Electronic Surveillance Reform

CRF Response to the Discussion Paper

21 September 2021

Introduction

1. The Carly Ryan Foundation is a not-for-profit, registered harm prevention charity created to promote internet safety and prevent crime against children under the age of 18 years. The Foundation supports families and the community through education, awareness, engagement, harm prevention, promotion and political advocacy.

2. The Foundation's namesake, Carly Ryan, was murdered by a sexual predator in 2007. Digital connectivity was key in providing her murderer the opportunity to engage in a sustained campaign of emotional manipulation that abused her trust and youthful innocence, making it the first crime of its kind in Australia.

3. Since its establishment in 2010, the Foundation has been at the forefront of educating children and youth on online risks through a school-based education program. Students are encouraged to engage their critical thinking skills on topics such as bullying, online child sexual exploitation, image-based abuse and the harmful impacts of online pornography. The Foundation assists in the development of positive self-protective behaviours by raising awareness on the laws that protect them, where to go for help and the importance of consent.

4. The ability of law enforcement to respond to online crimes against children is critical, and the Foundation takes a 'lead by heart' approach in advocating for improving its ability to respond and investigate these crimes. For too long offenders have been able to use unregulated online spaces to abuse children, young people and vulnerable adults. This type of criminal offending is sadly a continuation of what occurs offline, but with every advancement in technology new ways to abuse emerge in lockstep. It's a natural conclusion for the Foundation that law enforcement should then have access to a framework of electronic surveillance that allows them to possess a similar agility in preventing and responding to these crimes.

5. It is also acknowledged that this cannot be achieved without balancing the democratic principles that maintain public trust in our institutions and rule of law, and so it is within this context that the Foundation contributes to this discussion paper and responds to the questions contained therein.

Question 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?

6. Existing prohibitions and offences against unlawful access to information and data are challenged by evolving technological capabilities, in the same way it challenges our traditional understanding of privacy. This results in privacy not being adequately protected by the current prohibitions and offences.

7. Prefacing access to information and data by first describing a general prohibition is useful; it demonstrates that the priority is on privacy, not access. However, as has been established by the Comprehensive Review, access is based on specific technologies. Continuing with this model will not achieve the technology-neutral guiding principle of reform.

8. Another guiding principle of reform is to better protect individuals' information and data, which feeds directly into the notion of 'privacy'. Unfortunately, privacy is not a well defined term. For example, Article 17 of the International Covenant of Civil and Political Rights protects privacy, but offers no further explanation of the term: "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation."[1]

9. It has been noted that privacy can generally be understood as being able to control access to personal information, access to 'oneself' or controlling the management of social interaction.[2] The Foundation adopts a similar approach and views privacy as a catch-all to describe *the importance of an individual being able to control or choose the extent they wish to be known by others at any given moment*.

10. In this regard, if the new framework wishes to better protect individuals information and data, then this feeds directly into the Privacy Act Review.[3] Alternatively, the new framework could make it clear that it deals only with privacy in relation to regulating government agency surveillance powers. Criminal offences of privacy intrusion should be within criminal code, and civil privacy intrusion should lie within the new Privacy Act. However, the Foundation considers this approach as a missed opportunity to develop a holistic, streamlined understanding of what privacy means in the 21st century. Importantly, a streamlined understanding would generate the public trust that is necessarily required to maintain a surveillance framework based on democratic principles.

Question 2

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

11. The Foundation has no comment on this question other than to support the pursuit of objectives of societal benefit. Where these objectives are pursued, information and data gathered should, in general, not be able to identify any one individual. Exceptions could include protecting an individual against loss through a scam, for example.

---

[1] *International Covenant on Civil and Political Rights*, opened for signature on 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976) art 17.
[2] Joel Kininmoth et al, 'Privacy Concerns and Acceptance of Government Surveillance in Australia' (2018) *Australasian Conference on Information Systems* 2018 (Sydney, Australia) p 3.
[3] See Attorney General's Department, 'Privacy Act Review - Discussion Paper' https://consultations.ag.gov.au/rights-and-protections/privacy-act-review-discussion-paper/.

Question 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?

12. Agencies that operate within regulations that create criminal offences may have an interest in accessing particular information and data. For example, Centrelink fraud generates criminal offences, and so the prosecution of fraud investigations may benefit from accessing particular information and data.

Question 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?

13. The proposed considerations appear appropriate.

Question 5 - Question 11

14. Reexamining the definitions of key concepts is beyond the expertise of the Foundation. However, if one of the principles for reform is providing a framework that is technology neutral, it seems counterproductive in anchoring the new framework in terms that are considered outdated even by the technology we already have. As the Foundation sees it, the most efficient way to remain technology-neutral is to focus on the outcomes or effects of privacy intrusion, rather than attempting to describe the mechanics of technology use.

15. It is noted that ASIO suggested a similar approach of outcome/effect focus in their submission into the Comprehensive Review.[4] Their reasons in suggesting this approach were:

    - minimise the risk of capability gaps emerging between different warranted powers
    - provide greater operational flexibility for agencies to use the most appropriate surveillance capability at different points in time, and
    - achieve greater administrative efficiency from being able to make an omnibus application.[5]

16. This approach was considered but ultimately rejected on the following:

    - For agencies, issuing authorities and oversight bodies that deal with these powers on a daily basis, some continuity is likely to reduce the risk, complexity and cost of transitioning to a new legal framework.[6]

[4] See Report of the Comprehensive Review ('The Comprehensive Review') of the Legal Framework of the National Intelligence Community, Chapter 26 p 245 where ASIO is quoted as saying "We propose shifting the legislation's emphasis to the effects sought rather than the tools being used. This could, for example, be in the form of a single authorisation which approves the intrusion into an individual's privacy for the purpose of collecting security intelligence - irrespective of the particular methods that may be applied."
[5] Report of the Comprehensive Review, Chapter 27 p 272.
[6] Report of the Comprehensive Review, Chapter 27 p 272.

- For the Parliament and the public, whose trust and support will be required to develop, pass and implement the new Act, maintaining a degree of continuity is likely to assist them to understand and engage with the key changes that we have recommended.[7]

17. The Review went on to note that their view is "it would be possible to achieve the benefits outlined [by ASIO], while also taking the benefits of retaining familiar concepts and powers, by retaining separate warrants for covert access to communications, computer access and the use of surveillance devices, but harmonising the limits, controls and safeguards that apply to equivalent powers."[8]

18. Instead of maintaining continuity in concepts and powers, the Foundation argues that continuity can be found by anchoring warrants according to the agency requesting use, or to an overall privacy against government surveillance principle. As the Review commented more than once, each surveillance power has a similar impact on privacy.[9] Why keep them connected to concepts and terms that will need regular reviews to keep pace with a technology that is already evolving beyond current concepts? What is the purpose of defining communication, computer access and surveillance devices when they are all as intrusive as each other?

19. An outcome-focus approach could still include harmonised limits, controls and safeguards.

Question 12

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

20. As noted previously, all the kinds of information mentioned within the current warrants involve similar levels of intrusions into privacy; what differs is the outcome of the intrusion. This question goes to the *extent to which an individual wishes to be known by others*, according to the Foundation's interpretation of privacy. The phrase 'known by others' introduces the concept of social judgement of an individual. So when considering the impact of privacy intrusion, perhaps this can be viewed as considering the extent to which an individual will experience negative social judgement. This will undoubtedly be linked to the nature of the criminal offence/security concern that justified the intrusion.

Question 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?

21. If the purpose of electronic surveillance is to investigate or disrupt crimes or threats to national security, then useful information is potentially any information that speaks to the actions or intentions of an individual. Consequently, any technology that has the capacity to capture actions or intentions could be covered. For example, is it possible that someone's Netflix viewing history can be used as circumstantial evidence to prove intention to commit murder or

[7] The Comprehensive Review, Chapter 27 p 272.
[8] The Comprehensive Review, Chapter 27 p 272, 27.19.
[9] See para 26.80, 26.93 and 29.70 of The Comprehensive Review.

engage in a terrorist act? As we continue to develop the ability to break down a human being's identity by analysing the large data footprints they leave, this could be a potential outcome. If Facebook data can already predict someone's sexual identity, this isn't as far-fetched as it may first seem.[10]

22. This is also another argument for reviewing the electronic surveillance framework in line with the Privacy Act Review: how privacy will be defined and protected within the 21st century will impact the amount of information and data that will be allowed to be collected by communications providers and others (and therefore available to access through warrants).

Question 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?

23. The above approach is impacted by the same restrictions of linking surveillance to technology, which runs against the reform principle of remaining technology-neutral. How can information that is obtained by surveillance devices be clearly separated from information collected by a computer access warrant? If it can be, the definition of information in either case will continue to be shackled to specific technologies (ie. surveillance devices or computers).

Question 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?

24. As previously described, a framework that has an outcome or effect focus keeps privacy protection firmly in the mind of organisations using electronic surveillance powers, and also the decision makers who authorise them.

Question 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?

25. Please refer to previous responses regarding an outcome focus framework.

Question 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?

[10] See Facebook can tell whether you're gay based on a few 'likes,' study says (NBC News, 23 November 2017).

26. If warrants continue to be framed by the current powers, then it is appropriate to harmonise legislative thresholds. As has been previously mentioned, all powers give similar levels of intrusion into privacy. It makes sense then that all powers should have similar levels of thresholds to meet before the intrusion is granted.

Question 18

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

27. The Foundation has no comment on this question.

Question 19

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

28. The Comprehensive Review says that tracking information should be treated at a lower threshold because a person's movements are typically observable to others and less private in nature. However, this goes to the amount of data that can be accumulated and what emerges from analysis of that data. Tracking information, if there is enough of it, can build a significant picture of a person (especially if AI is applied in analysing it).

29. If access to information is based on the Foundation's definition of privacy, then tracking information would be treated in the same way as any other intrusion.

30. In relation to agencies' ability to internally authorise the use of tracking devices where it does not involve entry onto premises without permission or interference with the interior of a vehicle without permission of the owner, the Foundation supports retaining this ability. Although it is noted that these two exceptions are based in potentially outdated understandings of private and public spaces. This could be worth reviewing either through this consultation or the Privacy Act Review.

Question 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)?

31. There is a definite need to be able to retain warrants in relation to third parties, groups, unidentified persons and foreign intelligence, but the presumption to target a person in the first instance is appropriate for most functions. Object or premise-based warrant should also be retained.

32. Incorporating SLAID warrants into the framework is also an important function to retain, especially in relation to law enforcement work relating to child sex offending, sex trafficking, and human slavery (where there are significant global criminal networks).

Question 21

Is the proposed additional warrant threshold for third parties appropriate?

33. Yes, this is appropriate. There is a global network of coordination in the sharing of child sexual

abuse material, and significant dark web forums that support and encourage the sexual abuse of children. However, where third party thresholds are introduced to powers that didn't before have them (such as a computer access warrant), the impact to an agencies' investigations should be minimal (ie. not introduce delays, or unnecessary hurdles).

Question 22

Is the proposed additional threshold for group warrants appropriate?

34. Yes, this is appropriate, with the similar disclaimer as above.

Question 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?

35. The Foundation has no further considerations to add.

Question 24

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

36. Independent authorities should continue to remain decision makers for law enforcement agencies. The Foundation has no particular view on seniority or authority other than it seems appropriate for the authorising body to operate at a federal level. They should always have resourcing to respond to warrant authorisations in a way that does not compromise the timeliness of investigations.

Question 25

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

37. Principle-based tiered approach seems effective, but open to corruption and abuse. These concerns appear to have been appropriately considered by the proposed safeguards and oversight.

Question 26

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

Information could be destroyed at the point that the reason for obtaining has been finalised (generally through prosecution and conviction), but the Foundation has no strong views on this matter other than there should be a presumption that information will not be retained indefinitely.

Question 27

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

38. The proposal to not exhaustively define what amounts to an emergency seems appropriate. The Foundation agrees with the approach to focus on whether the purpose of the warrant would be defeated by the delay involved in obtaining written authorisation.

Question 28

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

39. The Foundation offers no further considerations.

Question 29

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

40. These could be matters that are considered in the Privacy Act Review, if the focus in this consultation is electronic surveillance.

Question 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?

41. There is significant nuance in balancing crime prevention and national security interests against the privacy of Australian citizens. As Kininmoth et al noted:

> Policy makers should exercise caution, however, as reliance on emotional responses could potentially lead to counter-productive effects if a similarly emotionally evocative story or campaign were to diminish perceived need for surveillance, leading to widespread rejection and evasion of government security policies. Arguably, this is particularly likely if such a campaign were to undermine public trust in the government, given that *an individual's general trust in the government also significantly determines the acceptance of surveillance*. Efforts to maintain transparency around the use of surveillance methods and techniques would potentially improve general public trust in the government, and also lead to sustained or even increased acceptance.[11] (emphasis added)

42. The Foundation believes that a clear and simplified oversight framework is only one of many factors that can increase general trust in government, and encourages governments moving forward to continue focusing on representation based on tolerance, respect, evidence-based and rational decision-making, and beneficial long-term outcomes.

Question 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?

43. The Foundation has no recommendations for this question.

[11] Joel Kininmoth et al, 'Privacy Concerns and Acceptance of Government Surveillance in Australia' (2018) *Australasian Conference on Information Systems* 2018 (Sydney, Australia) p 9.

Question 32

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

44. It would be useful if there could be a central repository (where possible) that contained reporting of (as examples only):

    - How many people have had their privacy invaded by the use of electronic surveillance powers;
    - How many times a warrant request has been denied/issuing authority requested additional information or amendments to terms of warrant;
    - How many times the emergency issuing of a warrant had occurred, or the usual warrant process was not followed (in comparison to the amount of usual warrants authorised);
    - How many people's (and how much) information had been destroyed, or something to that effect;

    This could be something that the Commonwealth Ombudsman and IGIS could provide annually through the annual reports (noting that some reporting of these measures already exists). It may be seen as obfuscatory if this information was only made available through estimates questioning.

Question 33

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

45. The Foundation has no further suggestions.

Question 34 - Question 36

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

46. The Foundation defers to the experience of industry and authorising bodies in responding to these questions.

Question 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?

47. The Foundation currently has no view on these matters.