

The Director, Online Content
Department of Communications and the Arts
GPO Box 2154
Canberra ACT 2601

Dear Sir/Madam,

Submission in relation to the Discussion Paper on a civil penalty regime for non-consensual sharing of intimate images

Thank you for the invitation to provide comments on the Discussion Paper regarding the civil penalty regime for non-consensual sharing of intimate images (the Discussion Paper).

The Office of the Commissioner for Privacy and Data Protection (CPDP) administers the *Privacy and Data Protection Act 2014* (PDPA), which is designed to protect all information held by the Victorian public sector, including individuals' personal information. While the non-consensual sharing of intimate images between individuals falls outside the remit of my office, I welcome the opportunity to provide comment on this important issue, which bears on the privacy of Victorians and all Australians.

The significance of non-consensual sharing of intimate images, or image-based abuse, goes beyond privacy and speaks to broader social issues of gendered violence and equality. While people of all genders can be subject to technologically facilitated abuse, based on the research available it is clear that image-based abuse is predominantly used as a tool of power and control by men against women. Further, harm from image-based abuse is not limited to the individual; there are broader public harms that flow from the intersection of technology with sexual and domestic violence.

One of the shortcomings of privacy law in Australia, including both the *Privacy Act 1988* as well as Victoria's *Privacy and Data Protection Act 2014*, is that despite having its roots in human rights law it offers very little protection for privacy interferences that fall outside the area of information privacy in government or the private sector. In particular, there is limited redress for individuals whose privacy is interfered with by another individual. Unfortunately, this gap in privacy regulation means the tools available to individuals when responding to breaches of their privacy are largely insufficient.

Since 2014, Victoria has been one of the few states in Australia with legislation in place to combat image-based abuse. However, as the 2015 Senate Inquiry observed, there remains need for a consistent and uniform approach across Australia.¹ A civil penalties regime, in combination with other measures, such as a national statement of principles relating to the criminalisation of image-based abuse, would go a long way to addressing this need.

The issues raised by the Discussion Paper are numerous. I will limit this submission to three observations in relation to privacy.

¹ Senate Legal and Constitutional Affairs References Committee, Parliament of Australia, *Phenomenon colloquially referred to as 'revenge porn'*

The government response: use of technological tools and information sharing across organisations and jurisdictions

In order to deal with image-based abuse quickly and effectively, there will undoubtedly be a need to share information between organisations and across state and national borders (Issue 4). As the nature of this information will be both personal and sensitive, it is vital that privacy and protective data security measures are in place. Unfortunately, there remain several states in Australia that lack robust legislative privacy and data security protections. As such it should be considered from the outset how state and federal agencies can come to an agreement on sharing personal information regarding image-based abuse where the privacy and security provisions are not of equal standard.

We recommend that one set of standards be adopted for the handling of this kind of information. While still in its infancy, the Victorian Protective Data Security Framework (VPDSF) published by my office in June 2016 is an example of a proportionate and risk-managed approach to security. We have also published guidelines on Information Sharing, which, while written in a Victorian context, provide a robust framework for approaching information sharing situations. The Department may wish to consider these guidelines as well as the VPDSF as a policy framework for managing data security across any information sharing arrangements.

Regarding the technological tools used to combat as well as respond to technological abuse, I would like to reiterate the importance of assuring adequate privacy and security protections are *built-in* to the technology from the outset (Issue 10). It goes without saying that any public-facing portal for information collection or online complaints process must treat the personal information collected in accordance with information privacy law, and appropriate protective data security protocols. This means considering a range of matters from the security architecture of the system itself to the law and policy surrounding the use of information collected.

It is important to emphasise that while image-based abuse is not solely a privacy issue, those seeking redress will have suffered an immense breach of trust and invasion of their privacy. It should follow that any interaction with government should not exacerbate the harm caused to that individual in any way. In order for technological tools to be effective there must be an established level of trust as individuals are unlikely to use them if they feel their privacy may be further compromised. It should be communicated clearly with individuals that their privacy is valued and protected.

Consent

As highlighted by the Discussion Paper, consent can be a complex area, and the nature of sharing content online does not allow for such nuanced understandings of consent. While consent remains an important concept when it comes to control of one's personal information, placing too much emphasis onto it can be problematic. For instance, the notion of implied consent in this context would need to be considered carefully. If an image has been wilfully taken or voluntarily shared initially, this should not amount to implicit consent to use or disclose the image beyond that original purpose (Issue 22). Similarly, consent given at a particular time cannot be assumed to endure indefinitely, and individuals should be able to change their mind and revoke said consent (Issue 25). Further, the question of meaningful consent is a major factor in the context of non-consensual sharing of intimate images. The fact that power dynamics within relationships may impede upon the individual's ability to give *meaningful* consent should not be overlooked (Issue 21, 23). For these reasons, it may be preferable to place less emphasis on the role of consent to share intimate images. In any case, the onus of proof to show consent should be with the perpetrator, *not* the complainant (Issue 24).

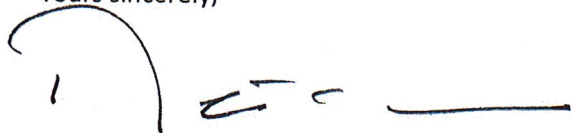
'Sharing' and 'intimate images'

The definition of 'intimate images' should not be explicitly sexual in nature. The consideration as to whether an image is intimate or not should firmly rest on whether there was a reasonable expectation of privacy at the time it was captured and/or if there was a reasonable expectation of privacy at the time it was shared. Focussing solely on the sexualised nature of the images runs the risk of adopting a narrow understanding of 'intimate' and overlooking other intimate but not overtly 'sexual' situations. For example, an image of a Muslim woman without her headdress could cause harm in a similar way (Issue 26, 28). Similarly, the definition should include digitally manipulated images, as the damage caused to an individual's online reputation by distributing such content can be comparable to if the images were genuine (Issue 27).

An image shared with one person should not necessarily be considered to be less harmful than an image publically shared with a wider audience or unknown parties (Issue 31). The harm that results from non-consensual sharing depends on the context, and the size and nature of the audience should be considered as just one factor when determining harm. For instance, sharing with one person could have potential to cause significant harm (for example, to an employer, significant other, or family member) just as much as sharing more broadly.

If you have any questions regarding the above comments, please contact Samantha Floreani at [redacted]. Once again, thank you for the opportunity to make a submission regarding this Discussion Paper, we look forward to watching with interest as this discussion progresses.

Yours sincerely,



Adjunct Professor DAVID WATTS
Commissioner for Privacy and Data Protection