NEW ZEALAND
POLICE
Ngā Pirihimana o Aotearoa

4 November 2020

Andrew Chen
By email to: fyi-request-13714-63893316@requests.fyi.org.nz

Dear Dr Chen

OFFICIAL INFORMATION REQUEST – OUR REFERENCE: IR-01-20-26373

A quick follow-up to our earlier correspondence, to make good on the commitment regarding proactive release of the point-in-time stocktake report from July 2020.

In the interests of openness and transparency, please find a full copy of the report attached. By way of additional context, you will see that the stocktake identified (as at midyear) close to 20 examples of emergent technologies that have either been tested, trialled or rolled out. These include core capabilities that support the important crime prevention and law enforcement work New Zealand Police does, such as in the area of detecting and countering child abuse material; or assisting with the investigation of offences, such as making use of lawfully-accessed CCTV footage or the data seized from suspected offenders' mobile phones or computers. Only a sub-set of these tech capabilities are what would be called public facing; most of them are in-house tools which are used by specially-trained Police staff. And, in many cases, they simply speed up or help with initial triaging of what have, in the past, been manual and highly labour-intensive tasks. In all cases, the use of such technologies is consistent with lawful policing purposes under legislation.

We are also making available a copy of the Privacy Impact Assessment (PIA) that was recently completed on the use of the IMS Photo Manager application, which supports some of the work of our specialist National Biometric Information Office. In line with our recently strengthened policy (www.police.govt.nz/sites/default/files/publications/proposals-to-test-or-trial-use-of-emergent-technologies.pdf), the PIA and its recommendations was recently reviewed and approved by Police's Security and Privacy Reference Group, followed by an executive-level governance group.

In closing, thanks again for your patience in receiving details of the July 2020 report, as we worked through the first 'deep dive' of privacy implications associated with emergent technologies that New Zealand Police is engaging with, using the enhanced governance and oversight arrangements that were recently agreed.

Respectfully

Mike Webb
Director: Assurance

July 2020

Assurance Group

NEW ZEALAND POLICE
Ngā Pirihimana o Aotearoa

Assurance review of emergent technologies

Prepared by: Principal Advisor: Privacy, Assurance Group, PNHQ

PURPOSE

This assurance review has a dual purpose:

- to assess the extent of New Zealand Police's involvement in trials making use of emergent technologies - including, but not limited to, artificial intelligence (AI) and surveillance technologies; and
- to identify opportunities for how to most safely position New Zealand Police around emergent technologies in the future.

BACKGROUND AND SCOPE

In May 2020, the Commissioner of Police requested that a targeted assurance review be undertaken to better understand the extent of Police engagement with what are known as emergent technologies. This is a term generally used to describe 'new tech', but may also refer to ongoing development of an existing technology. Emerging digital technologies, in particular, can generate opportunities; but can also raise ethical issues, particularly related to privacy interests.

The review was sparked by concerns raised by the Police Executive and other stakeholders about Police's engagement with Clearview AI (a facial recognition software firm based out of the United States), and the process Police followed prior to that engagement.

Questions about the potential investigative applications of emergent technology, such as Clearview AI, in turn prompted consideration of what other technology is currently being piloted (or being proposed) elsewhere in Police. For instance, the Service Delivery Group's Digital Person ('Ella') and Virtual Access Portal (a.k.a. 'Police Connect') prototype trials have both incorporated AI; and AI helps with the operation of the NIA User Manual, 105 Online Form, and Police's public-facing Internet site. Automated Identity Matching is also used to a limited extent in the work of the Police Vetting Service.

Covert surveillance regulated by the Search and Surveillance Act 2012 was out of scope for the review. In addition, given the imperative to bring the results of the review back for the Executive's consideration as swiftly as possible, the review's scope was confined to relevant work groups; including National Operations, the Service Delivery Group, and other relevant business units such as the Legal Service Centre (LSC) and the Evidence-Based Policing Centre (EBPC).

A copy of the formal *Terms of Reference* for the review are attached.

OBJECTIVES AND APPROACH

The assurance review has three main objectives:

- complete a stock take of what trials of emergent technology are currently being undertaken by New Zealand Police
- assess the ethical and privacy implications of such trials
- provide assurance that such implications have been appropriately flagged to key stakeholders, such as the Privacy Commissioner and Independent Police Conduct Authority.

In order to advance these objectives, the reviewers first consulted National Operations to establish the context for the Clearview AI trial, and any other relevant technologies; then similarly consulted Service Delivery Group on current and future options for developing Police's AI capability, particularly vis-à-vis digital services. Inquiries were also made with other relevant areas, such as the LSC and EBPC. The second phase of the review involved assessing Police's trials of emergent technology against the Government Chief Data Steward's and the Privacy Commissioner's *Principles for safe and effective use of data and analytics* (2018). Finally, the review looked at both domestic and overseas models for how to approach trials of emergent technology.

KEY FINDINGS

- Compared to counterpart law enforcement agencies, New Zealand Police currently makes limited use of 'new tech'. Even so, the review identified close to 20 examples of emergent technologies which have been either tested, trialed or rolled out. With an eye to the future, other technologies are under various stages of consideration.
- Use of Clearview AI software was a relatively short test, which was approved by an internal governance group, albeit not at Executive level.
- Opportunities have been missed to inform or consult some stakeholders before certain trials of 'new tech'.

CONCLUSIONS

- Against a backdrop where the use of AI and other 'new tech' has become commonplace in other fields, New Zealand Police's use of emergent technologies has been reasonably conservative and carefully thought-through.
- To varying degrees, privacy, legal and ethical implications appear to have been considered before such technologies are deployed, although there is room for improvement in consistently sharing this knowledge with stakeholders.

RECOMMENDATIONS

- Consider centralising the governance of emergent technologies, to provide strengthened oversight and better ensure consistent stakeholder engagement.
- Consider new policy guidance specifically on emergent technologies, that draws on domestic and international best practice for the safe and responsible use of data, and sets out a standard process for business groups to submit a proposal for pre-approval to the recommended new central governance group.
- Consider commissioning a more comprehensive 'deep dive' into ethical and privacy implications of technologies which have already been rolled out within Police.

1. Stock take of piloted and/or rolled out use of emergent technologies

The stock take established that Police has either tested, trialed or rolled out the following emergent technologies:

Clearview AI

- Clearview AI is software that compares a photograph of a facial image for matches in the company's database.
- A short non-operational test of Clearview AI was conducted in February-March 2020. This was confined to a free trial of a small number of licences to test the viability of the product (i.e., its accuracy in recognising faces).
- Both LSC and the Assurance Group's privacy team were consulted. Advice was provided that if the test proved viable, and if the software was to be considered for ongoing (i.e. non-test) use, then a Privacy Impact Assessment (PIA) and a formal legal review would be necessary – before the software was deployed as an investigative tool.
- The team responsible for the test briefed the relevant operational governance group, which supported the test.
- The tests uploaded photos of the faces of Police volunteers and the faces of a small number of persons of interest wanted by Police.
- It is current Police practice to disclose to media the photographic images of faces of persons of interest.
- In total, 133 searches were completed using photos of the faces of Police volunteers and other available images.
- Another 49 searches were made by three users across Wellington and the upper North Island, using real case data, from 20 February 2020. The last search was on 19 March 2020. No positive results were noted by the users.
- No licenses of Clearview AI were subsequently purchased or deployed operationally.

Darknet website scraper

- A set of python scripts/utilities, written by a Police technical investigator, used to programmatically scrape Darknet sites.
- A PIA was not considered necessary, as the information that is obtained using this program is readily available to anyone with an Internet connection. The program simply automates the day-to-day Darknet analysis by Police operators – work that would be done manually, should this automated process not exist.
- No formal business approval was sought or received prior to first use, and there was also no on-boarding process.

Child Protection System (CPS)

- Program that searches peer-to-peer networks for people who are offering to supply child exploitation material. It searches based on hash sets and keywords of the files that are being offered.
- Police staff were trained in the use of CPS by Australian law enforcement in 2011. A Police member received further training in the USA in 2015.
- It is unclear whether first use of CPS was supported by any prior business approval. Advice was sought from LSC. In short, the advice was that no information is obtained from suspects that isn't already publicly available online.

Auror: Child Abuse

- A program used to analyse images to categorise them as child abuse material.
- Matches hash values and metadata and compares them with known images.

Griffeye

- A program used to analyse images to identify them as child abuse material. This is done by matching hash values and metadata, and comparing them with known images.
- Police has been using this software for 7–8 years. Other New Zealand law enforcement agencies involved in investigating child abuse also use it, and it is the most common tool used by law enforcement worldwide to categorise images. A trainer came to New Zealand to train Police staff before its implementation.
- A full PIA was not considered applicable, as the information obtained using this program compares images already held of child abuse and compares them to other images, based on similarities and hash values.

Brief Cam

- Used to analyse CCTV footage acquired by Police to establish the presence of a known face or a car movement.
- Approved for use by the Investigations Governance Group on 20 February 2020.
- It is estimated that use will cut the time Police staff spend analysing evidential CCTV footage. For example, the time it takes to analyse three months' worth of CCTV footage will likely reduce from six weeks to two hours.

NewX

- Searches unstructured data and platforms for faces, guns, and body markings (tattoos).
- Already in use. Forensic and Asset Recovery Unit staff use NewX to search evidential clones of computers.

Cellebrite

- Analytics enterprise tool which searches lawfully-seized cellphones for data.
- Includes a facial recognition capability that Police has not made use of.

Automated Biometric Information Survey (ABIS)

- Project has been ongoing for a number of years and, once commissioned, ABIS will have an upgraded algorithm to provide better facial recognition.
- Deployment is planned by September 2020. By Q1/Q2 of 2021, ABIS will also be able to provide search capability across scars, marks and tattoos; enabling searches of our images database for matches with evidential images.
- The tool is managed by the Forensic Group and isn't available to Police staff in general, except by formal request.
- A formal business case for ABIS was signed off, recognising that National Criminal Investigations Group (NCIG) is ABIS's business owner. A PIA and security certification and accreditation (C&A) are ongoing considerations.

Automatic Number Plate Recognition (ANPR)

- Deployed by several Districts/Areas (Tāmaki Makaurau, BoP, Taupō, Putaruru) to assist enforcement initiatives.
- Currently managed out of Tāmaki Makaurau using a convergent server supplied by an external provider, which enables ANPR to be acquired by Police for locating vehicles of interest.
- The project is developing policy, defining/accommodating privacy and other risks, and considering governance.
- Current deployment in Tāmaki Makaurau is managed at Inspector-level in the District Command Centre (DCC) where the designated senior officer is responsible for security of the system and responding to requests for ANPR information sought for investigations of serious offending.
- At present, the system is predominantly used for detecting vehicles of interest, but where a valid and authorised request is made to the system manager for information that will support the investigation of a serious crime, information may be released to the investigation team.
- Auror is an independent provider of CCTV and ANPR platforms for the private sector, including fuel stations and other retail outlets.
- In the case of fuel stations, the retailer has access to the Auror system; and if an offender returns to a station, the ANPR system will alert the retailer who can then shut off the fuel pump. Police can then be notified by email.
- The business owner for ANPR is the National Prevention Centre.

RPAS

- Use of remotely-piloted aircraft systems (a.k.a. 'drones') was endorsed by the Police Executive on 12 June 2019.

Axon Citizen (Evidence.com)

- This system is currently used by Police to store evidentiary video interviews acquired from family harm victims. It is also used to store video footage generated after activations during the deployment of TASERs by our officers.
- Communication Centres can use Axon to store images or videos provided by members of the public for evidential purposes. The images are saved through a URL link that is sent to the caller. This was trialled at Central Comms and is likely to be rolled out nationally in the near future. There is no AI or facial recognition capability.
- The product was proposed for use by the supplier at no extra cost to Police and is a simple way to receive and store digital photographic evidence from a witness to an incident.
- The business owner for Axon is the Communications National Management Group.

MobileLocate

- MobileLocate is used by Land and Marine SAR to locate missing people (who wish to be found).
- Police uses MobileLocate to find the location of a cellphone of someone who has rung in to say that they're lost. We send the person a text, asking the lost person to reply (the reply will contain the GPS location of the device).
- If mobile locate is turned off, the person is sent another email that activates mobile locate. Police is then sent the location information needed to pin-point the missing individual.
- The business owner for MobileLocate is the Communications National Management Group.

Device Location Information (DLI)

- This is an enhancement to the MBIE-owned product ECLI (Emergency Caller Location Information).
- The ECLI Service enables call takers from a range of emergency services (including Police) to receive automatically generated geographical information about the likely location of a caller when a 111 call is made from a mobile device on a cellular network. ECLI extracts real time location information on demand at regular intervals from a person's mobile device if it is connected to the cellular network – whether or not they've called 111. To this extent, it's intrusive and can be operated without the knowledge of the person being enquired after.
- The system has been scrutinised by the Privacy Commissioner, who publicly consulted and issued an amendment to the Telecommunications Information Privacy Code (TIPC) to allow use of this service for restricted purposes, where it is required to prevent or lessen a serious threat to the life or health of an individual.
- The business owner for DLI and the ECLI Service is the Communications National Management Group.

Online Forms

- AI used on the Police 105 Form website (for non-emergency reports) to help prioritise jobs.
- The AI scans the 105 Form for key words and assigns a priority. This fast tracks priority jobs to Comms for action.
- Rollout followed an appropriate internal governance process, including privacy and security risk considerations.

Natural Language Processing

- AI deployed as a training aid to look for common themes used by Police staff when searching a system manual.
- This application is no longer used, though the ongoing value of this kind of software is still being examined.
- Rollout followed an appropriate internal governance process, including privacy and security risk considerations.

Front counter person tracking and counting

- Deployed in Christchurch's Justice and Emergency Services Precinct, Te Omeka, to gain an accurate picture of Police public counter demand and requirements in the CBD, and across the Christchurch Metro Area stations.
- Information is collected to improve service delivery at the public counter. The service uses cameras to assess the volume of people visiting a station, when people visit, and the length of time people spend at the counter. The technology is sensitive enough to detect when one staff member is faced with 10 customers, as well as when four staff members are faced with just one customer.
- Rollout followed internal governance and TEB decision-making processes, including consideration of privacy and security risks.

Digital Human

- An Electronic Life-Like Assistant ("Ella"), powered by conversational machine-learning AI, was stationed in the lobby of PNHQ for a three-month trial, from February to April 2020. Ella assisted the concierge team and talked to visitors about Police services. Users could ask for information, or be connected to whoever they were visiting.
- Rollout followed an internal governance process, which included consideration of both privacy and security risks.
- Police extended an invitation to see a demonstration of the capability to the Office of the Ombudsman and the Office of the Privacy Commissioner.

2. Emergent technologies being considered for piloting and/or potential use

In addition, the stock take found Police staff considering the following potential uses of emergent technologies:

Hubstream

- Software which takes overseas referrals relating to child exploitation material and completes checks on any phone numbers, IP addresses, user names, and emails for referrals that have already been seen, based on already-held data. Police is one of three agencies which is considering seeking permission to use this software for a proof of concept trial.

NewCops website

- Although not currently considered viable, some discussions have occurred in the People and Capability Group about the use of chatbots for the NewCops recruitment website, as a way to help answer site visitors' questions.

Other potential 'new tech' applications which were mentioned during the review as being under consideration

- ANPR feed directly into CAD where, for example, a number plate matching a stolen vehicle would present an alert, which CommCens would currently manually create a CAD event for, but AI could create automatically.
- Displaying CCTV feed by camera location as an icon on a CAD map, that when clicked would display a pop-up window (web browser) displaying either a direct video feed or the last still photo taken. Current functionality has NZTA Traffic Operations Centre camera feeds coming in to the Centres along with some other CCTV feeds. A number of these feeds are provided through external provider SecuroGroup and Auror.
- CommCens' use of chat bots for call management for some less urgent situations.
- Communications National Management Group and the Service Group are looking at options to allow community patrols to interact with CommCens in the automated logging-on and logging-off procedures, which are currently manual and require a phone call.
- Aspect and MyPolice – We are currently unable to connect these two systems so that they 'talk' to one another, creating interest in an e-solution to run a disparity report between MyPolice and Aspect which can be acted on (i.e. shifts do not match or leave records do not match). This would better ensure staff are getting their correct entitlements, reduce the risk of employment disputes, and should reduce overall leave liabilities as all leave taken will be followed up for recording in My Police. This could also do the work using desktop automation to actually update MyPolice with changes in schedules, and starting times made by the Workforce Team in Aspect, so there is no need for double-keying.
- Part of our EBPC performance reporting regime will look to use some sort of process automation in the future.
- Towed Vehicles/Keys taken – Comms are looking to put a system in place where people can query a database to see if their car has been towed - and if so, where to – as well as finding out where their keys are, if they have been taken. This may use either a chat bot or some form of automation.
- Body-Worn Cameras (BWCs). Response and Operations Group have been looking at BWC technology for some time and are keen to run a proof of concept, but a directive was given to pause any further work on this idea.
- Digital Information Management. ICTSC has indicated it will be running an RFI/RFP to look at systems that will store both evidential information and CCTV, social media and photographs. It is likely the tenders will list AI and potentially facial recognition as part of the requirements.

3. Assessment

New Zealand Police's use of emergent technologies is fairly limited compared with overseas police agencies. Such technologies are basically used to detect and investigate crime, or to assist with communications and road policing.

Of note, we use 'new tech' to search the large amounts of unstructured data we capture when we seize computers from suspected child exploitation offenders. The main purpose of these kinds of searches is to establish if a computer holds photographic images. Use of AI reduces the sheer volume of data our people would have to sift through, and saves considerable investigative time.

We also use these technologies to aid major investigations, for example we would use search software to filter masses of historic CCTV footage for relevant evidence. This saves police investigations considerable time, reduces investigator fatigue and aids accuracy. Searches that once took six weeks can now be done in two hours; freeing up detectives to spend more time considering the accuracy of information they are evaluating as potential evidence.

Many technological tools that we use (for example, mobility devices) have an in-built facial recognition capability. However, we do not use this functionality.

We also use emergent technologies to assist with communications functions: essentially to populate data collected by one process into another system, such as to prioritise the relative importance of 105 non-emergency forms, and to detect vehicle number plates linked to traffic offending and serious crime.

While Automated Identity Matching is used to a limited extent in the work of the Police Vetting Service, we do not generally substitute machines and algorithms for human decision-making. Likewise, while New Zealand Police does use the YORST algorithm, as a 2019 Law Foundation and University of Otago report into *Government Use of Artificial Intelligence* noted, YORST can only be considered an algorithm "in a weak sense of the term". Unlike police agencies in the United States (and United Kingdom, in a limited way) New Zealand Police does not use algorithms to predict patterns of emerging and reoccurring crime at the community level. Rather, Police sets the parameters of searches and police officers review data which are selected for relevance, accuracy and evidential sufficiency. And our use of these technologies as part of investigations is regularly reviewed by the Courts and subject to judicial oversight.

4. Ethical and privacy framework

The ethics and privacy implications of Police's use of emergent technologies are subject to the overarching requirements of necessity and proportionality. Necessity boils down to the legal framework that sets out the purposes of an agency. To meet our legal obligations we are obliged to make sure that we collect information related to our purposes, and no more. The lawful functions of Police include keeping the peace, maintaining public safety, law enforcement and crime prevention. In addition, the enabling provisions of the Privacy Act 2020 give Police the authority to collect personal information for a lawful purpose connected with our functions and activities.

The Privacy Act enables Police to collect personal information directly from the individual concerned, unless our responsibility to maintain the law provides reasonable grounds to make non-compliance necessary. There will be times when we will need to collect information covertly, or not directly from an individual to carry out our functions. In addition to our legal framework, the Government Chief Data Steward and Privacy Commissioner have published *Principles for the Safe and Effective Use of Data and Analytics*. The *Principles* provide agencies with high level guidance on the collection and use of data. The *Principles* emphasise that data and analytics should be used to deliver a clear public benefit, be fit for purpose, focused on people, transparent, and maintain human oversight. The inherent limitations of such an approach need to be understood.

Our processes for evaluating the use of data are both grounded in law and are broadly consistent with the *Principles*. We have developed internal guidance around personal information. Our approach relies on Privacy by Design (PbD), which mandates a risk and legal assessment of proposed projects for privacy and human rights implications. PbD is formally written into the *Police Manual*, and reflects the 'three lines of defence' model recommended by both the Office of the Auditor-General and Government Chief Privacy Officer's Privacy Maturity Framework. Proposed projects typically benefit from specialist privacy advice, a Privacy Analysis and/or a full Privacy Impact Assessment. As a project matures, it will be supported by increasing levels of advice, analysis and assessment. Legal review is also considered case-by-case and traverses the legal, privacy and human rights implications of a proposed project.

5. Stakeholder engagement

Police consults with the Office of the Privacy Commissioner (OPC) when it considers there are valid issues for concern for the Privacy Commissioner and the public. Prior consultation examples include the gun buy-back scheme and Device Location Information (resulting in amendments to the Telecommunications Information Privacy Code). We worked closely with OPC, and the IPCA, when Police Vetting Service operations were reviewed. In addition, we consulted on: the Child Sex Offender Register; Other Countries' Nationals (a collaboration with MBIE to share information about deportees leaving and returning to New Zealand); the review of the Privacy Act; an AISA on name change, death and information sharing (including the Operating Procedures and Reporting Notice); the automated business process between TradeMe and Police to confirm any auction of firearms involves registered individuals; and deployment of an All of Government (AoG) dashboard to assist with geographic location of Covid-19 infections.

The Privacy Commissioner and Commissioner of Police entered into an MoU for consultation on agency-to-agency agreements pursuant to section 95D of the Policing Amendment Act 2015, which includes an understanding of the obligations on both parties during consultations.

Beyond section 95D, consultation with the Privacy Commissioner is done at the discretion of Police, consistent with the need under section 16(2) of the Policing Act for the Commissioner of Police to act independently on operational matters. Even so, both policy and practice encourages Police to consult regularly with OPC, and we do so often. There will be times when Police's deployment of a technology to gain a law enforcement advantage will see the project subject solely to internal checks and balances. These internal checks and balances include Executive review, as well as scrutiny from LSC and specialist privacy and security assessments led by teams in the Assurance Group. We also consult extensively with the Police Association and the IPCA on any technology deployments involving the collection of information about our own staff. And, as noted earlier, we typically consult with or proactively brief the Privacy Commissioner on relevant developments, especially on issues of wider public interest.

Despite this context, the surprise created when details emerged of the short-lived testing of Clearview AI software indicates that opportunities can still be missed to inform or consult stakeholders before certain technology is trialed. While the Clearview AI example would appear to be 'the exception that proves the rule', it still offers valuable lessons.

6. Discussion

New Zealand Police has deployed a range of technologies over the years to assist legitimate law enforcement goals, and keep pace with the enthusiastic adoption of 'new tech' by criminal elements. For example, we have replaced our labour intensive fingerprint card index with digital searching. Digital technology is now integral to the Police communications network, and is more secure than analogue radio. Word processors have replaced type writers, and biometric databases store and have the capability to search for matches of fingerprints and photographs using digital technologies. Digital case files are increasingly replacing paper-based records, and much of the day-to-day work of frontline officers is now done using small mobility devices. Capturing photographic images in the form of cell phone cameras or CCTV footage is now the norm, replacing the use of the hand held 'box' cameras of the past.

At times, the rollout of a new technology will be accompanied by public questioning on ethical and privacy grounds. In New Zealand, concerns expressed about Police's use of emergent technologies have focussed on issues raised overseas around use of facial recognition in public settings, and use of algorithms for so-called "predictive policing". We have done neither. We have not used algorithms to profile communities for crime and we have not deployed facial recognition in public places. Our deployment of ANPR has not gone beyond a trial, and Police use of CCTV is limited in scale. Moreover, both projects were reviewed by LSC and formal PIAs were completed in a timely manner.

7. Opportunities to more safely position Police

Before concluding this review, the opportunity was taken to look at both domestic and overseas models for how to approach trials of 'new tech', with a view to identifying opportunities for most safely positioning New Zealand Police around emergent technologies in the future.

Domestic models for how to approach emergent technologies

The Government Chief Data Steward and Privacy Commissioner have developed *Principles for the safe and effective use of data and analytics*, while Statistics New Zealand have proposed an *Algorithm Charter for Aotearoa New Zealand*. The *Principles* and *Charter* provide state sector agencies with high-level guidance on the responsible and safe use of data. Both the *Principles* and *Charter* highlight the importance of governance oversight and the need to give staff clear guidance around data use.

The *Principles* remind agencies that any new use of data must have a solid foundation in law; the views of relevant stakeholders should be considered; and data products should be bias free. "Guidance, oversight, and transparency are essential to fostering trust, confidence, and integrity around the use of data the government holds on behalf of New Zealanders", the *Principles* make clear. "It's important for Kiwis to understand how their personal data is used."

The Government Chief Data Steward has also established a Data Ethics Advisory Group to help agencies make the most of the opportunities and benefits presented by the new and emerging uses of data, and to assist the responsible management of potential risks and harms. This group of independent experts encourages the innovative and ethical use of data and provides advice to agencies on how to seize data opportunities appropriately.

Broadly speaking, New Zealand Police's legal and privacy guidance is consistent with the *Principles* and the *Charter*. There is no evidence that our testing, trials and use of emergent technologies has been inconsistent with either the *Principles* or the *Charter,* and our operational groups take care to consider ethical and privacy related implications, make use of our PbD and legal review processes, and refer new projects to relevant governance groups within their reporting lines.

That said, we would benefit from taking advantage of the expertise of the Data Ethics Advisory Group when considering the operational deployment of emergent technology, or when we propose to change the way we use an existing technology. Using the Data Ethics Advisory Group as a sounding board would allow us to put our thinking before a panel of some of the best experts to get advice on ways to safety deploy technology. The experience of London's Metropolitan Police Service (MPS) suggests engagement with a panel of this kind could be valuable. In addition working with this Group would enable us to draw on expertise to work through the implications of international best practice, such as the work of the OECD on AI ethics and the Australian government's AI ethics framework.

The *Principles* also emphasise the need for transparency, as openness helps foster public trust and the confidence that government agencies will use and hold data on behalf of all New Zealanders. We could consider being more transparent around our uses of 'new tech' to fight crime, and this may potentially help dispel some misconceptions.

During the course of this review, operational staff identified the value of modernising our governance processes around emergent technology. We could benefit from enhancing our internal governance of any 'new tech' proposals to better balance operational considerations with privacy, legal, human rights and ethical considerations. Centralising governance around 'new tech' would provide a clearer path for operational groups to follow when seeking approval to deploy an emergent technology, support strengthened oversight, and create a mechanism to encourage greater consistency around approaches to stakeholder engagement.

Overseas models for how to approach proposed trials of emergent technologies

Emergent technologies, when used responsibly, offer significant advantages. CCTV and ANPR, if widely deployed and integrated, offer the potential for law enforcement to significantly improve detection and prevention. The use of these technologies has, for example, enabled London's Metropolitan Police Service (MPS) to significantly reduce vehicle theft, car pursuits, burglary and serious violent crime taking place in public spaces. To take another example, South Wales Police (SWP) have deployed automated facial recognition (AFR) at major public events to detect persons of interest. The deployment of facial recognition technology by SWP was examined by the High Court in May 2019, with the Court finding that SWP's limited use of AFR was consistent with relevant human rights and data protection laws.

The experiences of the MPS and SWP serves to demonstrate that these kinds of emergent technologies can be used safely and responsibly in a policing context. These deployments also provide us with insights that we could examine as we look to strengthen our safe and responsible use of emergent technologies. For instance, the UK has a specific Surveillance Camera Code which offers police a framework of transparent guidance and the social license to deploy 'new tech'. [The principles of the UK Surveillance Camera Code are reproduced at Annex B.] Similarly, inspiration could be taken from specific guidelines developed by SWP to help its officers weigh up whether to make use of AFR: "It is important to ensure that a balance is maintained between transparency and engagement whilst not unduly impacting on the effectiveness of the deployment", the guidelines state. "This balance is achieved via a risk-based approach, at times it may be appropriate to advertise a deployment so that individuals of concern are deterred from attending. At other times it may be more appropriate to encourage attendance by not disclosing deployment specifics so that an individual is more likely to attend and be detained."

Also of note, the Mayor of London has established an independent Ethics Panel, and the Panel's assessment of the MPS' use of live facial recognition software has come up with a set of overarching rules that could be usefully considered here as we grapple with emergent technologies (even though we do not use AFR). The Panel recommends police only deploy emergent technologies like AI when the overall benefits to public safety are great enough to outweigh any potential public distrust in the technology; assess and authorise each deployment to ensure that it is both necessary and proportionate for a specific policing purpose; and train operators to understand the risks associated with emergent technologies and to understand that they are accountable.

Finally, the MPS publishes information about its use of public facing technologies on the MPS website, and use this information platform to help educate the public about what relevant software (like AFR) is attempting to achieve. This model chimes with the *Principles for the safe and effective use of data and analytics*, highlighted earlier, which emphasise the need for openness and transparency to help foster public trust and the confidence. Again, the MPS experience might serve as inspiration for New Zealand Police to consider being more transparent around our uses of 'new tech' to fight crime, particularly to help 'myth bust' and counter any concerns about New Zealand Police's use of emergent technologies.

8. Charting a course forward

While the discussion of leading-edge international practices is of more relevance to any future consideration of 'new tech' trials, more immediately there would seem to be some areas for improvement to current practices. We could strengthen our internal governance by centralising the Police governance of emergent technologies. Centralisation would help drive policy, operational and ethical consistency, and ensure our standardised processes for C&A, PIAs and legal review are consistently followed. Any new governance arrangements (and the processes work groups should use to raise proposals for governance consideration) should be set out in a policy document easily accessible to operational groups.

We could also consider introducing new policy guidelines for the deployment of emergent technologies in light of domestic and international best practice. Such an exercise would do well to draw on the Government Chief Data Steward's and Privacy Commissioner's *Principles for the Safe and Effective Use of Data and Analytics* and the UK Surveillance Camera Code of Practice.

We could also consider consulting the Data Ethics Advisory Group around any more significant 'new tech' proposals.

9. Conclusions and recommendations

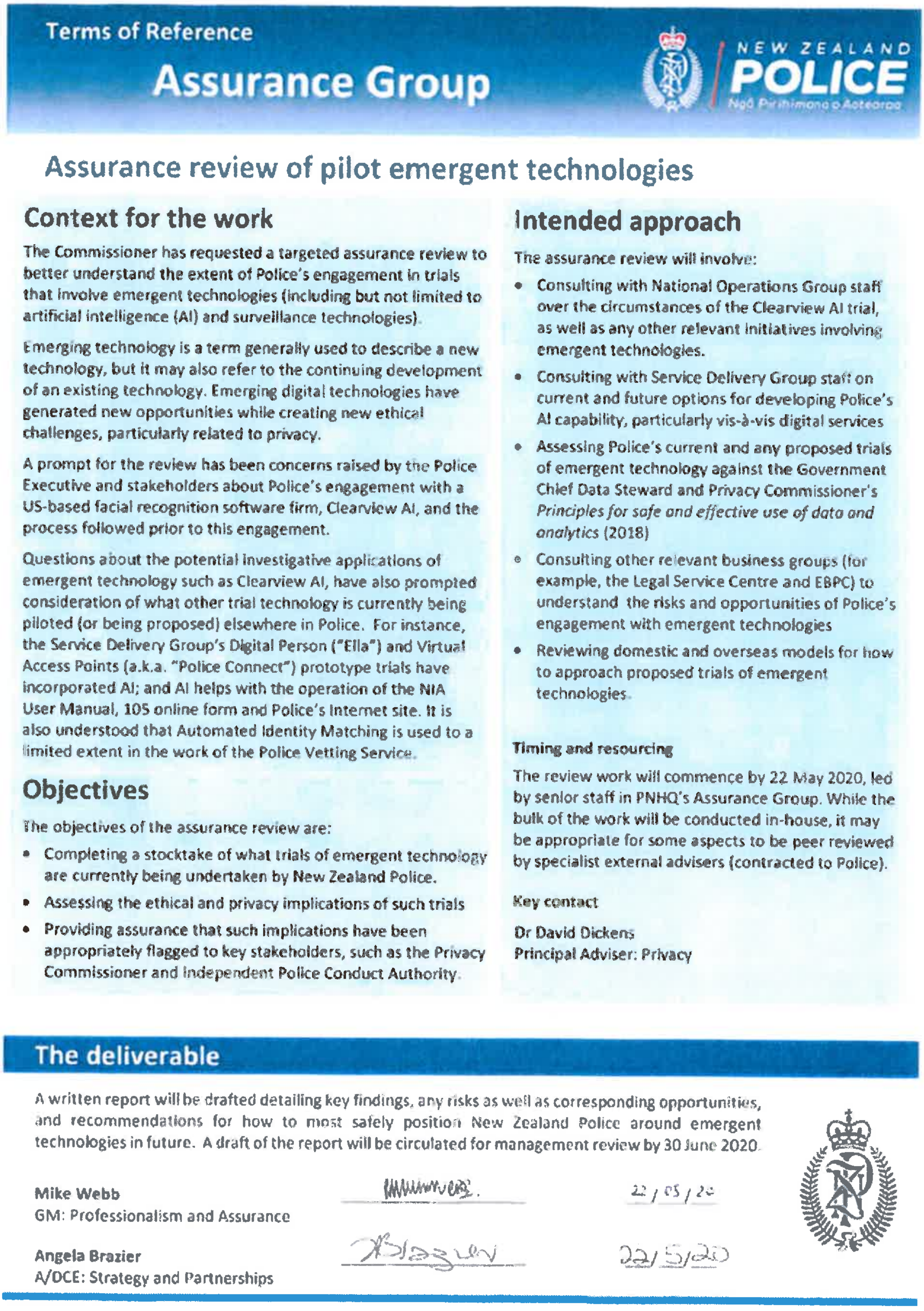
The key conclusions of this review are:

- Against a backdrop where the use of AI and other 'new tech' has become commonplace in other fields, New Zealand Police's use of emergent technologies has been reasonably conservative and carefully thought-through.
- Privacy, legal and ethical implications have appropriately been considered by Police before emergent technologies are deployed, although there is room for improvement in consistently sharing this knowledge with stakeholders.

Based on the findings of the review, it is recommended that the Police Executive:

- Consider centralising the governance of emergent technologies, to provide strengthened oversight and better ensure consistent stakeholder engagement.
- Consider new policy guidance specifically on emergent technologies, that draws on domestic and international best practice for the safe and responsible use of data, and sets out a standard process for business groups to submit a proposal for pre-approval to the recommended new central governance group.
- Consider commissioning a more comprehensive 'deep dive' into ethical and privacy implications of technologies which have already been rolled out within Police.

Annex A: Terms of Reference for the review



Terms of Reference

Assurance Group

NEW ZEALAND POLICE

Ngā Pirihimana o Aotearoa

Assurance review of pilot emergent technologies

Context for the work

The Commissioner has requested a targeted assurance review to better understand the extent of Police's engagement in trials that involve emergent technologies (including but not limited to artificial intelligence (AI) and surveillance technologies).

Emerging technology is a term generally used to describe a new technology, but it may also refer to the continuing development of an existing technology. Emerging digital technologies have generated new opportunities while creating new ethical challenges, particularly related to privacy.

A prompt for the review has been concerns raised by the Police Executive and stakeholders about Police's engagement with a US-based facial recognition software firm, Clearview AI, and the process followed prior to this engagement.

Questions about the potential investigative applications of emergent technology such as Clearview AI, have also prompted consideration of what other trial technology is currently being piloted (or being proposed) elsewhere in Police. For instance, the Service Delivery Group's Digital Person ("Ella") and Virtual Access Points (a.k.a. "Police Connect") prototype trials have incorporated AI; and AI helps with the operation of the NIA User Manual, 105 online form and Police's Internet site. It is also understood that Automated Identity Matching is used to a limited extent in the work of the Police Vetting Service.

Objectives

The objectives of the assurance review are:

- Completing a stocktake of what trials of emergent technology are currently being undertaken by New Zealand Police.
- Assessing the ethical and privacy implications of such trials
- Providing assurance that such implications have been appropriately flagged to key stakeholders, such as the Privacy Commissioner and Independent Police Conduct Authority.

Intended approach

The assurance review will involve:

- Consulting with National Operations Group staff over the circumstances of the Clearview AI trial, as well as any other relevant initiatives involving emergent technologies.
- Consulting with Service Delivery Group staff on current and future options for developing Police's AI capability, particularly vis-à-vis digital services
- Assessing Police's current and any proposed trials of emergent technology against the Government Chief Data Steward and Privacy Commissioner's *Principles for safe and effective use of data and analytics* (2018)
- Consulting other relevant business groups (for example, the Legal Service Centre and EBPC) to understand the risks and opportunities of Police's engagement with emergent technologies
- Reviewing domestic and overseas models for how to approach proposed trials of emergent technologies.

Timing and resourcing

The review work will commence by 22 May 2020, led by senior staff in PNHQ's Assurance Group. While the bulk of the work will be conducted in-house, it may be appropriate for some aspects to be peer reviewed by specialist external advisers (contracted to Police).

Key contact

Dr David Dickens
Principal Adviser: Privacy

The deliverable

A written report will be drafted detailing key findings, any risks as well as corresponding opportunities, and recommendations for how to most safely position New Zealand Police around emergent technologies in future. A draft of the report will be circulated for management review by 30 June 2020.

Mike Webb
GM: Professionalism and Assurance

22/05/20

Angela Brazier
A/DCE: Strategy and Partnerships

22/5/20

Annex B: Principles of the UK Surveillance Camera Code of Practice

The Principles of the UK Surveillance Camera Code of Practice are:

- Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.
- The use of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.
- There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints.
- There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.
- Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them.
- No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged.
- Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes.
- Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.
- Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.
- There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published.
- When the use of a surveillance camera system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should then be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value.
- Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up to date.

IMS Photo Manager and ABIS 2 Project

Privacy Impact Assessment

Prepared by the National Biometric Information Office (NBIO) and the Assurance Group, New Zealand Police

October 2020

Executive Summary

The ABIS 2 Project aims to upgrade image management with an enhancement to the existing IMS Photo Manager, utilising DataWorks Plus's WebWorks Plus system; which deals with the loading and use of images taken from individuals and the upgrade of the IMS facial recognition capability using NEC's FACE Plus software. The package is being provided by DataWorks Plus. Further interface work between IMS Photo Manager and the NIA Police system is being developed in-house.

The improved system will also enable a comparison of scars, marks and tattoos. The new system is not creating a new collection of information, nor is it operating in a "public facing" capacity.

The addition of a more up to date facial comparison system will give Police the capability to load, search and compare crime scene / incident images from a variety of sources (including but not limited to static images captured from CCTV footage and digital photographs) with poorer quality facial images in the footage against known identity images. The electronic searchable tattoo image database will also increase Police's intelligence capability.

The capability to Livestream CCTV was not included in the Business Case, the RFP requirements, the detailed design or the build.

The IMS Photo Manager image comparison tool will be operated and managed from the National Biometric Information Office (NBIO) and will only be available to trained staff within the NBIO. The system will be governed by defined business processes and system rules which will be created before deployment. There will be a reporting capability for user activity for auditing purposes.

A range of risks arise around the governance and management of the system; access to the tool by the wider policing capability; and, transparency with the public about Police's uses of the system. In Privacy Act terms the relevant Information Privacy Principles include IPP 3 (Advice about the use of collected personal information; IPP 5 (Security); IPP 8 (Accuracy of Personal Information); and IPP 10 (Use of personal information).

The recommendations within the report are –

Recommendation 1: Establish an administrative and user system within the NBIO that safeguards the system to the management and use of trained and experienced staff only and potential links will be provided for intelligence purposes only. The establishment of Active Directory Groups should only give authorised users the capability. Only NBIO and ICT Administrators ought to have access. Comprehensive system rules and reporting tools will ensure User Activity is recorded and reportable for audit purposes.

Recommendation 2: Establish administrative oversight of the system so that results are overseen by NBIO staff and scrutinised by them prior to release to investigative staff. All potential match reports to be generated by trained NBIO staff members.

Recommendation 3: Establish a business process where requests for searches of the image database are submitted in writing, approved by a supervisor and tied to a function of Policing.

Recommendation 4: Establish oversight of IMS Photo Manager by an appropriate governance group that receives regular reports detailing the effectiveness of the system and provides assurance that the operation of the system remain ethical and lawful.

Recommendation 5: Establish a communications plan to signal widely the use of the IMS Photo Manager system within the ABIS 2 project.

Overall the estimated risk rating without controls sits at *High 14 to High 22.* If effective controls and mitigations are deployed the residual risk rating is likely to be *Medium 6 to Medium 13.* The residual risk would be within Police's acceptable risk rating. Table 2 at the end of the report details identified risks and suggested mitigations and controls.

Privacy Impact Assessment

Why a Privacy Impact Assessment?

A PIA examines a change, project or system to evaluate how, and to what extent, it might impact on individual privacy. It also identifies inherent risks pertinent to the Police operational use of a business process or tool. The PIA process is about designing privacy into the project, to ensure that risks are identified early and processes, products and safeguards are designed with privacy in mind from the outset. It's about setting the right course early.

This assessment has a focus on ABIS 2 project (Automated Biometric Identification Solution) which is an umbrella term that encapsulates a suite of products used within Police Biometrics, including the original AFIS (Automated Fingerprint Identification system). ABIS 2 specifically refers to an upgrade to the photo Management (IMS) aspects of Biometrics, including improved facial comparison software and the capture of Scars, Marks and Tattoos at the point of capturing other Biometric data at police stations. The assessment is intended to assist the National Biometric Information Office (NBIO) to avoid privacy pitfalls and deploy ABIS in a way that strikes an appropriate balance between business benefits and good privacy practice.

Like all risk assessment reports, this PIA should be viewed as a living document, which ought to be revisited later in the process either to accommodate changes to the project or when the tool has merged into 'business as usual'. Over time it should be used to establish how risks have been managed and whether controls continue to be effective.

Scope of this PIA

This PIA looks at the privacy impacts of the deployment of a new and upgraded tool that will assist the NBIO to manage its growing image database. The new system is not creating a new collection of information, nor is it operating in a "public facing" capacity. The NBIO currently has responsibility for managing Police's fingerprint records and images library. The images a drawn from a range of existing collection practices including custody photographs, firearms licence photographs, informal photographs of suspects collected in connection with law enforcement activities and missing persons. The PIA will cover the deployment of the technical tool and management of the images data base. Not necessary within the risk assessment is examination of collection (IPP 1 – 4), (but the expectations of good management of personal information that derive from them are, concepts such as transparency around why and how we are using information), retention (IPP 9) or use of the images as these practices are current business as usual and will not change as a result of the ABIS 2 upgrade.

The assessment will consider the issues that arise in the deployment of the Image Management System (IMS Photo Manager). Risk will be identified and quantified by reference to Police's risk matrix.

Privacy Considerations

Several lenses are used to assess a project – Information Privacy Principles (IPPs) in the Privacy Act; Privacy by Design©[1]; and, principles used in the deployment of data analytics or emergent technologies. IPPs are outlined in the Privacy Act 1993[2] and provide for responsibilities around how agencies may collect, store, provide access to, use and disclose personal information. They encourage a view right across the lifecycle of the information from collection to disposal. They are designed to ensure that an agency can use personal information to achieve its lawful purposes efficiently and effectively, while protecting the privacy rights of the individuals the information is about. Although sourced from the Privacy Act, these IPPs are reflective of globally accepted best privacy practice, and provide an effective framework through which to assess privacy issues in the context of the IMS Photo Manager.

In addition the seven principles of Privacy by Design© are relevant. These help to build privacy controls into systems, technologies and processes. If implemented correctly, individuals should not have to take any action to protect their privacy – the system's design achieves this by default.

Lastly, emergent technologies that use algorithm calculation for analytical purposes require further consideration of their use from a fairness and ethical perspective. The Privacy Commissioner's *Principles for the Safe and Efficient Use of Data Analytics – May 2018*[3] point to considerations that include ensuring that the tool delivers a clear public benefit; the data is fit for the purpose of analytics; privacy and ethical issues are explored; where appropriate the technological use is transparently used; maintain human oversight of the process including decision making; and, adequate governance.

Image Management System (IMS Photo Manager)

The existing image management system (Photo Manager) was fully implemented by Police in 2009 to replace the Photographic Image Management System (PIMS) which was a standalone system implemented by Police in 1992. The current image management system has provided a single repository for all identification images including Formal Prisoner Photographs, Firearms Licence holders, Suspect images and Missing Persons images. However the system has very limited and outdated facial recognition capability. Currently scars, marks and tattoo details are held in a

[1] Privacy by Design© 7 Principles - Privacy measures should be proactive not reactive; Privacy should be the default setting; Privacy should be embedded into design; Aim for full functionality rather than viewing privacy in opposition to other interests; Ensure end-to-end information security; Promote visibility and transparency of risks and solutions; and, make sure systems are user-centric.

[2] Note that on 1 December 2020 the new Privacy Bill is scheduled to come into effect. However the current privacy principles will not be substantively different in the new legislation.

[3] Principles-safe-and-effective-data-and-ana

coded/textural format. Police have no image based capability to capture, classify, search and match scars, marks and tattoos and logos for intelligence or identification purposes.

The addition of a more up to date facial comparison system, via IMS-Photo-Manager~~,~~ will give Police the capability to load, search and compare crime scene / incident images from a variety of sources (including but not limited to static images captured from CCTV footage and digital photographs) with poorer quality facial images in the footage against known identity images. The electronic searchable tattoo image database will also increase Police's intelligence capability.

The capability to Livestream CCTV was not included in the Business Case, the RFP requirements, the detailed design or the build.

Purpose of the change, including any projected benefits to your organisation or to the individuals affected.

IMS Photo Manager will provide a more advanced electronic facial comparison system that improves image quality and can provide more opportunities for matching, particularly with poorer quality facial images often encountered with CCTV footage. This improved searching and matching capability will reduce investigation time and prevent crime and victimisation rates. It will provide a significantly higher level of success at identifying suspects/offenders when compared with manual searching, leading to early perpetrator intervention and reducing the time taken to make the links.

Current technology and processes do not allow NZ Police to capture and utilise individuals' identifying particulars, scars, marks and tattoos (SMT) in a timely manner. This leads to the opportunity for re-offending and re-victimisation. The investigation time involved in comparing images will be significantly reduced, meaning greater time for other investigative activity.

Both facial and SMT images from offenders will be captured within stations/sites and retained under ss.32 and 33 of the Policing Act 2008.

The IMS Photo Manager enhancement will enable records to be stored and classified in categories and sub-categories, and in addition to facial comparison capability, searches can be made on soft biometrics such as scars, marks and tattoos.

The IMS Photo Manager image comparison tool will only be available to trained staff within the NBIO who will be trained to use the system, governed by defined business processes and system rules. These rules and protocols will be established before the IMS is deployed. There will be a reporting capability for user activity for auditing purposes.

The Nature of the Information.
Facial images in the Police images collection include Formal Offender (custody suite photographs), Child Sex Offender images, Returning Offender images, missing person's images, and Firearms Licencing photographs. Images of scars, marks and tattoos are also collected from the custody suite and from registered Child Sex Offenders. (See Appendix 1 for details of the collection processes). The formally acquired images are used to compare images on a variety of mediums that are provided to Police by witnesses to crime or acquired by Police through criminal investigative processes.

Current and projected volumes of images are contained within the table below, showing that at any stage the Photo Manager system will have in excess of 2 million images to manage.

Category	Historic Records (Current)	Estimated Additional Records per Annum (Future)
Image Management - Prisoner	1.85M from 800,000 individuals	50,000 per annum
Image Management - Suspect	N/A	7,500 per annum
Image Management - Firearms Licence holders	245,000 at any one time	10,000 renewals per annum 9,500 new per annum
Image Management - Missing Persons	200	300 per annum
Image Management – Child Protection (Child Sex Offender Register)	1,500	2,300 per annum
Facial Recognition Search, Compare, Match and Report	Nil	At least 15,000 per annum
Photo line-up Production	12,000 (Time to prepare standard line-ups: 20 – 60 minutes)	15,000 (Time to prepare standard line-ups: 10 minutes)
Scars Marks and Tattoos and Logos Capture, Search, Match and Report	2,500	30,000 (estimated)

Table 1 - Current and Projected Data within the Photo Manager System

Initial risk assessment

The images library contained with IMS Photo Manager comprise a significant volume of images. These images will be used for comparison with photographs that Police wish to identify for a variety of law enforcement reasons. The tool used for comparison purposes uses algorithms deployed to match a defined quantity of features to produce a potential match or matches.

The risks in deploying the facial recognition aspect of the technology arise out of appropriate deployment, use and security (IPP 10 – Appropriate use; IPP 5 – Security and IPP 8 – Accuracy) of the comparison tool and the image library, ensuring that the tool is only used for a lawful business purposes (IPP 1 – Purpose) and ongoing oversight of the deployment. There are potential 'transparency' issues that require managing (IPP 3 – Advice about the use of collected information). The remaining IPPs are not relevant to this deployment of IMS Photo Manager and the use of existing and to be collected personal information.

Use and Deployment of the Facial Comparison Tool

The proposed application uses industry-leading algorithms and can be tasked to perform facial comparison searches for both newly-acquired images, as well as previously-enrolled images. Newly-acquired image queries can be configured for automatic searching and on an ad-hoc basis as new records are generated. Previously-enrolled image queries can also be performed on an ad-hoc basis by authorised users.

The biometric matching process is controlled by the user so that only the best few images are returned as matches in descending order from the highest match score. The Administration Module allows Administrators of the system to set the facial match scoring thresholds to determine what query scores are considered a match or non-match. Only images that are above the match score threshold will be displayed to the user.

There is a risk that if the system is not managed by trained and competent users, the tool may be used in an unnecessarily liberal manner therefore returning matches that are questionable. This raises a risk of contravening IPP 8 which requires personal information not to be used or disclosed without taking steps to ensure the information is accurate, up to date, complete, relevant and not misleading. This risk would be *likely* if the tool were to be used by untrained and inexperienced users. This may result in *moderate* to *major* consequences including scrutiny by public media, scrutiny from the IPCA or the Privacy Commissioner either on their own initiative or driven by complaints from individuals who have been incorrectly identified as persons of interest to the Police. The incorrect identification of individuals is a potential risk to the individuals that may result in unnecessary or arbitrary arrest or detention. Currently there is a high level of public concern about emergent technologies and any misuse or perception of misuse creates media and political interest, and potential harm to individuals. It is likely that unless adequate controls are put in place the inherent risk would sit at *High 17 to 22*.

Appropriate controls would include limiting the deployment of the algorithm to only those trained members of the NBIO. Training ought to include a high level understanding of the effect of any changes that the user can make to the way the tool carries out the search function. Administrative settings ought to be determined and applied consistently within the system. These setting ought to be a part of the business protocols and rules for using the system. In addition the images database and the results of searches, ought to be managed solely by the NBIO group so that the integrity of the images within the database and the use of the comparison tool are confined to highly trained users and consistent algorithmic thresholds are applied. Decisions about whether a matched image is appropriate for release to an investigation team should remain with the NBIO staff.

Recommendation 1: Establish an administrative and user system within the NBIO that safeguards the system to the management and use of trained and experienced staff only and potential links will be provided for intelligence purposes only. The establishment of Active Directory Groups should only give authorised users the capability. Only NBIO and ICT Administrators ought to have access. Comprehensive system rules and reporting tools will ensure User Activity is recorded and reportable for audit purposes.

Recommendation 2: Establish administrative oversight of the system so that results are overseen by NBIO staff and scrutinised by them prior to release to investigative staff. All potential match reports to be generated by trained NBIO staff members.

Applying these controls will reduce the likelihood to *unlikely* with the consequences remaining at *moderate* to *major.* The residual risk is likely to move to Medium 9 to 13.

Lawful Business Purposes

The IMS Photo Manager is deployed to assist with Police's functions of law enforcement and keeping the community safe. Operational business groups should only seek facial comparisons by trained NBIO staff for a range of appropriate business reasons from the comparison of suspect images with those in the image database to establish the identity of a suspect for a crime, through to locating better images of lost or missing persons or establishing identity of an unidentified deceased individual.

It is *possible* that the image library and the facial/image comparison tool could be misused or abused if careful oversight of requests for access to the system are not scrutinised. IPP 10 expects an agency to only use personal information for the purpose for which it was obtained. Personal information within the scope of the NBIO is acquired for law enforcement purposes or public safety. It is important to maintain oversight of the use of that information so that unlawful purposes are not applied. Like the previous risk category, abuse of the tool would expose Police to unwanted attention from a number of public quarters and have a *moderate* to *major* impact on the trust and confidence of Police. In addition misuse of the system may have a significant impact on individuals who are the subject of aberrant searches of the database. The inherent risk would be *High 17 to 22*.

Controlling access to the image library and the corollary use of the facial/image comparison tool ought to include a business process where requests for searches of the image database are submitted in writing seeking access to the system. All 'suspect' searches will be submitted via Lotus Notes (or a new alternative) with full details of the offence, including Case (DOCLOC) Reference, Submitting Officer and details of the Supervisor Authorising Submission. All 'suspect' images will be dealt with as Exhibits; entered into Police Register of Property (PROP) prior to submission. The Chain of Evidence / continuity will be maintained throughout the process. The requests ought to describe in sufficient detail the reason for the request and the particular Police function that is at the heart of the request. In addition the request ought to be approved by the requester's supervisor in all cases to demonstrate the legitimacy of the request and the business reason for it. Records of the requests and responses ought to be maintained indefinitely to contribute to audit and assurance reporting.

Recommendation 3: Establish a business process where requests for searches of the image database are submitted in writing, approved by a supervisor and tied to a function of Policing.

By establishing a business process that ensures oversight of the requests for access to the image database the likelihood of misuse of the system would be reduced to *rare* with the residual risk reduced to *medium 6 to 10.*

Ongoing Oversight of IMS Photo Manager

The community interest and tension around the deployment of emergent technologies such as facial recognition or facial and image comparison tools receives global attention at present, particularly where the tools are deployed in the law enforcement space. Recent public furore over the NZ Police's interest in the Clear View AI tools created heightened interest in our use of emergent technologies. Police's interest in Clear View AI is not a relevant interest in the ABIS 2 Project. The Commissioner of Police has set an approval and governance oversight for all projects that involve emergent technologies. NECs algorithm fits into the category of emergent technologies.

In addition to there being a requirement to run the deployment past executive and other governance arrangements to approve the deployment, it is very appropriate to ensure that the ongoing governance of the system is established. Governance is an aspect of meeting our general obligations within the relevant IPPs including security (IPP 5), accuracy of the tool (IPP 8), and appropriate use of the personal information provided to and used by the NBIO (IPP 10). The absence of ongoing business governance risks the tool not receiving sufficient oversight to ensure that controls remain fit for purpose, that the tool remains lawfully used and that the system continues to provide a benefit to Policing and contributes to keeping the public safe. Without ongoing governance oversight it is *possible* that the system may fail to deliver a safe and defensible service or its use is inadvertently widened beyond the current stated purpose, known as function creep. Were the system to become subject to external scrutiny Police would be seriously criticised for not establishing governance over the system. This would be unacceptable, particularly in the context of an emergent technology, as Police might be seen as potentially cavalier about its oversight of technology, an unacceptable rhetoric for a law enforcement agency. The consequences of an unexpected event may be *moderate* to *major* depending on the context, with an inherent risk rating of *High 14 to 18*.

Establishing governance oversight to an appropriate new governance group ought to involve regular reporting to that group in a '3 lines of defence' assurance mode. That would at least mean reporting that demonstrated the worth of the tool by reference to the number of requests; the success of the system with examples; the time saved if capable of quantification; and, updates about the reliability and effectiveness of tools capability in identifying images correctly. Additionally, periodic reporting ought to demonstrate that the controls remain in place, remain effective and if not recommendations for any changes are made, if warranted. Demonstrating that the efficacy of comparisons continues to be overseen by human decision making is an important aspect of ensuring that the system remains lawful and ethical. The NBIO intends to supply prescribed and ad hoc reports as required.

Recommendation 4: Establish oversight of IMS Photo Manager by an appropriate governance group that receives regular reports detailing the effectiveness of the system and provides assurance that the operation of the system remain ethical and lawful.

Regular and constant assurance reporting to an appropriate governance group will ensure that the integrity of the system is maintained, that it continues to provide a benefit to the business and provide assurance that the tool is used ethically and lawfully. The likelihood of an unexpected event would reduce to *unlikely* or *rare* and the consequences while remaining *moderate* to *major* the residual risk value would reduce to Medium 6 to 13.

Transparency

As mentioned earlier in the report there is a heightened community interest in emergent technologies such as facial recognition and artificial intelligence. That interest is particularly heightened where the technology is deployed overseas and more so when the state agency is a law enforcement agency. Media coverage has focussed on the deployment of technology in public places, for example at large sporting events where facial recognition tools are used to locate wanted persons or persons of interest. IPP 3 expects that an agency will communicate with individuals at the time of collection of their information and while this is not relevant in the context of IMS Photo Manager, the wider expectation of transparency around use of information remain good business practice.

New Zealand Police will not be using IMS Photo Manager technology in a public facing way. The correct rhetoric is that Police is deploying the tool to assist with searches of its existing and growing images library. Images that Police lawfully acquire as a consequence of carrying out its functions under the Policing Act. As a result it is important for Police to be open and transparent about our deployment of IMS Photo Manager to dispel any potential unrealistic views of the project and the system.

The inherent risk of not getting on the front foot and being transparent about the project is that public thought will be influenced by incorrect assumptions about the extent of the use of the system, therefore bringing Police into unnecessary negative commentary about its use of technology.

Recommendation 5: Establish a communications plan to signal widely the use of the IMS Photo Manager system within the ABIS 2 project.

The risks to Police through introducing the IMS Photo Manager technology will be reduced if a communications plan includes –

- Consultation with the Privacy Commissioner's office before full deployment
- At appropriate times, media statements about the deployment of IMS Photo Manager accompanied by assurances about the controls and limits of the system
- Commentary of the Police Website under the area 'How We Manage Personal Information' detailing how we deploy IMS Photo Manager

Table 2 - Inherent Risk – Residual Risk & Recommended Controls

Inherent Risks	Recommended remedies and controls and Residual Risk	Privacy Act Principle applicable	Date Considered or Implemented
Risk 1 & 2 - There is a risk that if the system is not managed by trained and competent users, the tool may be used in an unnecessarily liberal manner therefore returning matches that are questionable. It is likely that unless adequate controls are put in place the inherent risk would sit at *High 17 to 22*.	Appropriate controls would include limiting the deployment of the comparison tool to only those trained members of the NBIO. Training ought to include a high level understanding of the effect of any changes that the user can make to the way the tool carries out the search function. In addition the images database and the results of searches, ought to be managed solely by the NBIO group so that the integrity of the images within the database and the use of the comparison tool are confined	IPP 8 Accuracy of personal information	

	to highly trained users. Decisions about whether a matched image is appropriate for release to an investigation team should remain with the NBIO staff. Applying these controls will reduce the likelihood to *unlikely* with the consequences remaining at *moderate* to *major.* The residual risk is likely to move to Medium 9 to 13.		
Risk 3 - It is *possible* that the image library and the facial/image comparison tool could be misused or abused if careful oversight of requests for access to the system are not scrutinised. The inherent risk would be *High 17 to 22.*	Controlling access to the image library and the corollary use of the facial/image comparison tool ought to include a business process where requests for searches of the image database are submitted in writing seeking access to the system. The requests ought to describe in sufficient detail the reason for the request and the particular Police function that is at the heart of the request. In addition the request ought to be approved by the requester's supervisor in all cases to demonstrate the legitimacy of the request and the business reason for it. By establishing a business process that ensures oversight of the requests for access to the image database the likelihood of misuse of the system would be reduced to *rare* with the residual risk reduced to *medium 6 to 10.*	IPP 10 – Appropriate use of personal information	
Risk 4 – It is appropriate to ensure that the ongoing governance of the system is established. The absence of ongoing business governance risks the tool not receiving sufficient	Establish oversight of the IMS Photo Manager system by appropriate governance group that receives regular reports detailing the effectiveness of the system and provides assurance that the operation of the system remain ethical and lawful.	IPP 5 Security; IPP 8; and IPP 10.	

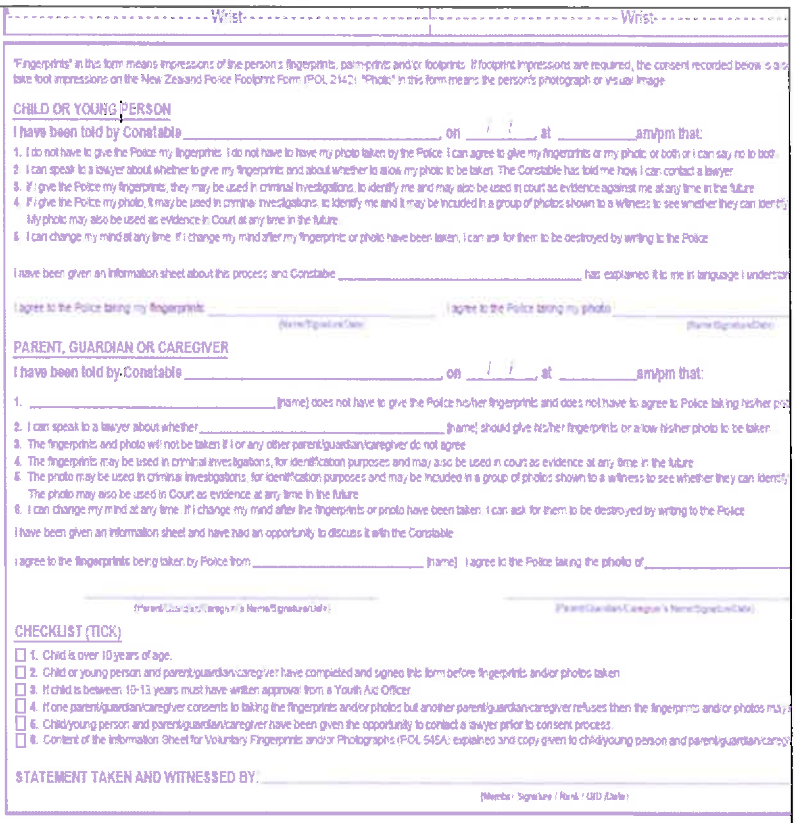
oversight to ensure that controls remain fit for purpose, that the tool remains lawfully used and that the system continues to provide a benefit to Policing. The consequences of an unexpected event may be *moderate* to *major* depending on the context, with an inherent risk rating of *High 14 to 18*.	Regular and constant assurance reporting to an appropriate governance group will ensure that the integrity of the system is maintained, that it continues to provide a benefit to the business and provide assurance that the tool is used ethically and lawfully. The likelihood of an unexpected event would reduce to *unlikely* or *rare* and the consequences while remaining *moderate* to *major* the residual risk value would reduce to Medium 6 to 13.		
Risk 5 – There is an inherent risk of not getting on the front foot and being transparent about the project resulting in the public thought being influence by incorrect assumptions about the extent of the use of the system, therefore bringing Police into unnecessary negative commentary about its use of technology.	Establish a communications plan to signal widely the use of the IMS Photo Manager system within the ABIS 2 project that includes – o Consultation with the Privacy Commissioner's office before full deployment o At appropriate times, media statement about the deployment of IMS Photo Manager, accompanied by assurances about the controls and limits of the system o Commentary of the Police Website under the area 'How We Manage Personal Information' detailing how we deploy the IMS Photo Manager system.	IPP 3 – advising individuals about how their information is used	

Appendix 1

Category Overview - Legislation / Authorisation

The images held by Police are stored in logical categories; Formal (which includes Offender, Voluntary, Customs, Child Sex Offender, and Returning Offenders), Firearms Licence holders, Missing Persons and Suspect images. The following table sets out the overview for each category.

Category	**Legislation / Authorisation / Policy**	**Comments**
Offender	Policing Act 2008 ss.32, 33, 34 34A	Identifying Particulars Taken on Arrest or Summons. Retained on Conviction
Voluntary	Police Instructions – Youth Justice POL 545 Page 2 of the Fingerprint Form POL545A Information Sheet	The taking of voluntary fingerprints and photographs MUST be the result of an assessment involving a number of sources that identify the child or young person being at risk of or developing a pattern of offending. The reasons why it is believed the child or young person is at risk of or developing a pattern of offending should be recorded. There are several factors considered prior to requesting voluntary fingerprints and photographs. If there has been no arrest and section 33 of the Policing Act does not apply because a Family Group Conference (FGC) has not been completed the following are considered before the request is made: • The nature and seriousness of any suspected offending. • The nature and extent of information already collected on the child or young person's offending / behaviour. • Whether Police already have the child or young person's fingerprints and / or photographs. • Whether the situation requires a formal action and would be more appropriately dealt with by way of arrest (in this situation fingerprints should be taken under s.32) **POL545 page 2** sets out the informed consent process



Wrist Wrist

"Fingerprints" in this form means impressions of the person's fingerprints, palm-prints and/or footprints. If footprint impressions are required, the consent recorded below is als take foot impressions on the New Zealand Police Footprint Form (POL 2142). "Photo" in this form means the person's photograph or visual image

CHILD OR YOUNG PERSON

I have been told by Constable ______________________, on __/__/__, at ________am/pm that:

1. I do not have to give the Police my fingerprints. I do not have to have my photo taken by the Police. I can agree to give my fingerprints or my photo or both or I can say no to both
2. I can speak to a lawyer about whether to give my fingerprints and about whether to allow my photo to be taken. The Constable has told me how I can contact a lawyer
3. If I give the Police my fingerprints, they may be used in criminal investigations, to identify me and may also be used in court as evidence against me at any time in the future
4. If I give the Police my photo, it may be used in criminal investigations, to identify me and it may be included in a group of photos shown to a witness to see whether they can identify My photo may also be used as evidence in Court at any time in the future
5. I can change my mind at any time. If I change my mind after my fingerprints or photo have been taken, I can ask for them to be destroyed by writing to the Police

I have been given an information sheet about this process and Constable ______________________ has explained it to me in language I understa

I agree to the Police taking my fingerprints ______________________ I agree to the Police taking my photo ______________________

(Name/Signature/Date) (Name/Signature/Date)

PARENT, GUARDIAN OR CAREGIVER

I have been told by Constable ______________________, on __/__/__, at ________am/pm that:

1. ______________________ (name) does not have to give the Police his/her fingerprints and does not have to agree to Police taking his/her ph
2. I can speak to a lawyer about whether ______________________ (name) should give his/her fingerprints or allow his/her photo to be taken
3. The fingerprints and photo will not be taken if I or any other parent/guardian/caregiver do not agree
4. The fingerprints may be used in criminal investigations, for identification purposes and may also be used in court as evidence at any time in the future
5. The photo may be used in criminal investigations, for identification purposes and may be included in a group of photos shown to a witness to see whether they can identify The photo may also be used in Court as evidence at any time in the future
6. I can change my mind at any time. If I change my mind after the fingerprints or photo have been taken, I can ask for them to be destroyed by writing to the Police

I have been given an information sheet and have had an opportunity to discuss it with the Constable

I agree to the fingerprints being taken by Police from ______________________ (name) I agree to the Police taking the photo of ______________________

(Parent/Guardian/Caregiver's Name/Signature/Date) (Parent/Guardian/Caregiver's Name/Signature/Date)

CHECKLIST (TICK)

□ 1. Child is over 10 years of age.
□ 2. Child or young person and parent/guardian/caregiver have completed and signed this form before fingerprints and/or photos taken
□ 3. If child is between 10-13 years must have written approval from a Youth Aid Officer.
□ 4. If one parent/guardian/caregiver consents to taking the fingerprints and/or photos but another parent/guardian/caregiver refuses then the fingerprints and/or photos may
□ 5. Child/young person and parent/guardian/caregiver have been given the opportunity to contact a lawyer prior to consent process.
□ 6. Content of the Information Sheet for Voluntary Fingerprints and/or Photographs (POL 545A) explained and copy given to child/young person and parent/guardian/caregi

STATEMENT TAKEN AND WITNESSED BY: ______________________

(Member: Signature / Rank / QID /Date)

POL 545A INFORMATION SHEET FOR VOLUNTARY FINGERPRINTS AND PHOTOGRAPHS OF CHILD/YOUNG PERSON

(Full form attached as Appendix 2) explains the process for the Child /
Young Person and their Parent / Guardian / Caregiver in plain language under the headings:

- **What is this notice about?**
- **Do I have to have my fingerprints or photo taken?**
- **Can someone help with me with this decision?**
- **Can I have someone with me when I have my fingerprints taken**
  or when I have my photo taken?
- **What will the fingerprints be used for?**

What will the photo be used for?

Police may use the photo to identify you or to work out whether you were involved in criminal offending. Your photo may also be included in a group of photos shown to a witness to see whether they can identify an offender.

If the photo shows that you were involved in criminal offending, it may be used as evidence in Court against you at any time in the future.

How long will the Police hold my fingerprints and photos?

Your fingerprints will be kept by Police until you or your parent/guardian/caregiver asks for them to be destroyed. Your

		photo will also be kept by Police until you or your parent/ guardian/caregiver asks for them to be destroyed. You can ask for your fingerprints and photos to be destroyed at any time. You do not have to give a reason. You can write to the following address if you want your fingerprints destroyed or your photos destroyed or to have both of them destroyed.
Customs	Memorandum of Understanding (2015) between NZ Police and NZ Customs; Schedule 4: Arrest and Prosecution / Arrest and Prisoner Processing Also letter of clarification (20 November 2015) from Commissioner Mike Bush to NZ Customs	Police agree to receive into custody, process and hold, persons arrested by Customs officers on behalf of Customs. Normal processing procedures must be completed by Police. As soon as practicable following the filing of charges, Customs will provide the Police National Biometric Information Office with charging information, for the purposes of ensuring the biometric records are linked to relevant charge information. The information will be sent electronically to the National Biometric Information Office and will include: • Arrested person's name, sex and date of birth; • Date of arrest; • Police station where the person was processed; • Justice Person Record Number (PRN); • Details of the charges and appropriate charge codes. The National Biometric Information Office will ensure the charging information for the arrested person will be linked to their electronic biometric records; in NIA the biometrics are held in relation to charges on the associated Justice PRN.
Child Sex Offenders	Child Protection (Child Sex offender Government Agency Registration) Act 2016	s. 32 Identifying particulars and other information may be stored by Police
Returning Offenders	Returning Offenders – Returning Offenders (Management and Information) Act 2015	s. 8 Purpose of obtaining information for use by Police for any lawful purpose s. 9 Police may request returning offender to provide identifying particulars s. 10 Police may detain returning offender for purpose of taking identifying particulars s. 11 Police may take identifying particulars s. 12 Storage, etc, on Police information recording system of identifying particulars

Firearms Licence	Arms Act 1983	Firearms Licensing Application form: *'The information you provide on this form is collected for the purpose of administration of the Arms Act 1983. NZ Police will hold, store, use or disclose the personal information collected in accordance with the provisions of the Privacy Act 1993. This means that, where necessary, NZ Police may use or disclose your personal information to enable it to carry out its lawful functions, including prevention, detection, investigation and prosecution of offences. Please refer to the Privacy section of our website for more information'.* Use of the Firearms Licensing Application form photograph is essential for initial vetting and for continued integrity of the licensing process and management of firearms licences.
Missing Persons	Police instructions – Missing Persons Common Law POL 65 Publicity Form	Photographs of Missing Persons are obtained to assist with enquiries to locate or ensure the safety of that person. These enquiries are carried out under the common law power to make all necessary enquiries to protect and preserve life. Part of the enquiry involves obtaining from the informant a recent photograph of the missing person and a signed authorisation for Publicity form POL 65. Not all Missing Persons photographs will be loaded to the Missing Person database. This process will be managed by the Missing Person Unit.
Suspect		Suspect images will be held on the unsolved suspect database and are images of unknown person image from a scene / incident. They will be treated as an exhibit being entered on PROP system and linked to a NIA Case with a NIA Forensic Examination. The submitting officer will select a forensic test for the exhibit. The Test being Facial Comparison. This is the same process as when officers submit Fingerprints or DNA for examination; they select a Test. Submission for a Facial Comparison examination will need to be authorised by a supervisor, as with other forensic exhibits with subsequent tests / analysis. This Facial Comparison capability may be used as an alternative/additional option for 'identity sought' when districts publish photos of individuals on Police Intranet / websites etc. It can also be used for the linking of scenes / incidents where the same individual is involved. The images will be used for intelligence / investigation purposes. These images will be used for facial comparison purposes and searched against the known person databases (Offender, Voluntary, Customs, Child Sex Offenders, Returning Offenders, Firearms Licence holders and Missing Persons) to provide intelligence / identity of the individual featured in the Suspect image. The system cannot be used for Facial Recognition of Live streaming or within a public facing context.