NEW ZEALAND POLICE
Ngā Pirihimana o Aotearoa

24 February 2021

By email to:

Dear

OFFICIAL INFORMATION REQUEST – OUR REFERENCE: IR-01-20-33757

I refer to your email dated 6 November 2020, requesting a range of information relating to technologies identified in New Zealand Police's *Assurance review of emergent technologies* (July 2020), and our letter of 30 November 2020 notifying you of the need to extend the expected timeframe to respond to your request under the Official Information Act 1982 (OIA).

Having now been able to work systematically through the various aspects of your OIA request, I am now able to provide the following response.

Information in relation to identified technologies

The main body of information sought relates to seven technologies, which you identified as:

1. *Brief Cam*
2. *New X*
3. *Cellebrite*
4. *Drones/RPAS*
5. *ANPR*
6. *Body-worn cameras (BWC)*
7. *Digital Information Management (as per p5 of the stocktake, which refers to ICTSC to run an RFI/RFP)*

In respect of these technologies, you requested the following information:

1. Which police unit(s) or similar, owns/governs the tech and the use of it

2. The name of the company supplying the tech

3. The name of the key software the tech relies on

4. The name of any other company supplying that software in whatever way, eg to police or to the police's supplier above (eg NEC provides software to Dataworks Plus to run ABIS 2)

Police National Headquarters
180 Molesworth Street. PO Box 3017, Wellington 6140, New Zealand.
Telephone: 04 474 9499. Fax: 04 498 7400. www.police.govt.nz

5. The name of any software in this tech that gives this tech any facial recognition capability – whether used by police, or not used (relevance as per stocktake: "Many technological tools that we use (for example, mobility devices) have an in-built facial recognition capability. However, we do not use this functionality")

6. A copy of any RFI, RFP or RFT run under which this tech was procured

7. A copy of any 'requirements document' for the tech procured (or similar, eg like the one for ABIS 2 released to RNZ in August 2020)

8. A copy of any outline of police future strategic requirements similar to that in the ABIS 2 document p52, for the tech

9. The title of any and all legislation and which sections of it, that police refer to with regards to use of the tech in investigation, surveillance and/or search functions

10. Who/which entity will audit the use, data capture, transfer and storage related to the tech, using what internationally accredited audit system if any (pls name this system) and how often; – if not using an internationally accredited audit system, pls specify what audit system WILL be used

11. How data captured by the tech is stored and where

12. Re data storage, specifically whether the data MUST contractually be kept onshore in NZ or if that is not a requirement

You have specifically requested information only in so far as it relates to the investigative, and not administrative, use of the listed technologies. To avoid the term 'investigative' becoming more limiting than you may have intended, I have interpreted your request as being for information related to operational rather than administrative use. This ensures it captures operational uses that may be public-facing but are not necessarily related to investigating an alleged criminal matter, such as (for example) actual or potential use of Remotely Piloted Aircraft Systems (RPAS) for search and rescue or traffic management.

The material contained in the attached table, and appended documents, addresses this part of your request. Note that some material has been withheld in accordance with relevant provisions of the OIA, as noted in the table. Some parts of your request have also been refused on the grounds provided by sections 18(e) and 18(g) of the OIA, on the basis that the information sought either does not exist, or it is not held by Police. The relevant grounds for refusal are noted in the attached table.

Please also note also that the reference to "NewX" in Police's Assurance Review was unfortunately included in error. The correct name of the software platform is "Nuix". The attached table responding to your request uses the correct nomenclature.

Body-worn cameras

You have requested further information in relation to body-worn cameras, as follows:

> *Re BWC, pls provide:*
>
> *1. A copy of the directive given to pause any further work on this (stocktake p5)*
>
> *2. Any and all additional documentation and/or correspondence re this pause*
>
> *3. Any business case for procuring this*

The instruction to pause work on body-worn cameras is understood to have been a verbal instruction. No written directive exists. No further documentation or correspondence in respect of the decision to pause work has been identified. Both of these limbs of your request are therefore refused under section 18(e) of the OIA, on the basis that the information sought does not exist. No formal business case for this technology has been developed, though the Police Executive Meeting paper PEM/13/78 (September 2013) on 'Taser Camera Systems' is referred to as a 'business case' in the subsequent 2014 On Body Camera Proof of Concept proposal (CP00034). Neither proposal was accepted, and no proof of concept trial went ahead. Both documents are attached in response to question 8 of the first part of your request.

By way of context, body-worn cameras have not been the subject of any specific acquisition process or proposal, however they have been considered within the context of the Taser programme as a potential further assurance and evidential adjunct to the existing Taser camera. The documents relating to those considerations have been included in response to question 8 of the first part of your request ("*any outline of police future strategic requirements"*).

The technology has also been the subject of occasional background research associated with monitoring Australasian and global trends in law enforcement. Notably, this included work to establish a specific research project into body-worn cameras, which was initiated in early 2018 and put on hold with only a literature review and early scoping work having been done. While outside the scope of your request, a document containing the Terms of Reference, entitled *Research on Body-Worn Cameras*, has previously been released (subject to redaction of non-executive staff names) and is attached for your background.

Digital Information Management

You requested additional information in relation to Digital Information Management as follows:

> *Re Digital Information Management, pls provide*
>
> *1. Any business case for procuring this tech*

2. Any and all additional documentation and/or correspondence re requiring or potentially requiring facial recognition in this tech (stocktake p5)

No business case for this potential procurement has been developed, as no decision has been made to proceed beyond the Request for Information (RFI). A copy of the RFI has been provided in response to the first part of your request. No documentation or correspondence in respect of requiring or potentially requiring facial recognition in this technology exists. Both questions in this part of your request are therefore refused under section 18(e) of the OIA on the basis that the information sought does not exist.

Again, by way of context, it may be helpful to explain that the Digital Information Management proposal is essentially concerned with the possible acquisition of a platform to manage ever-growing volumes of data securely and cost-effectively, rather than with the acquisition of new investigative data-analysis capabilities. Investigative analysis of data held by Police is functionality that is generally delivered by specialised applications, such as some of those you have asked about in other parts of this request. Those applications currently store and draw their data from a range of Police locations. The Digital Information Management proposal, if adopted, would see the storage and management of digital data held by Police change, for reasons articulated in the RFI. While, hypothetically, a solution could also potentially consolidate some investigative analytical capabilities onto the same data management platform, since that might for example deliver efficiency and data integrity benefits, the project does not seek to introduce new facial recognition capability.

In respect of the comment contained in the Assurance Review to which your request refers, the author of the review and the business group owner of the proposal have confirmed that the comment was intended to convey the fact that data held by Police is currently used by a range of Police applications, including for example non-live 'facial recognition' of suspect images (the ABIS2 Privacy Impact Assessment, which has been publicly released, refers); and that any data management solution that may be acquired in future will likely need to continue to be able to support this functionality.

RPAS/drones

You requested additional information in respect of RPAS/drones as follows:

Re Drones/RPAs, pls provide documentation that evidences:

1. how these drones are used currently for policing

2. any potential future use identified by NZP

3. how data is captured by the drone, how it is transmitted, to where, and how it is stored

4. how police decide/assess where and how to use a drone(s), at what level of NZP

5. controls are over drone use

Firstly, and for the avoidance of doubt, the terms RPAS and drones are used interchangeably throughout this response, and it should not be inferred from the use of one term or the other that the response is caveated. No such caveat applies or is intended.

Questions 2, 3, and 4 above are addressed by the responses to questions 8, 5 and 11, and 10 (respectively) of the main body of your request. I refer you to the attached spreadsheet for those responses. Question 5 above appears to be a numbering error.

In response to question 1 above, New Zealand Police has used RPAS for:

- search and rescue operations, particularly to look in locations that are difficult or dangerous to reach
- civil defence/disaster response
- photography of some serious crash scenes
- arson and crime scene photography
- photography of some accident and sudden death / suicide scenes
- situational awareness during mass gatherings that could pose a risk to Police staff and members of the public
- situational awareness during Armed Offenders Squad and other tactical operations
- cannabis recovery operations
- locating fleeing offenders

In many instances, these uses of RPAS/drones have been in support of other Police aerial operations (for example to supplement or follow up observations made from helicopters or fixed wing aircraft), or as a more cost-effective alternative to traditional aircraft. Some of these uses have been undertaken very infrequently and/or solely on a proof-of-concept basis. The vast majority of deployments are undertaken for arson, crime scene, and crash scene photography; with these uses accounting for more than two-thirds of all operational flights. Situational awareness deployments, which might be described as tactical surveillance or reconnaissance flights in connection with a particular operation, account for less than one in every five flights; with the majority of those being in support of high-risk Armed Offenders Squad or Special Tactics Group operations.

RPAS have not been used for general or routine aerial surveillance or monitoring purposes (for example, they were not used to monitor compliance during the COVID-19 lockdown).

It may also be helpful to note that RPAS/drone use is very infrequent across Police, with most Districts operating about one or fewer RPAS flight per week on average. Given the flight time of RPAS is measured in minutes rather than hours, it is evident that drone operations remain a very small part of New Zealand Police operations – notwithstanding the demonstrably high value of those operations in helping ensure staff and public safety in a range of scenarios.

The document entitled Police Instructions on Remotely Piloted Aircraft Systems (RPAS), provided in response to the first part of your request, also responds to aspects of these additional questions.

ABIS2

In respect of ABIS2, you have requested information as follows:

> *Re the ABIS 2 PIA p 5, pls provide documentation that explains:*
>
> *1. What 'Facial recognition search, compare, match and report ' refers to as in:*
>
> *1. Where would/do the expected 15,000+ images to be recorded come from?*
>
> *2. Who are they the facial images of?*
>
> *3. Do these include facial images of members of the public who are not suspects, and if so who?*

The business group owners of the ABIS2 project advise that no existing documentation provides an explanation in terms approximating those you have requested. However, I am able to offer the following response to provide the information sought.

The estimated 15,000 per annum facial recognition search, compare, match and report instances are expected to comprise the following types of searches:

- Person to Person searches. These are comparisons of images acquired by Police into specific image collections (including Formal Offender, Child Sex Offender, Returning Offender, Missing Persons and Firearms Licencing images) for matches with other images held across Police image collections. These are essentially screening searches undertaken as images are lawfully acquired into these collections, which may assist for example in verifying identities of missing persons, resolving potential duplicate identities, and in firearms licence vetting.
- Suspect category images (estimated 7,500 per year) to Person searches. These are comparisons of images of unknown suspects from a crime scene or incident, which are held on the Unsolved Suspect Database, against images held in the image collections described above. These searches may assist in identifying the unknown suspect.

The facial images are therefore of persons within the categories described above. Except as implied by those categories (for example, missing persons and firearms licensees), it is important to note that the facial images do not include members of the public who are not either offenders, or suspects in relation to a specific crime scene or incident.

Facial image data-sharing

You have also requested:

> *With regard to any of the new tech listed in the stocktake, and regards Police access to sources of facial images, pls provide documentation* that evidences:*

1. the identity of any and all entities with which police have a data-sharing agreement (s) that can include or does include police acquiring any facial image/s from an external source, covering both:

1. public-sector entities both within the core public sector and without, eg NZDF and security agencies

2. private sector entities

**RNZ is not asking for a copy of each individual agreement but rather the likes of an index or list showing all such agreements.*

No existing documentation provides an index or list of data-sharing agreements of the kind requested, or would provide the information requested in respect of facial image acquisition. I therefore respond as follows.

New Zealand Police is able to access identity information (which may include facial images) held by a range of public sector agencies pursuant to the provisions of the Privacy Act 2020 (effective from 1 December 2020). Analogous provisions were in place under the preceding Privacy Act 1993. In summary, the law allows Police to access or obtain for limited, specific purposes as detailed in Schedule 3 of the Privacy Act 2020, identity information held by the agencies listed in the Schedule, in order:

"To verify the identity of a person:

- whose identifying particulars have been taken under section 32 (identifying particulars of person in custody) or 33 (identifying particulars for summons) of the Policing Act 2008
- whose identifying particulars have been taken under section 11 of the Returning Offenders (Management and Information) Act 2015
- who has breached, has attempted to breach, or is preparing to breach a condition of any sentence, or order imposed under any enactment, that the person not leave New Zealand."

Police may also access (i.e. view) a particular person's driver's licence image in accordance with the provisions of s200(4) of the Land Transport Act 1998, which states:

"A person who is acting in the course of the person's official duties as an employee of a specified agency may access or use any photographic image stored under section 28(5) to verify the identity of a particular individual for the purpose of law enforcement."

Consistent with the statutory framework (and notably s166 of the Privacy Act 2020) Police also has memoranda of understanding (MOUs) or Approved Information Sharing Agreements (AISAs) with Department of Internal Affairs, Waka Kotahi New Zealand Transport Agency (NZTA), Corrections, Customs, and Ministry of Business, Innovation and Enterprise (Immigration) to detail the process and manner in which the agencies will interact within the legal regulatory framework. There is also an agreement between Police, Customs, and the Ministry of Health in respect of special patients, to facilitate exchange of

information (including identity information) for the purposes of generating and enforcing Border Alerts. Internationally, there is an MOU between NZ Police, Australian police agencies, and CrimTrac (now the Australian Criminal Intelligence Commission) governing access to images of long-term missing persons and unidentified victims or remains.

It is important to be clear that neither the legal regulatory framework nor the MOUs/AISAs allow for Police to be provided with other agencies' facial image or identity information datasets. Rather, they enable Police to use identifying information as provided to or lawfully gathered by Police (such as name, gender, date of birth, and driver's licence or passport number), in respect of a particular individual, to query other agencies' identity data to verify that information for lawful purposes: including, potentially, visual verification against images held by those agencies. Police does not retain driver's licence images. They are accessed to enable identity verification on an as-needed basis. Similarly, images provided by DIA are used to update or verify identity only.

Other provisions of the Privacy Act 2020 which enable information sharing for specific purposes, such as the exceptions contained in Information Privacy Principles 10 and 11, may also provide a basis for Police acquisition of images of a particular person, in respect of a specific matter, where lawfully justified on a case by case basis. Some of these arrangements are formally contemplated by policy arrangements but not specific data-sharing agreements, such as the policy which regulates the provision by Oranga Tamariki of a photograph (if available) of a child or young person under care as part of a Missing Person Report made to Police in the prescribed form. Individual images which may be provided by another agency to Police in respect of a specific matter can only be used and retained for the purposes for which they were provided, as required by the Privacy Act 2020.

You have asked specifically about data sharing agreements with the New Zealand Defence Force (NZDF) and security agencies which includes or could include the acquisition by Police of facial images. Police has an overarching MOU with NZDF which governs the general provision of operational and logistical support in accordance with the Defence Act 1990 and other relevant legislation. This is not a data sharing agreement and does not contemplate the provision of facial images.

Similarly, while Police works with the New Zealand security agencies as part of a wider National Security System (as described in the Auditor-General's 2016 report on *Governance of the National Security System*), no data sharing agreements exist between Police and New Zealand security agencies.

With respect to private sector entities, complainants alleging a crime has been committed regularly provide suspect images to Police. These images may for example be stills or CCTV footage captured at an alleged crime scene. Images received in this way are treated as Unsolved Suspect images and stills may be subject to image matching queries against Police image collections, as described above in response to your questions about ABIS2. These unsolicited images may also be retained by Police for their evidential value when investigating the particular alleged crime.

Complainants providing suspect images may be private citizens or companies (or, indeed, public entities if an alleged offence has been committed for example on their premises). Images may also be sought by Police, where investigation of a specific matter gives investigators reason to believe a CCTV owner or operator may have captured images that might assist the investigation. In most cases the images are provided directly by the complainant or CCTV owner and are not governed by any specific data sharing agreement.

Nevertheless, some of the relationships within which Police may be provided with or given access to CCTV-derived suspect images are the subject of specific agreements. These include agreements with the Financial Services Federation, New Zealand Bankers' Association, Retail New Zealand, Waka Kotahi NZ Transport Agency, and various local council authorities and/or their council-controlled organisations, and various community or business organisations (for example in relation to crime prevention camera monitoring arrangements).

Police also has an agreement with Auror, which is a commercial retail crime prevention platform, via which third party retailers may lodge for example theft complaints and may provide suspect images. The Auror platform acts effectively as an online complaint portal, however, like other channels for provision of suspect images, this does not alter Police's obligations in respect of criminal complaints and the treatment of any associated suspect images received via or viewed in the portal.

Once again, it is important to be clear that these agreements relate to general working arrangements for relationships within which Police might, from time to time, be provided with or seek imagery in relation to the investigation of a specific matter. They are not agreements "for" provision of facial images and do not contemplate or facilitate sharing of databases or facial image datasets.

No other private sector agreements have been able to be identified that give or could give Police access to facial images.

General comment

In response to your general invitation to provide information regarding how public privacy and security risks have been addressed, as you note in your request, technology acquisitions and proposals are subject to requirements for governance approvals and compliance with procurement processes as appropriate to the nature and scale of the project. These processes by their nature routinely canvas legal, policy, privacy, and security issues and may lead to more formal Privacy Impact Assessments and/or Security Risk Assessments where materially significant considerations are identified as being engaged.

The July 2020 Assurance Review's findings and recommendations nevertheless reflect that more can be done to systematise internal oversight and external stakeholder engagement on privacy and related issues, particularly in respect of new and emergent technology.

As you are aware, New Zealand Police has recently introduced a new policy which governs proposals to test or trial new technologies, and has also signed up to the *Algorithm Charter for Aotearoa New Zealand*. Further, Police has committed to establishing an independent expert panel to review new technology

proposals and the process of establishing the panel is underway. These are significant steps towards improving our ability to provide public transparency and assurance that privacy and security concerns are identified, fully considered, and appropriately weighed before a decision is made on whether or not to introduce a new or emergent technology.

In closing, I trust the information provided meets your needs. However, if you are dissatisfied with this response, you may ask the Office of the Ombudsman to investigate and review Police's handling of your request.

Finally, please note that, consistent with Public Service Commission guidance on proactive release of OIA responses which carry a degree of public interest [https://www.publicservice.govt.nz/assets/ Legacy/resources/oia-proactive-release-dec2017.pdf], we shortly intend to publish this letter (with your personal details removed) on Police's website.

Respectfully

Mike Webb
Director: Assurance