Facial Recognition

Technology Threats

Submission to the Federal Government

on the Proposing legislation of Facial Recognition Technology

From the Australian Privacy Foundation

**1. Introduction**

With the development of Artificial Intelligence as well as the improvements in computing technology and other areas, the Facial Recognition technology has recently become a so-called "hot shot" in technology companies and some developed countries (Gates, 2002).

This report here is a business submission to the Federal Government on behalf of the Australian Privacy Foundation, who strongly resists the proposal to apply facial recognition technology without constraints to people and organisations who have access to it. The Australian Privacy Foundation without doubt believes that the potential risks that the country is going to take, and the mess of pottage it receives by applying this technology everywhere, in exchange of convenience and surveillance, would not be nutritious. The appliance of the technology does have its advantages, but it will pose as many drawbacks in the meantime.

Thus the Australian Privacy Foundation is in no way supportive of the legislation, and this report will address its potential dangers and threats that may have been overseen and will only take effects after the legislation. That is, the universal employment of facial recognition technology would, if unwisely used, encroach on citizens' privacy as well as erode people's freedom and their sacrosanct human rights.

**2. Organisation Background**

The Australian Privacy Foundation is an organisation that is dedicated to protect citizens' privacy rights. It aims to raise concern among people about the rising issues that pose damage or destructing effects on people's freedom as well as their privacy. By joining a privacy network that is distributed worldwide called the Privacy International, as well as by working with other consumer organisations, civil liberty councils, and professional associations plus other community groups on privacy issues, the organisation has successfully ensured the Commonwealth Government’s changes to privacy legislation to cover the private sector. The organisation also prioritises the task of contributing to the development of industry codes, and more importantly, as will be discussed in this business submission, the task of highlighting privacy risks in emerging technologies which also includes biometrics and facial recognition technology as is discussed here.

1. **Current Issues**

Concerning the facial recognition technology, and upon reflection of the possibility of its universal application, there are two basic issues that are vital to every citizen, and should be brought into the Government's decision making process. First, the possibility of data leakage. To store all the data in one place, even if it is guarded by the government, could still not be secure enough, since data is stored in computers, but is guarded by men. Thus, if the data is not well protected, it could potentially cause serious consequences (Sebastian, 2020). The progress that have been made in recent years have witnessed the massively growing size of information gathered, uploaded, and stored. Besides, according to the results of the study carried out by the scholars mentioned earlier, the overall, nationwide application of facial recognition technology could have the potential risk of jeopardising Australia's national security, since there could be rival countries that seek to steal the information if it is improperly protected, or the information might leak due to various causes.

Moreover, it is still a contested area, as it has always have been, whether there should be nationwide adoption of facial recognition technology, since diverse views will rise and all respectively have their grounds justified. Among them, one view from the people would be the concern of whether the information, if they consent the uploading and storing of it. would be misused.

An example can be given here. The worldwide famous information technology company, Facebook, was before facing rather heavy fines due to its violation on the user privacy code (Young, 2013). In this case, the "user privacy", being defined as user information, was intended to be used only for commercial analyses and other advertising objectives (Ferguson, 2019).

Thus the problems can be clearly defined as: First, would the "storage system" be secure enough to prevent leakage or theft? Second, would the government or other officials misuse the technology to enforce surveillance and censorship? Third, would the technology be so effective that crime rate could actually drop as it was expected? The federal government would need to, before implementing the proposal and before anything is too late, have ensured itself and the citizens on these issues. There would be controversies otherwise if the decision is made without due consideration.

**5. Historical Development of the Technology**

The facial recognition technology falls under the category of Identity Recognition Technology (IRT). Historically, fingerprint technology has been until this day used universally as the most secure IRT (Mann, 2017). However, as science progresses, the facial recognition technology has substituted fingerprint technology as one form of IRT in that it allows faster and more accurate recognition of one person out of crowds, while at the same time remain away from people under its scanning. With the help of high speed computing algorithms, this technology has already embarked on new frontiers of recognition. The New Zealand Customs Service had invented a program SmartGate in collaboration with the Australian Border Force. The program incorporates facial recognition technology to compare the travellers' faces with the images on e-passports (Enus, 2020).

The federal government currently wishes to employ the facial recognition technology and store the information gathered in a database belonging to the National Home Affairs, The plan is to use the data to assist the government and its agencies, the banks, and other companies that involve identification, e.g. telecommunication.

1. **Submission as a solution to the issues**

This business submission includes a proposal that may serve as a solution to the current dilemma that concerns government regulation. It concerns how to ensure the data stored would not be misused, and that what ways we can better our use of the technology to actually help protect citizens' privacy (Crawford, 2019).

To ensure there will not be misuse of the technology, supervision must be included in the implementation process. Power contained is power for the good, and citizens themselves should also be included in the supervision framework as well as the government. Rights protected should be rights known. Government should make the use of information available to citizens online to reassure the people that the implementation is for the good of the all (Phillips, 2012).

Secondly, since it is and will always be a privacy issue on desk, then the government should do its best to ensure the data would not leak or stolen. That means there should be safeguard policies that are specially designed for the system. Experts, white hat hackers, consulting institutions, privacy organisations and more should all be consulted to line out a plan that would not only protect people from crime, but also their privacy.

1. **Counter Arguments**

One of the counter arguments stress upon the effectiveness of facial recognition technology to prevent crime and other hazards from happening. However, that objective could be reached in other ways, and there would not have been erosion on privacy as one of human rights. The Australian Privacy Foundation insists that human rights protection weighs as much as crime prevention, and that the government should without haste weigh up the pros and cons of installing this technology.

**8. Conclusion**

This business submission is, on behalf of the Australian Privacy Foundation, to the federal government to halt the current contested implementation of facial recognition technology. There should not be any pre-installment before safeguards are all set up and viable ways of protection of the data are found. The organisation holds the opposition view to the implementation of the technology in that it erodes one basic human rights.

**References**

Crawford, K. (2019). Halt the use of facial-recognition technology until it is regulated. *Nature (London), 572*(7771), 565–565. https://doi.org/10.1038/d41586-019-02514-7

Enus, F. (2020, July 10). *Australia’s privacy watchdog has joined forces with its UK counterpart to investigate the facial recognition technology firm Clearview AI*. In World News Australia.

Ferguson, M. (2019, April 25). *Facebook privacy breach: Facebook bosses are expecting a fine of up to $7 billion following a US federal probe into privacy violations*. In Seven News.

Gates, K. (2002). Wanted Dead or Digitized: Facial Recognition Technology and Privacy. *Television & New Media, 3*(2), 235–238. https://doi.org/10.1177/152747640200300217

Mann, S. (2017). Automated facial recognition technology : recent developments and approaches to oversight. *University of New South Wales Law Journal, 40*(1), 121–145.

Phillips, T. (2012, May 3). *Facial Recognition: New facial recognition technology tracks and identifies individual faces in a crowd*. In Catalyst.

Sebastian, M. (2020). Normalizing resistance: saying no to facial recognition technology. *Feminist Media Studies, 20*(4), 594–597. https://doi.org/10.1080/14680777.2020.1750790

Young, Q. (2013). PRIVACY PROTECTION STRATEGIES ON FACEBOOK: The Internet privacy paradox revisited. *Information, Communication & Society, 16*(4), 479–500. https://doi.org/10.1080/1369118X.2013.777757