consumer.

7 May 2024

Office of the Privacy Commissioner
By email: biometrics@privacy.org.nz

SUBMISSION on Exposure draft of a biometric processing code of practice: consultation paper

1. Introduction

Thank you for the opportunity to make a submission on the Office of the Privacy Commissioner's (OPC) *Exposure draft of a biometric processing code of practice: consultation paper (the Consultation Paper)*.

This submission is from Consumer NZ, an independent, non-profit organisation dedicated to championing and empowering consumers in Aotearoa. Consumer strives to be fair, impartial and provide comprehensive information and advice.

Contact: Jon Duffy
Consumer NZ
PO Box 932
Wellington 6140
jon@consumer.org.nz

2. General comments on Consultation Paper

1. As noted in previous submissions, we agree there needs to be further regulation of biometrics in Aotearoa and we strongly support the introduction of a biometric processing code of practice.

2. In general, we agree with OPC that biometric information is a special type of personal information and warrants specific regulation within New Zealand's privacy regime. We agree that a code of practice is the right mechanism to use under the Privacy Act (the Act) to quickly introduce this subject specific regulation. However OPC (and the Ministry of Justice) may want to consider whether amendments to the Act itself may be required in the future, based on a review of the effectiveness of the final code of practice after a suitable period of time. We

also highlight other amendments that we believe should be made to the Act, regardless of whether a biometric code of practice is introduced.

3. We agree with the scope of the draft code of practice and, in particular, that the scope is broad with the intention of future proofing the code as technologies continue to evolve.

4. We have set out an expanded response on the point of consent as a safeguard below and then responded to selected questions in the Consultation Paper.

Consent as a safeguard

5. We support the rationale behind drafting Rule 1 as an obligation on agencies collecting biometric information, rather than putting the onus on consumers to consent to that collection.

6. Ongoing Consumer NZ research into the use of Facial Recognition Technology (FRT) has produced preliminary findings that suggest consumer awareness and understanding around the use and capability of the technology is limited or confused with other types of surveillance, like CCTV.[1]

7. These findings suggest that even where agencies go through a nominal consent gathering exercise (such as a sign at the entrance to a retail store disclosing the use of FRT), this has little practical benefit where individuals lack the understanding of the technology itself to meaningfully provide their consent.

8. These findings raise the question as to whether agencies currently collecting biometric information using technology such as FRT in quasi-public spaces like supermarkets, are adequately complying with disclosure requirements under the existing IPP 3. The findings also raise the further question of whether those agencies could *ever* comply with a traditional consent model, given the knowledge imbalance between agencies and many individuals.

9. We note the requirements set out in draft Rule 3 and consider these should be expanded to more explicitly require agencies, in appropriate circumstances, to provide a more detailed plain language explanation of what the technology is

[1] Consumer NZ is happy to discuss these findings in more detail with OPC once the analysis is finalised.

doing (for example explaining the differences between FRT and CCTV surveillance). We consider this may be particularly useful as emergent technologies come on the market and consumers are confronted with them for the first time.

10. OPC's proposed approach recognises that technology, such as FRT, is not widely understood and places the onus on the agency collecting the biometric information to justify its use. We agree this is a practical workaround of the traditional consent model, but note the following two concerns with the practical implementation of draft Rule 1:

    10.1 **Monitoring** –to protect consumers and understand the effectiveness of Rule 1 as an alternative to the traditional consent model, OPC will need to implement a monitoring programme to understand how agencies are interpreting Rule 1 and to monitor compliance. This is particularly important where consumer awareness and understanding is low (see above), and agencies are collecting information in spaces where consumers could have limited alternative options (such as supermarkets in rural areas or where transport options are limited). Low levels of consumer awareness and understanding may lead to a lack of complaints against agencies – OPC should be considering its role as a watchdog in these circumstances[2].

    10.2 **Enforcement** – In addition to monitoring compliance, in our view, OPC should be seeking greater powers in the Act itself, to deter and punish non-compliance with the Act generally, including the draft code. The Act plays an important role in protecting consumers from agencies that seek to exploit their positions to gain a commercial advantage. In the same way the Fair Trading Act creates offences and imposes criminal liability on traders for misleading or deceptive conduct, we take the view the Act should contain offences that impose criminal liability for privacy breaches.

    In our view, these provisions should apply to the Act and any codes made pursuant to it. However, to use Rule 1 as a specific example, a business would commit an offence if it collected biometric information for biometric

[2] OPC may also wish to consider whether the information gathering powers it currently has under the Privacy Act are sufficient to enable it to gather the information required to effectively monitor agencies and their collection of biometric information for processing.

processing in circumstances where the risks outweighed the benefits and/or without putting in place reasonable and relevant safeguards.

While creating offences for Act or code breaches may be out of scope for this consultation, it may be more appropriate to pursue following implementation of this code and an appropriate period of monitoring demonstrates evidence of consumer detriment.

3. Responses to specific questions in the Consultation Paper

Question one: How should organisations have to balance the pros and cons of biometrics before using them? (proportionality).

11. In our view the Consultation Paper rightly identifies a risk that agencies will be attracted by the availability and appeal of technology and this could distract from an objective assessment of the benefits and risks of use. Where technology is available in other jurisdictions, agencies could assume that similar checks and balances apply in New Zealand. There is a danger that this risk will be further amplified by marketers promoting the commercial benefits of technology and downplaying or ignoring risks to individuals.

12. Organisations should be able to demonstrate that an objective assessment has been undertaken. Typically, this would be through the documentation of that process.

13. At a practical level, without professional assistance, many organisations may struggle to appropriately balance the risks and benefits of adopting biometric solutions. Technology in this area is likely to develop quickly, producing novel use cases for both organisations considering the technology and regulators. We consider a market for professional services will need to develop to meet the need for advice (beyond that which already exists). We believe effective monitoring and, if appropriate, increased liability for breaches of this draft code of practice and the IPPs more generally (the introduction of criminal liability as discussed above) will be important to incentivise agencies and their Boards to invest in professional advice before adopting biometric solutions.

Question two: How and what should people be told when their biometrics information is being collected? (transparency).

14. We consider disclosure will always be dependent on the circumstances in which the collection of personal information takes place. As noted above, with rapidly evolving technology, to be effective, disclosure may require a degree of education for some consumers. Organisations considering adopting biometric solutions will be best placed to understand the characteristics, including levels of understanding of the individuals who they intend to be subject to the solution under consideration. In most commercial use cases, those individuals will be users or customers of the organisation considering the solution. Organisations should therefore use what they know about their users or customers to tailor disclosure to those individuals. At scale this may mean developing customer cohorts, but scale should not be an excuse to providing sufficient disclosure for individuals to understand what they are consenting to.

Question three: What are some things that biometrics should not be used for (fair processing limitations).

15. We agree that the collection of information by means of biometric classification should be restricted and agree with the rationale set out in the Consultation Paper.

16. We agree that collecting biometric information to infer someone's inner state raises human rights and Bill of Rights issues and could allow that information to be used in ways that threaten freedoms valued in a democratic society. We strongly support the proposal to prohibit the use of biometrics to collect information about a person's inner state (emotions, personality or mental state).

17. In June 2023 Consumer NZ revealed that Westfield shopping centres in Auckland and Christchurch had deployed digital billboards that used AI-powered FRT to analyse customer's biometric information and use it to target advertising at them[3]. Along with age and gender, the technology is also capable of detecting mood to tailor marketing to the individual targeted.

18. Although Consumer NZ received a limited response from Westfield on the use and capability of the technology in question, it appears the technology did not identify specific individuals, only characteristics about them. It is likely exceptions under IPP 3(4) applied to the collection. Notwithstanding the lack of individual identification,

[3] https://www.consumer.org.nz/articles/facial-detection-used-by-westfield-malls-for-targeted-advertising

the use of FRT in a quasi-public space like a shopping centre was surprising and concerning to some people. Two Consumer NZ members summarised their reactions as follows:

> *"This 'if you have nothing to hide, you have nothing to worry about' attitude is so short-sighted. Everyone deserves the right to choose what they reveal or conceal about themselves, even if it is currently innocuous."*
>
> *"Our family were appalled on reading this article. It is becoming exhausting as we learn of the increasing manipulation by advertising people and related industries. We choose to shop at smaller places but sometimes there's little choice. It feels as if our voices aren't being heard. We support Consumer and hope you can speak on behalf of those who do not want this intrusion."*[4]

19. We support these comments from our members and note the sharing of biometric templates based on information collected from individuals without their consent or in many instances, knowledge, creates a risk that this information is shared with other agencies or businesses and could lead to further identification through other processes.

20. It is important to acknowledge other comments on the article referenced above that suggest some people are comfortable with the technology, particularly where it is used to detect and identify known criminals or criminal activity in public or quasi-public spaces. While insight on consumer sentiment is valuable for the broader discussion, this view largely misses the central issue in the article; namely the intrusive collection of biometric information to detect mood for *marketing* purposes. This is a further illustration of gaps in consumer awareness and understanding of the technology as discussed above.

21. In the example above, the fair processing limit on emotion recognition and physical state would restrict Westfield's ability to deploy the technology outlined above in the manner it was deployed leading up to our June 2023 article. Organisations like Westfield would no longer be able to collect biometric information that infers the emotional state of the targeted individual. We agree this is an appropriate evolution of the law and will help address the concerns raised by Consumer NZ members above.

[4] Ibid, comments.

22. We agree with the fair processing limit on categorising individuals into restricted categories and see the Human Rights Act grounds of prohibited discrimination as the most appropriate categories to base this limit on. We note that as technology evolves, further grounds, not currently in contemplation, may emerge and should be considered for inclusion in the code of practice.

ENDS