[Draft for Human Rights Committee Discussion]

Law Society Position on Face recognition technology and the Right to Privacy

1. The right to privacy is protected at the international level. See, eg, Article 17 of the *International Covenant for Civil and Political Rights* which provides: '1. No one shall be subjected to arbitrary or unlawful interference with his [sic] privacy, family, home or correspondence, nor to unlawful attacks on his [sic] honour and reputation. 2. Everyone has the right to the protection of the law against such interference or attacks': *International Covenant for Civil and Political Rights,* opened for signature 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976). The right to privacy is not absolute, and can be subject to justifiable limitations if shown to be necessary, effective and proportionate to achieving a legitimate end.

2. The use of facial recognition technology – which extracts information from the contours of a person's facial image in order to match it with another – has a direct impact on the right to privacy. It extracts, stores and compares highly sensitive personal information. Because of the highly sensitive nature of the information it collects, the use of facial recognition technology must be subject to strict safeguards and limitations in order to constitute a justifiable limitation of the right to privacy.

3. Facial recognition technology can be a valuable rights-enhancing tool if the following conditions are met:
    1. Accuracy of technology can be assured
    2. Security of data and data storage can be assured
    3. Facial images are obtained with informed consent
    4. Use and sharing of facial images occurs with informed consent
    5. Legal safeguards are in place to guard against non-consensual or unauthorised use, sharing or storage of facial images.
    6. Specific legal protections are in place to protect privacy rights.

4. These conditions are not currently present in South Australia. This is because:
    1. There is no standalone right to privacy at the federal level in Australia,[1] or under South Australian law, although there are a range of legislative and regulatory protections that operate to limit the use, disclosure and sharing of personal information in certain contexts
    2. Unlike many other Australian jurisdictions, South Australia does not have legislation specifically concerning privacy. Instead, in South Australia, privacy complaints relating to state departments, for example the Department for Correctional Services, the South Australian Housing Authority, the Department

[1] The right to privacy is protected at the international level. See, eg, Article 17 of the *International Covenant for Civil and Political Rights* which provides: '1. No one shall be subjected to arbitrary or unlawful interference with his [sic] privacy, family, home or correspondence, nor to unlawful attacks on his [sic] honour and reputation. 2. Everyone has the right to the protection of the law against such interference or attacks': *International Covenant for Civil and Political Rights,* opened for signature 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976).

for Child Protection, are handled by the Privacy Committee of South Australia (herein after 'the Privacy Committee').

3. The laws that currently authorise the use of facial recognition technology in a range of contexts (including covert collection) do not include robust protections against the non-consensual or unauthorised use, sharing or storage of facial images.

5. As a result we support a moratorium on the use of facial recognition technology until specific legislative safeguards can be developed as recommended by the Australian Human Rights Commission's in its *Human Rights and Technology Report*.

6. The model established in the ACT *Information Privacy Act 2014* could provide a model for South Australia. This legislation describes facial recognition technology and biometrics as 'sensitive information', includes specific safeguards around personal information whilst still acknowledging legitimate exceptions; includes practical Privacy Principles for departments and others to adhere to, and includes an accessible complaints process.