New Zealand's Privacy Commissioner Releases Draft Biometrics Privacy Code

Biometrics is a trending issue and with the development of technology there are consistently more ways biometric data can be used, from replacing a password to identifying repeat shoplifters in a shop. With these developments, issues have started to be identified from a privacy perspective.

Last year, the Privacy Commissioner (**Commissioner**) announced the intention of his office to release an exposure draft for a privacy code that will govern the collection and use of biometric information in biometric processing in New Zealand. The exposure draft of the Biometric Processing Privacy Code (**Code**) and an associated consultation document have now been released.

Biometric information – what is it?

Biometric information relates to a person's physical and behavioural characteristics. For example, a person's facial features, voice, fingerprints, signatures, keystroke patterns, and more. Biometric information is personal information and is already regulated by the Privacy Act 2020 (**Act**). However, the Commissioner considers biometric information to be a special type of personal information that requires specific protection in certain circumstances.

What are the concerns?

The use of biometric information can have great benefits, including convenience and security. But there are risks too. The Commissioner has identified risks such as lack of transparency and control, accuracy, bias, and risks relating to surveillance and profiling. The Code is intended to give some guidance as to how this type of information can be processed and used.

The Commissioner is seeking feedback on the Code and is asking three main questions:

- How should organisations have to balance the benefits and disadvantages of biometrics before using them?
- How and what should people be told when their biometrics are being collected?
- What are some things that biometrics should not be used for?

So, what exactly does the Code cover?

The new Code is intended to apply to the activity of biometric processing and biometric information (as a class of information for the purpose of that activity). The Code applies to the use of biometric information to recognise or classify people by way of biometric processing.

The Code sets out thirteen rules that must be complied with when undertaking biometric processing and collecting, using and disclosing biometric information. Overall, there are general similarities with the thirteen Information Privacy Principles (**IPP**) in the Act. However, some key changes have been suggested. These include:

Rule 1 of the Code

Rule 1 of the Code places responsibility on organisations to demonstrate that their biometric processing is proportionate. In the Code, in addition to only collecting biometric information for a lawful purpose, organisations must not collect biometric information for biometric processing unless (1) they believe on reasonable grounds that their biometric processing is

proportionate in the circumstances and (2) they have put in place any privacy safeguards that are reasonable in the circumstances.

Rule 3 of the Code

The proposed Rule 3 would, amongst other things, require organisations to have a clear and obvious notice advising individuals that biometric information is being collected, the specific purposes the biometric information is being collected for and whether there is an alternative option to biometric processing available. Agencies will also need to have an easily accessible notice that advises individuals of additional information such as the agency's retention policies, complaints processes, policies, procedures and protocols for the collection and disclosure of biometric information.

Rule 4 of the Code

The Commissioner wishes to restrict certain unfair and intrusive uses of biometric processing. Accordingly, Rule 4 of the Code prohibits an agency from collecting information about an individual's health by way of biometric classification (a type of biometric processing), using biometrics to obtain information about a person's emotional or physical state or to place individuals into restricted biometric categories e.g., age, race, sex, ethnicity, etc.

The default position under the Code is that these types of biometric activity are prohibited unless an exception applies. The intent is that these types of biometric processing will only be used where there are clear benefits.

Upcoming developments

The Commissioner is currently in the process of reviewing submissions received on the exposure draft. There will then be a further period of formal consultation before the Code can be issued.

Authors - Julika Wahlmann-Smith, Partner and Brooke Taylor, Solicitor of Hesketh Henry, Auckland, New Zealand.