consumer.

30 September 2022

Office of the Privacy Commissioner
PO Box 10 094
Wellington
Sent by email to: biometrics@privacy.org.nz

SUBMISSION on Privacy Regulation of Biometrics in Aotearoa New Zealand Consultation Paper

1. Introduction

Thank you for the opportunity to make a submission on the Office of the Privacy Commissioner's (OPC) 'Privacy Regulation of Biometrics in Aotearoa New Zealand Consultation Paper' (Consultation Paper). This submission is from Consumer NZ, an independent, non-profit organisation dedicated to championing and empowering consumers in Aotearoa. Consumer NZ has a reputation for being fair, impartial and providing comprehensive consumer information and advice.

Contact: Elizabeth Kim
Consumer NZ
Private Bag 6996
Wellington 6141
Phone: 04 384 7963
Email: elizabeth.kim@consumer.org.nz

2. General Comments on the Consultation Paper

We agree there needs to be further privacy regulation of biometrics in Aotearoa New Zealand. This is particularly important in our rapidly changing environment in which the use of biometric technologies is becoming more widespread.

Biometrics information contains sensitive personal information so needs to be treated with extra care as it relates to the unique characteristics of an individual. Also, biometric characteristics often remain with us for life and

cannot be changed or replaced. It is vital that we protect this.

Although it is outside the scope of the review, as the Consultation Paper notes, there may be human rights concerns about discrimination that can't be fully addressed within a privacy framework, and this review will only address some of the problems and concerns surrounding the use of biometric technologies and information. We have concerns about the greater implications on consumers and their rights. We have expanded on this in our answers below.

3. Answers to Specific Questions in the Consultation Paper

Q1: Do you have any comments on the case for more regulatory action set out above?

We agree there is a strong case for more regulatory action.

Q2: Do you have any comments on the scope and focus of OPC's review of the privacy regulation of biometrics?

We agree the scope and focus of OPC's review of the privacy regulation of biometrics is appropriate.

Q3: Do you have any comments on these assumptions?

We agree with the assumptions set out in the Consultation Paper.

Q4: Do you have any comments on these objectives?

In general, we agree with the objectives set out in Consultation Paper. In our view, OPC should also add an objective aimed at reviewing and strengthening the current privacy regulatory framework.

Q5: If your organisation is a user, potential user or vendor of biometric technologies: how do you or your customers use these technologies (or how might you or your customers use them in future)?

No comment.

Q6: Do you have any comments on the concerns about the use of biometrics discussed in the position paper?

We agree with the concerns listed in the Consultation Paper. We suggest an additional concern about how inadequate regulatory and enforcement powers can impede effective oversight of the use of biometric information

and systems. Where there are ineffective and inadequate regulatory systems in place, we think that the concerns about the use of biometrics becomes greater.

Q7: Are there concerns about biometrics that can't be addressed through privacy regulation (because they don't involve control over personal information)?

As stated above, we recognise there are broader human rights concerns about discrimination that cannot be addressed by a privacy framework. However, we consider that a review of privacy regulations for biometric information in isolation will be insufficient, and that any regulatory action needs to happen in conjunction with a review of the human rights framework.

In our view, this is fundamental to ensuring that any privacy framework or regulation of biometrics is effective. We urge the Human Rights Commission and Honourable Minister Kiri Allan to consider conducting such a review.

We also have concerns about the use of biometric information between private individuals which is then passed on to third parties. We have concerns about the lack of consent in these scenarios. For example, if a private individual approaches a property with a doorbell that captures biometric information about them (with or without their knowledge), and this is then passed on to a third party by a property owner, we question whether the individual has given full consent in these types of scenarios. A recent example of this is where Amazon has created a television show using footage from smart doorbells.

In 2021 the Australian Human Rights Commission published its "Human Rights and Technology Final Report", which included a chapter on biometric surveillance and facial recognition and privacy, recommended the Australian Government introduce a statutory cause of action for the serious invasion of privacy.[1] We would like to see something similar here.

Q8: What factors should be considered in assessing the level of risk from particular uses of biometrics?

In addition to the potential human rights implications, we consider the New Zealand Bill of Rights Act should be considered when assessing the

[1] Australian Human Rights Commission, "Human Rights and Technology Final Report", May 2021.

level of risk from particular uses of biometrics where Government entities are involved.

The New Zealand Bill of Rights Act is part of Aotearoa New Zealand's human rights framework, and ensures the rights and freedoms of individuals are protected from government interference. As noted above, it is essential to consider the human rights implications when establishing a privacy framework, as there are high risks and possibilities of government interference in the use of biometric systems.

Q9: What types of uses do you see as low, medium or high risk?

Low risk:

We consider there is relatively low risk where biometric information is used to strengthen the security of individual's personal information and it is stored locally. For example, biometric information stored on personal devices and used for the purposes of strengthening the security of an individual's personal information i.e. smartphone access.

We consider that in these situations, the risk is low as the consumer most often makes an active and conscious decision to install the biometric system. There is relatively clear consent where the consumer has elected to opt-in to the biometric system. There are usually alternatives for consumers who do not wish to use functionality relying on biometrics. Where biometric information is stored locally, and on the individual device, we consider the potential for the misuse of this information is relatively low.

Medium risk:

We consider that in some circumstances there is medium risk even if there are procedural safeguards and effective oversight of the use biometric information. For example, where biometric information is used for verification purposes and where the individual's identity has already been authenticated and enrolled in a database.

We consider that even if there are procedural safeguards in place and effective oversight, there is still a level of risk that biometric information may be misused in these sorts of situations. However, overall, the use of biometric information to secure personal information or access particular services can be beneficial to the public. Some examples where the application for biometric systems might be of medium risk include using biometric information for national registries to facilitate accessing local

and national governmental services, driving licenses, venue access, secure database access, and computer systems.

High risk:

We consider that there may be high risk where biometric information is used for purposes beyond verification and security. There is heightened risk where biometric information systems are used in sensitive and high-stakes contexts, because in these sorts of situations an error can harm individuals. As the Australian Human Rights Commission notes, "certain biometric technologies are prone to high error rates, especially for particular racial and other groups".[2]

We consider there are high risks in healthcare identity management, criminal justice records, crime detection, CCTV surveillance, border security and passport issuing systems, refugee assistance, and financial services contexts. We think that using biometric information and technologies in these contexts has the potential to harm and create a heightened risk for privacy and human rights infringements. This has been demonstrated by the recent Independent Police Conduct Authority and OPC Joint Inquiry into the New Zealand Police's conduct when photographing members of the public.

This inquiry found that New Zealand Police were not justified in photographing rangatahi and found that the "[New Zealand] Police as an organisation have not developed appropriate training, guidance or policies to enable officers to collect and retain personal information, including photographs, effectively and lawfully".[3] This demonstrates that if users of biometric information and systems do not have adequate processes in place, this contributes to a higher privacy risk. If the New Zealand Police cannot adequately protect photographs, it is unlikely people will have confidence that it can protect and properly collect and use other sensitive biometric information.

[2] "Human Rights and Technology Final Report 2021", page 111.

[3] Independent Police Conduct Authority and the Office of the Privacy Commissioner. "Joint inquiry by the Independent Police Conduct Authority and the Privacy Commissioner into Police conduct when photographing members of the public", September 2022.

Q10: If you are a Māori individual or organisation:

- *what privacy implications do you see for Māori in the use of biometrics*
- *what protections would you like to see for the impact of biometrics on Māori*
- *what should happen to give effect to Te Tiriti in the regulation of biometrics?*

We are concerned about the potential for bias and profiling for tāngata Māori resulting from the use of biometric information and technologies.

Although we aim to represent all consumers, we are not a Māori organsiation, and we are not experts in Te Tiriti o Waitangi, Te Ao Māori, and tikanga Māori. We would therefore encourage OPC to engage Te Tiriti, Te Ao Māori and tikanga Māori experts and communities to seek guidance on matters relating to these areas of expertise.

Q11: Are there any other cultural perspectives on biometrics or impacts on particular communities that OPC should be aware of?

It is important to consider the perspectives of those who are at risk of digital exclusion or heightened risk of harm through the use of biometric technologies. For example, refugee, migrant, and ethnic communities, younger and elderly members of society, trans and gender diverse people, Māori and Pasifika people, and people living with disabilities.

Q12: Do you have any major concerns about what the biometrics position paper says about OPC's regulatory expectations or how the Privacy Act applies to biometrics?

No comment.

Q13: If you are a user or potential user of biometrics: does the position paper provide enough clarity about what you need to do to comply with the Privacy Act and with OPC's regulatory expectations? If not, where does it fall short?

No comment.

Q14: If users or potential users of biometrics were complying with OPC's regulatory expectations in the position paper, would this provide enough privacy protection? If not, where does the position paper fall short?

Compliance with OPC's regulatory expectations on its own would not provide enough privacy protection for consumers. We consider that OPC and the Human Rights Commission should conduct a joint investigation into the impacts of using biometric technologies and information.

Q15: Do you think current privacy regulation of biometrics is adequate? Why, or why not?

No, we consider the Privacy Act does not have any enforcement provisions that provide sufficient deterrent to agencies handling personal information, including biometric information. Beyond limited ability to issue compliance notices, the current regime relies on individuals to take action. Legislative change is required to strengthen and expand OPC's enforcement and regulatory toolbox to include a wider range of powers. Currently, there are no provisions for OPC to enforce the end of the lifecycle of permitted use of personal information. Additionally, there are no specific provisions where a right to be forgotten can be upheld.

Q16: Are there any other regulatory options not covered in this paper that you think should be considered for biometrics?

No comment.

Q17: If you think more regulatory action is needed, which option(s) would you recommend focusing on?

We support a biometrics code of practice under the Privacy Act, and the introduction of offence provisions in the primary legislation to enhance OPC's regulatory and enforcement powers. In particular, the Privacy Act should be amended to include offence provisions and create the ability for OPC to issue fines and infringement notices. We also support the publication of further guidance from OPC.

Q18: Do you think OPC should develop more guidance on biometrics? If so, on what specific topics?

Yes, we support the topics set out in the Consultation Paper, and consider it would be beneficial for OPC to provide more guidance focused on educating consumers about their rights and agencies about their obligations, with regard to the use of biometric information, and what steps they can and should take to protect biometric information. We would be happy to work with OPC to facilitate this.

Q19: What role do you see for standards and principles for the use of biometrics?

We prefer a code but consider that standards and principles can play an educative and guiding role in ensuring that consumers' biometric information is adequately protected. However, without mandatory requirements and strong enforcement powers, we think that voluntary measures to regulate the use of biometrics would be insufficient.

Q20: What role do you see for direction and expectation-setting from Government for government departments and other public sector agencies? Are there any specific areas in which you think Government direction would be helpful?

We consider that directions and expectations from Government can play a role in setting high standards of good practice and deterring substandard practices. We see value in having Government directions and expectations for public agencies. However, it is ultimately up to the regulator, or alternative independent oversight body to regulate and supervise governmental use of biometric information.

Q21: Do you think OPC should develop and consult on a code of practice for biometrics? If so, what do you think the code should cover – biometric information in general, or particular types or uses of biometric information?

Yes, we support a code of practice for biometrics. It should cover biometric information in general and address particular types and uses of biometric information. This is especially important where biometric information is used in sensitive contexts such as for criminal justice records, crime detection, border security/passport issuing systems, refugee assistance,

financial services, and health care systems. These contexts are often highly sensitive, personal, and some of the time will involve people in vulnerable situations. There is considerable risk that any loss or misuse of biometric information will result in significant harm.

The code of practice should provide guidance on the most appropriate way to inform individuals their biometric information is being collected and used, and why. The code of practice should stipulate the need to delete that information once it has been used for the purpose it was collected. It should also require agencies to assess the proportionality of any risk of harm to individuals and whether the relevant use and type of biometric information is necessary for the purpose stated, or whether alternative, less sensitive information could provide a safer option.

Q22: Do you think there should be any changes to legislation to improve the regulation of biometrics?

Yes, the legislation should be improved by giving OPC a wider range of enforcement and regulatory powers. We think that offence provisions are necessary to ensure that OPC can effectively protect consumers' privacy, as well as regulate and have oversight over the various uses and types of biometric information.

These offence provisions should include criminal offences. Without calling for legislative changes to strengthen protections of consumers' privacy, we consider that there is a heightened risk that biometric information will be misused.

Q23: What would you like any new regulatory measures to cover and what key expectations should they set?

As noted above, any new regulatory measures should cover methods of assessing proportionality against the necessity for the particular collection, use or storage of biometric information. In our view, anyone using biometric information must be able to clearly demonstrate that it's use is not outweighed by the actual or potential harms it could cause. If the objective can be achieved through other means, then biometric information should not be used.

We would like to see expectations similar to the recommended practices set out in the "United Nations Compendium of Recommended Practices

For the Responsible Use and Sharing of Biometrics in Counter Terrorism".[4] The new regulatory measures should set out best practice measures, such as the requirement to:

- Carry out a Privacy Impact Assessment.
- Have training and awareness programmes and procedures in place to increase education on the importance of upholding privacy and human rights when dealing with biometrics.
- Implement encryption or data reduction techniques at the key stages of handling biometric information, such as collection, storage, use and sharing of biometric information.
- Implement rigorous access controls and logging of access.
- Ensure that there are documented processes in place for when a privacy or security breach occurs.
- Carry out regular tests and audits to ensure that security and privacy practices are being followed and remain robust and effective.
- Ensure there is a formal process to document and address issues that become apparent following the tests and audit.
- Ensure that there are regular, random checks conducted on the validity and integrity of the biometric information held in the system.

In an Aotearoa New Zealand context, there should also be a key expectation that any use of biometric information and systems should take into account tikanga Māori and Te Tiriti o Waitangi.

Q24: Do you have anything else you'd like to say about biometrics and privacy?

We recognise there are legitimate uses of biometric information and technologies. In a growing technological and globalised environment, some consumers have become more comfortable and accepting of biometrics technology. However, often they do not give any consideration to, or have any knowledge of, the implications. This stresses the urgency for greater regulation and protection of consumers' biometric information. We support the United Nations' view that 'in order to realise the full potential of biometrics, governments must also address the protection of those who are identified by such systems and ensure that the collection, storage and use of biometric data is conducted in accordance with

[4] United Nations, "United Nations Compendium of Recommended Practices For the Responsible Use and Sharing of Biometrics in Counter Terrorism", June 2018.

international human rights and privacy laws including the International Covenant on Civil and Political Rights (ICCPR) and the UN Universal Declaration of Human Rights (UDHR)'.[5]

Thank you for the opportunity to provide comment.

ENDS

[5] "United Nations Compendium of Recommended Practices For the Responsible Use and Sharing of Biometrics in Counter Terrorism", page 6.