of the regulatory process – co-regulation
- iv. the extent of its powers are extended to allow for imposition of compliance penalties
- v. major breaches of public privacy/surveillance Laws are handled by the properly authorized body and punitive penalties apply
- vi. this regulatory body is responsible for a comprehensive industry and public awareness campaign

However, as surveillance is always done from a Control Room or Monitoring Centre there are already many regulations in place which provides for the licensing of operators in both these facilities. Victoria Police is currently the regulator of the security industry and it has put in place competency based training requirements for license qualification.

There is also a series of Australian Standards which cover all aspects of the operation of these facilities – AS2201.1 - AS2201.5 which all such facilities must comply with to get a 'grading' in Victoria to be able to operate such a business within the security industry. These Australian Standards are not mandatory but are required for licensing purposes. They are very stringent and extensive.

It is my understanding that an AS also exists which covers surveillance equipment and delivery of service. However, I am unaware that there is particularly extensive training modules or certificates specifically dealing with surveillance. There are some units under CPP07 which are incorporated into Control Room and Monitoring Centre licensing requirements both at Cert II and Cert III level. Perhaps these need expanding or new units specific to this activity added.

In general, training within the security industry is hard to define currently. Anna Henderson, Executive Director, Business Skills Victoria and myself have been working on establishing career pathways for the security industry for some years. Initially, through a series of Reframing the Future grants and now with an Industry Pathfinder grant. We anticipate when we have established what it there and how it can be accessed it will be put up on the BSV website and linked to NTIS. The next step is to campaign for more relevant training and perhaps this CCTV training needs to be incorporated.

As an operator of a monitoring centre we are always aware of the issues of liability in playing the

'Where's Wally' game. It is of great concern. Even though this exercise is about public place surveillance it would be good if it could lead on to a more extensive review of surveillance practices and training in Victoria.

In summary, it would seem an unnecessary overkill to put another regulatory burden in place which will just bring another series of regulatory overheads for, perhaps, very little gain. Why not look to using what is established and improving on same. Our findings through the projects Anna and I have conducted shows that all stakeholders in the security industry recommend at least a co-regulatory approach to any type of regulation. We have seen the training aspects to often hijacked by the RTO's for monetary rather than professional gain.

Perhaps the answer is for the VPC to work with the industry stakeholders (through its Associations) to establish the guidelines for a comprehensive and usable registration and/or licensing scheme which can be incorporated into the current requirements of the LSD of Victoria Police and Australian Standards and resource the LSD properly to fulfill its obligations particularly with regard to compliance.

It should be noted that currently in-house control rooms and monitoring centres are not covered by the Private Security Act 2004 and Regulations 2005. Therefore in-house facilities such as these do not require grading of to have the operators licensed. It has been recommended by VSIAC that these in-house facilities be captured in the review of the Act currently underway.

Specific functions of the regulator

4. Should the regulator be given the functions proposed by the commission?

These functions should be extended to include a registration and/or licensing system that is not onerous as well as the powers for conducting the functions listed in 3ii above. As we have experienced in the Security Industry not regulatory system has any impact (it is a toothless tiger) unless there are specific consequences for non compliance.

5. Are there any other functions that should be given to the regulator?

See 3 and 4 above.

6. Would a registration scheme assist the regulator to acquire information about surveillance use?

Yes it would be relevant for a regulator to know where surveillance is being conducted in public places by whom, for what purpose, to what extent and how any recorded information is to be used. It would also be beneficial for the public to access such information readily. An online register would be easy to establish. In the security industry all registered and licensed providers are listed on the Victoria Police website.

Is such a scheme practical?

Seems to work within the security industry so why not. Also being applied in UK. The appointed regulator just needs the necessary resources to make it work properly particularly in relation to processing of applications and compliance. Currently Victoria Police, LSD, is under resourced to act as the regulator to the security industry and the industry is only too well aware that the bulk of the revenue

raised through licensing does not go back into supporting the process. Hard to think it is then a public safety exercise as the DOJ claims.

Should some users be exempt from registration requirements?

No users of overt surveillance should be exempt. However, there may be some use of covert surveillance by properly authorized bodies that may need to be exempt. These may, for example, include Victoria Police for purposes of solving major crimes or Army Intelligence for tracking terrorist activities.

There may be a situation where these organizations could be registered in a private and secure register known only to the regulator and not available for public scrutiny and there may be circumstances under which they are required to be kept secret even from the regulator.

7. What (if any) investigatory powers should be given to the regulator?

Regulators should be given extensive investigatory powers in line with those of the Federal Privacy Commissioner or Victoria Police. The recommendations of the Commission would strengthen any regulator's ability to ensure the regulations are complied with. The right to prosecute and apply punitive punishment is another issue and should be reserved for law enforcement agencies.

8. Should the regulator have an own- motion investigatory power in order to identify systemic problems with surveillance in public places?

Absolutely – from my experience of the security industry complaints are rare particularly those which are sufficiently backed up by qualified evidence on which the regulator can act.

9. Should the regulator have the power to develop advisory guidelines which explain the law concerning surveillance in public places?

Essential – public awareness including industry stakeholders is essential. This type of material should be widely disseminated and education of both the affected public and the service providers is very important. Consistency of interpretation is very necessary. All this type of material should be developed on a co-operative bases with industry stakeholders.

Voluntary best practice standards

10. Would voluntary best-practice standards developed or approved by the regulator be useful?

Voluntary best-practice standards would be useful but without there being consequences for non compliance they could gather dust on many a shelf. These should be developed with input from industry stakeholders.

11. Is linking voluntary best-practice standards to government procurement criteria a good strategy for encouraging responsible use of surveillance practices? Are there other strategies for encouraging compliance with the voluntary standards?

This seems a good strategy for encouraging compliance. However, there is a large range of surveillance conducted that may not be in the area of government procurement criteria particularly those public areas which, according to the Commission's definition, are by invitation.

Mandatory codes of practice

12. Should there be mandatory codes, if so, what conduct should they regulate?

Mandatory codes of practice combined with a properly functioning compliance scheme are one of the two only ways to ensure a code, if required, is complied with. Voluntary best-practice standards are useful guidelines but are rarely adhered to. The other useful tool to ensure a required standard/code is complied with is public awareness which creates its own sense of competition relying on ethical values as the currency. However, it must be emphasized that any introduced mandatory codes would need to be very general and must be developed with significant input from industry stakeholders. They should regulate ongoing overt and covert surveillance and not incidental surveillance by private individuals. Developing these mandatory codes will be a very time consuming and taxing exercise but one that should be achieved. After all it has been achieved in other places in the world where surveillance is more wide spread and populations greater. One of the areas which may come into question when developing such codes for surveillance is the outside of private properties where they border onto public places. When private properties have surveillance facilities that watch the perimeter walls and beyond into public places will the mandatory codes apply?

13. If mandatory codes are introduced, should the regulator have the power to approve industry codes that operate in their place?

Definitely – throughout my responses you will see words used like co-regulation, input from industry stakeholders – this would be an example of mutual recognition that is essential.

14. Should the regulator be empowered to investigate complaints made about potential breaches of a mandatory code? How broad should any such powers be?

As previously stated mandatory codes are irrelevant unless the regulator has the power to impose sanctions for non compliance. Following on from this it would not be possible for the regulator to have the ability to impose sanctions for breaches of a mandatory code unless it has significant powers of investigation. Further, it is considered that the regulatory should not only have the power to respond to complaints but should have own-motion investigatory powers.

Another problem with complaints based investigations is the obvious exclusion of the ability to investigate covert surveillance activities.

15. What kind of sanctions should be imposed for breaches of a mandatory code?

The kinds of sanctions should be directly related to the severity of the breach and whether it is a first breach or subsequent breach.

Warnings which give the opportunity for proving better conduct and/or re-training of service providers plus the staff who deliver the service, should always be the first option. For minor breaches civil

penalties accompanied by such penalties as license suspension would be appropriate. Major breaches of the mandatory code which equate to breaking the law should be dealt specifically with by a law enforcement officer and should result in punitive and/or criminal penalties. This should not be the realm of a regulator.

It should be noted that the industry Associations in the New South Wales security industry are undertaking the role of compliance checking and, I believe, have powers of sanction for minor breaches of the regulations. More serious breaches are referred to the regulator which, in this case, is NSW police.

A licensing system for some surveillance practices

16. Should users of some forms of surveillance practices be required to obtain a licence from a regulator?

It is considered that, in certain situations where surveillance is particularly invasive or the material being gathered is particularly sensitive, a licensing system should be considered. However, as stated previously, as surveillance is usually provided out of control room or monitoring centre which is already bound by the extensive mandatory codes of the grading system of Australian standards and in which all operators must be licensed requiring the completion of mandatory competency based training units, it is considered that there is no need to re-invent the wheel or impose a secondary regulatory system.

Surely some reason can be achieved whereby the license required to conduct the activity of surveillance is merely an extension of the Control Room or Monitoring Centre Operators current license requirements. Same should apply for businesses conducting surveillance.

17. Are there any surveillance practices in Victorian public places that are particularly concerning? If so, why?

Covert surveillance should only be allowed to be practiced by certain persons holding specific public office (police, army intelligence) for a proportional legitimate purpose. Other forms of invasive surveillance such as x-ray body scanners should require licensing. These forms of surveillance are most open to abuse, however, even the more traditional camera surveillance can also be very invasive.

Changes to clarify and strengthen the *Surveillance Devices Act 1999 (Vic)*

18. Should the SDA (Vic) expressly prohibit the use of an optical surveillance devices in toilet areas, shower areas and change rooms?

Absolutely. These areas must remain private. However, there should be forms of security within these areas which can easily raise an alarm if the occupants require assistance or are at risk.

19. Should the definition of 'tracking device' in the SDA (Vic) be amended so that it includes all devices capable of determining the geographical location of a person or an object?

This would seem logical however exemptions may need to apply to law enforcement bodies when serious issues of public safety are at risk.

20. Should the SDA (Vic) be amended to include a new 'catch-all' category of surveillance devices to cover those devices that do not fit within the Act's existing listening, optical, tracking and data surveillance categories? How could this be done?

A 'catch-all' category may eliminate the need for SDA (Vic) to continuously revise its prohibition categories covering the types of surveillance devices that fall within the definition covered by a mandatory code or existing laws. It seems that, like all security equipment, the technology is developing so quickly it may become an onerous, if not impossible, task for a list of devices to be continuously updated to include all such relevant devices.

21. Should the exemption for participant monitoring in the SDA (Vic) be removed? If so, should this also be done for both listening and optical surveillance devices?

Yes – it should be extended for both listening and optical surveillance devices. It would be considered that the Privacy Laws would require permission from the other party/parties participating in the activity under surveillance to give permission for the surveillance to occur. Otherwise they should expect to have reasonable rights to privacy.

22. Should the enforcement regime of the SDA(Vic) be extended to include civil penalties?

Just as care must be taken not to over regulate, care should also be taken not to apply disproportionate penalties. Therefore, the use of civil penalties for minor breaches would be appropriate. However, when the breaches become severe these should be dealt with by an appropriate public officer (police) and criminal penalties may apply.

23. Should the regulator's proposed powers to develop guidelines be extended to clarifying the meaning of consent in the SDA (Vic)? If so how should the meaning of consent be clarified?

This would seem another appropriate course of action as implied consent can be a very grey area. Guidelines could be drawn up in conjunction with industry stakeholders.

Creating a statutory cause of action for serious invasions of privacy

24. Should there be a statutory cause of action for serious invasions of privacy along the lines proposed by the ALRC?

Yes.