OPEN LETTER TO:

- Hon. David Seymour, Minister for Regulation
- Hon. Judith Collins, Minister for Digitising Government; Minister of Science, Innovation and Technology
- Hon. Paul Goldsmith, Minister of Justice
- Hon. Andrew Bayly, Minister of Commerce and Consumer Affairs
- Hon. David Parker, Chairperson, Regulations Review Committee
- Ben King, Chief Executive, Department of the Prime Minister and Cabinet

6 August 2024

PLEA FOR INTERVENTION WITH THE OFFICE OF THE PRIVACY COMMISSION

The Office of the Privacy Commissioner (OPC) intends to introduce a Code of Practice for biometrics. This would have major unintended consequences harmful to business and the economy, which is why we are urgently seeking your[1] support to prevent this happening.

Through successive rounds of industry consultation on the proposed code, it has become clear to NZTech and our 2500 members from across the New Zealand technology landscape that we are not being listened to, despite the fact we represent the majority of businesses (both large and small) with significant knowledge and experience in using biometrics, as well as government agencies, academia and individual experts, all with a genuine willingness to engage with the OPC to ensure the best outcome for New Zealand, and with track records of working alongside government on many initiatives over the years.

While we recognise the need for continued and detailed good practice guidance to help inform and educate some agents where their implementation and management of biometrics may be falling short, unfortunately we are now faced with a situation where New Zealand is poised to become a global outlier in its biometrics regulations, with adverse consequences for business and individuals. We firmly believe the code would harm business by stifling innovation as well as threatening the privacy of individual New Zealanders rather than protecting it.

That is why we are appealing jointly to you. We ask you to use your influence to put a pause to the work of the OPC so that all parties can re-engage in genuine good faith and achieve a better outcome for the good of the country.

Key Concerns

The code poses a significant risk to innovation in New Zealand. The code starts from a position of complete prohibition with limited exceptions. This starting position of prohibition does not allow for flexibility nor does it signal a country that enables innovation in the use of data.

The current draft code bluntly prohibits practices that are low-risk, beneficial, and necessary for the functioning of modern technologies, often by relying on definitions whose scopes are unclear and overbroad. It also fails to clarify how certain privacy safeguards could be implemented in practice, creating significant compliance uncertainty. By potentially prohibiting low-risk practices in broad brush strokes without providing sufficient exceptions, the code will

stifle the progress of technology developments in the use of data and AI in New Zealand. Compliance with many provisions as written would be difficult, if not impossible.

- **Restricting Artificial Intelligence (AI)**

The code proposes to introduce a prohibition with respect to web scraping of "biometric samples". Given the broad definitions of "behavioural biometric" and "physiological biometric" as incorporated in the definition of "biometric sample," these restrictions may amount to a ban on using photos and videos scraped from the web to train AI models.

Put simply, this restriction would cripple New Zealand's AI industry. Cutting-edge AI models, including generative AI models, are trained on information scraped from the web. Blocking developers from using publicly available New Zealand data would materially restrict the ability of developers in New Zealand and worldwide to train generative AI models using New Zealand data and potentially inhibit the development of AI capabilities in the country. The sheer quantities of data required to train the large language models (LLMs) and neural networks simply would not be available to developers for New Zealand data.

The likely impact would be that LLMs and other products and services produced using contemporary machine learning/AI development techniques would not be readily available and would be cost-prohibitive to develop in New Zealand, or would not reliably reflect the nuances of New Zealand's distinctive culture. A lack of representation of different demographics or linguistic communities in training data could also lead to patterns of bias in data output.

- **Restricting collection of health information**

The code differs dramatically from overseas laws in its prohibition on using biometric classification to collect health information. The common approach around the world is to instead deem health information a kind of sensitive data under comprehensive privacy laws. This often means that its collection is permitted with an individual's consent. But under the OPC's code – which lacks a consent exception – collection of such information would be banned, devastating many sectors of New Zealand's economy. For example, there are many wearable health devices, including sports training devices, that collect health information. New Zealand would no longer be a safe jurisdiction in which to build and sell such devices.

- **Biometric classification**

Crucially, the code should apply only to biometric information used for identification or verification purposes, in line with global biometric laws. However, the OPC's current draft of the code introduces the concept of "biometric classification" and imposes prohibitions in relation to this processing. It is clear that the OPC has adopted similar concepts to the EU AI Act, but the EU legislation prohibits only using data about the body to deduce or infer legally sensitive traits (e.g. race, political opinions, sexual orientation), or to infer emotions in workplaces and educational institutions (unless for medical or safety reasons). Other forms of classification are legitimate and essential activities for any organisation dealing with many people.

This is underscored by the fact that the OPC has defined certain kinds of classification—such as collecting information about someone's "inner state" or "physical state"—so broadly as to encompass many kinds of benign, essential data processing. For example, "inner state" includes an individual's "intention." But nearly any observation of a human's behaviour could be characterised as an observation of their intention. Imagine a data point collected by a vehicle's acceleration system measuring how far down a driver presses the accelerator pedal. That data point would likely be considered a "behavioural biometric" under the draft code, and, because it represents an individual's "intention" to accelerate the car, it would in turn be considered an inference of someone's "inner state." The draft code, as written, would thus prohibit vehicles from using digital acceleration systems. This is just one example, but it shows how the OPC's code's broad prohibitions, combined with its broad definitions, create a wide range of unforeseen and unintended consequences.

- **Different from existing OPC codes**

This code would be unique for the OPC. It has been modelled on existing codes under the Privacy Act which are targeted at specific activities by specific agents in regulated industries. But this code is focused on any activity utilising biometric data or technologies, by anyone. The potential for unintended consequences is incredibly high.

- **Code purports to modify primary legislation**

Elements of the proposed code appear to be inconsistent with the extent of authorities delegated to the OPC under the Privacy Act. The proposed code would arguably modify the most fundamental element of the Privacy Act itself, by deeming certain types of information to be personal information regardless of whether or not that information comprises information about an identifiable individual. For example, biometric templates that are produced using an irreversible one-way hash function that can never be used to identify any individual absent additional information (about a particular individual) would be captured by the code.

- **Code does not respond to actual threats to privacy**

The proposed code is a response to perceived public concerns, rather than a response to any actual analysis of a threat to privacy. Most public concerns are well known, and huge efforts have been made in recent years to address them. These concerns are genuine, but some are no longer valid as the practices have been superseded. At the same time, there are significant, known privacy threats which are not acknowledged or addressed.

Unintended Harmful Consequences

The code's introduction would have major unintended consequences harmful to business and the economy.

A key example is the obstacle to board-level investment decision making. Many of us have already experienced this, as we wait for clarity on the code before even considering investing in solutions that include facial recognition.

The code would place restrictions on the use of virtual reality in the gaming industry. The intended definition and lack of ability to gain customer consent in the current code would severely hamper the development of the burgeoning NZ gaming industry and many NZ "software as a service" (SAAS) tech export business services by prohibiting the collection of behavioural information to provide enhanced tailored experiences. The risk is very real of driving these extremely mobile businesses to other countries such as Australia in order to continue operating many of their services.

In general, innovation gets stifled when risk assessment at the governance level is hard. The code's muddled rules, definitions, and exceptions will make risk assessments too difficult and arguably defeat the purpose of the OPC issuing a code of practice – to provide clarity and certainty to industry and the public. The irony is that biometrics have the potential to preserve anonymity, so impeding investment decisions will prevent businesses from making privacy improvements.

The exceptions necessary to accommodate legitimate and safe uses of biometrics appear to dilute the code to the point that some of the Privacy Act's privacy principles may be less enforceable.

Conclusion

The threat to business and the economy posed by the OPC's proposed Code of Practice is real. We have exhausted opportunities for consultation and have little confidence that the OPC will address our concerns. We therefore urgently seek your support in halting its introduction to allow stakeholders to re-engage in constructive dialogue and work towards a mutually beneficial solution that benefits the country as a whole.

Yours sincerely,

Graeme Muller
Chief Executive
NZTech
E| Graeme.muller@nztech.org.nz
P| +64 21 0252 0767

ABOUT NZTECH

NZTech is a not-for-profit, non-governmental (NGO) membership-funded organisation whose purpose is to help create a safer, more equitable, sustainable and prosperous Aotearoa New Zealand underpinned by good technology. We bring together the NZ Tech Alliance and represent 24 tech associations such as AgriTechNZ, BioTechNZ, FinTechNZ, the AI Forum, the NZ Game Developers Association, Digital Health, Digital Identity NZ and more. Collectively our 2500 members employ more than 10 percent of the workforce. Our members are startups, local tech firms, multinationals, education providers, financial institutions, major corporations, network providers, hi-tech manufacturers and government agencies that work closely with the tech ecosystem.