	Date of request:	6/11/2020										
Part 1 - main request												
Technology	**1. Which police unit(s) or similar, owns/governs the tech and the use of it**	**2. The name of the company supplying the tech**	**3. The name of the key software the tech relies on**	**4. The name of any other company supplying that software in whatever way, eg to police or to the police's supplier above**	**5. The name of any software in this tech that gives this tech any facial recognition capability – whether used by police, or not used**	**6. A copy of any RFI, RFP or RFT run under which this tech was procured**	**7. A copy of any 'requirements document' for the tech procured**	**8. A copy of any outline of police future strategic requirements similar to that in the ABIS 2 document p52, for the tech**	**9. The title of any and all legislation and which sections of it, that police refer to with regards to use of the tech in investigation, surveillance and/or search functions**	**10. Who/which entity will audit the use, data capture, transfer and storage related to the tech, using what internationally accredited audit system if any (pls name this system) and how often. – If not using an internationally accredited audit system,pls specify what audit system WILL be used**	**11. How data captured by the tech is stored and where**	**12. Re data storage, specifically whether the data MUST contractually be kept onshore in NZ or if that is not a requirement**
BriefCam	High Tech Crime Group	BriefCam Ltd	BriefCam Investigator for Teams	Refused [s18(g)]. This is vendor-proprietary software purchased by Police 'off the shelf', and Police does not hold any information relating to secondary suppliers that may or may not contribute technology to the product.	Refused [s18(g)]. While the purchased software offers image matching/facial recognition product features, this is vendor-proprietary software purchased by Police 'off the shelf', and Police does not hold any information relating to secondary suppliers that may or may not contribute technology to the product.	Refused [s18(e)]. No RFI/RFP/RFT or equivalent procurement documents exist, because the software was acquired as a retail purchase of an 'off the shelf' product direct from the vendor. No formal procurement process was required due to the total acquisition cost, and limited/'niche' product market.	Refused [s18(e)]. No requirements specification or equivalent pre-procurement documents exist, because the software was acquired as a retail purchase of an 'off the shelf' product direct from the vendor. By way of background, impetus for acquisition of these products has been operational need identified in the course of specific investigations, which have driven desktop scans of the market by investigators for products that might assist in managing or analysing the data obtained by the investigations.	Refused [s18(e)]. No future strategic requirements for the technology have been canvassed. These are 'off the shelf' software products purchased direct from the vendor, in response to operational need identified in the course of specific investigations, which have driven desktop scans of the market for products that might assist in managing or analysing the data obtained by the investigations. While these products may be subject to normal software updates and version release cycles, these reflect vendor-led rather than customer-driven product development.	Data which may, in the course of investigation, be analysed using these tools has been lawfully obtained as potential evidence in relation to specific matter, and is subject to the usual legislative controls imposed on investigators including the Privacy Act 2020 and such sections of the Search and Surveillance Act 2012, Crimes Act 1961, and Misuse of Drugs Act 1975 as are relevant to the particular case being investigated. Note that these software products are used by New Zealand Police on a relatively small scale as investigative analytical tools, and are not used for any form of surveillance.	Use of this product is limited by software licence to a small team of five specialist investigators with management oversight. Any evidence obtained is subject to the usual oversight of criminal justice processes.	This is a stand-alone system, which is loaded with CCTV footage lawfully obtained in relation to specific investigations (i.e., it is not loaded with 'all' CCTV footage or connected to live CCTV feeds). Data is stored locally on Police servers.	Refused [s18(e)]. This is an 'off the shelf' stand-alone software product, which does not have an associated data services contract.
Nuix	High Tech Crime Group; Asset Recovery Unit	Nuix Pty Ltd	Nuix Web Review, Analytics, and Investigate	As above.	As above.	As above.	As above.	As above.	As above.	As above.	This is a stand-alone system, which is loaded with documents and other data lawfully obtained in relation to specific investigations (i.e., it does not interrogate 'all' data held by Police). Data is stored locally on Police servers.	As above.
Cellebrite	High Tech Crime Group	Cellebrite Asia Pacific Pte Ltd	Cellebrite UFED; Cellebrite Pathfinder; Cellebrite Physical Analyser	As above.	As above.	As above.	As above.	As above.	As above.	As above.	These are stand-alone systems, which extract data from lawfully obtained electronic devices and/or are loaded with data lawfully obtained in relation to specific investigations (i.e., they do not interrogate 'all' data held by Police). Data is stored locally on Police servers.	As above.
RPAS/drones	Response & Operations Group; Districts	All current New Zealand Police owned RPAS/drones are manufactured by DJI (Dai Jing Innovations). Third party RPAS/drone operators engaged from time to time to provide aerial photography services to Police may operate various brands of device. Police does not hold technical information about the specific platforms operated by service providers. Therefore, to the extent that information is sought about technology operated by external service providers, this part of the request is refused under section 18(g) of the Official Information Act.	DJI proprietary flight controllers (various depending on model)	Refused [s18(g)]. This is vendor-proprietary software purchased by Police 'off the shelf', and Police does not hold any information relating to secondary suppliers that may or may not contribute technology to the product.	Certain models of RPAS sold by DJI have the capability to use facial recognition technology to authenticate a user (pilot), in the same way that many smartphones do, and may also be capable of 'recognising' the authenticated user in flight, under certain conditions (such as being at very close range and optimal angle). Certain models are also marketed as being capable of 'object follow' or 'tracking' flight modes; however these modes are understood to utilise object movement detection based on colour contrast, and not facial recognition. NZ Police does not hold any information in respect of any embedded software which enables these technologies and this part of your request is therefore refused under section 18(g) of the Official Information Act. However, it may be helpful to add that other than user authentication, no NZ Police owned RPAS are understood to be capable of any other embedded or live facial recognition application. It may also be helpful to note that the only live video stream generated by the RPAS is that provided directly to the pilot via the flight controller. The flight controller link is direct point-to-point (aerial device to controller) via a closed, local Wi-Fi network created by the flight control unit and is not carried via satellite or any other wider network technology. The flight controller software is a DJI proprietary product and its live stream cannot be shared with any New Zealand Police platform or device capable of performing real-time facial recognition or otherwise analysing the video stream. While the proprietary flight controller software can be operated in a mode that enables onward streaming via a connected smartphone to various social media platforms, for a range of reasons including data and operational security New Zealand Police does not utilise these controller modes and therefore does not onward stream any RPAS/drone videostream. Hypothetically, still suspect images captured by an RPAS mounted camera could be downloaded from the device on return to base and (subject to image quality) later searched against Police photo collections for potential matches, in the same way as any other lawfully acquired suspect image may be and subject to the same policy and legislative controls; however this is not an inherent RPAS capability and nor is capturing suspect facial images a purpose for which NZ Police RPAS are deployed.	Refused [s18(e)]. No RFI/RFP/RFT or equivalent procurement documents exist, because all current RPAS/drones have been acquired at District or workgroup level as retail purchases of 'off the shelf' products. No formal procurement process was required due to the total acquisition cost, and limited/'niche' product market.	Refused [s18(e)]. No RFI/RFP/RFT or equivalent procurement documents exist, because all current RPAS/drones have been acquired at District or workgroup level as retail purchases of 'off the shelf' products. No formal procurement process was required due to the total acquisition cost, and limited/'niche' product market.	The potential future strategic role of RPAS as a component of air support is considered within a draft evaluation report entitled "Remotely Piloted Aircraft Systems (RPAS) Proof of Concept (POC) Evaluation Report (June 2020)". Because this is a draft report, and also contains commercially sensitive material, it is withheld pursuant to sections 9(2)(g)(i) and 9(2)(b) of the Official Information Act 1982: in order, respectively, to maintain the effective conduct of public affairs through the free and frank expression of opinions by or between or to Ministers of the Crown or members of an organisation or officers and employees of any public service agency or organisation in the course of their duty; and to protect information where the making available of the information would disclose a trade secret or would be likely unreasonably to prejudice the commercial position of the person who supplied or who is the subject of the information. However, it may be helpful to summarise the relevant content of the draft report as follows. The draft report considers small RPAS, of the kind currently operated by Police, provide a useful complement to the capability of the existing Eagle resource; while noting the RPAS are significantly less capable than Eagle. The chief advantages of RPAS were assessed as being relatively lower cost and relatively higher speed to deployment in response to a local requirement. Potentially valuable strategic uses of the technology, having regard to these pros and cons, were identified as being in low-cost aerial scene photography, complementary aerial observation in search or search and rescue operations, and to provide better situational awareness during operations. The report suggests that all Districts would benefit from having this capability in future. The report further speculates that in future, larger RPAS (such as fixed-wing aircraft) may be capable of performing additional tasks currently suited only to traditional air support, such as tracking of fleeing drivers; or could serve as aerial platforms for ANPR operations; but states that any such consideration would need to be the subject of a separate study. Similarly, the potential for 'micro-drones' to be further investigated as a tool to support safer execution of indoor tactical operations such as clearing a building. It may further be helpful to confirm that the draft report does not propose a future role for RPAS in general or routine aerial surveillance (i.e., as opposed to tactical situational awareness or reconnaissance in connection with a specific operation), nor as an aerial platform for identification of individuals via facial recognition or other means.	Police use of RPAS/drones is governed principally by the same Civil Aviation Act and Civil Aviation Rules as apply to other drone users, in particular Parts 101 and 102. Privacy Act provisions apply in all cases, and provisions of the Search and Surveillance Act may also apply depending on the particular deployment circumstances and purpose: for example, warrants are unlikely to be required for road crash scene photography but would be more likely to be required for crime scene photography and tactical operations such as execution of search or arrest warrants. The current Police Instructions on Remotely Piloted Aircraft Systems (RPAS) contain further information and are attached in response to your request.	Use of RPAS/drones is governed by normal operational approvals and management oversight, subject to compliance with CAA and other regulatory/legislative controls including the conditions of a surveillance device warrant (if applicable). Devices can only be operated by trained and authorised pilots. Images captured for evidential or other forensic purposes are subject to the same image integrity controls as other Police photography, including assignment of exhibit numbers, and ultimately may be subject to the scrutiny of the criminal justice process if relied on as evidence. The current Police Instructions on Remotely Piloted Aircraft Systems (RPAS) contain further information and are attached in response to your request.	Data is captured directly to a microSD card inside the RPAS/drone and physically transferred to local storage on Police devices after deployment. This data is handled in the same way as other Police forensic photography. Where aerial photography images are captured for Police by third party service operators, the image media (SD card) is immediately given to Police on retrieval of the drone, without any copies or cloud storage being made, and any flight controller cache must immediately be cleared. The current Police Instructions on Remotely Piloted Aircraft Systems (RPAS) contain further information and are attached in response to your request.	Refused [s18(e)]. These are 'off the shelf' stand-alone products, which do not have associated data services contracts.
ANPR (NZ Police in-vehicle and fixed location devices)	Road Policing; National Prevention Centre	Nautech Electronics Ltd	3M PAGIS and Back Office System Software (BOSS)	Refused [s18(g)]. This is vendor-proprietary software, and Police does not hold any information relating to secondary suppliers that may or may not contribute technology to the product.	Refused [s18(e)] as this information does not exist. Automatic number plate recognition does not involve facial recognition; it involves matching of text strings generated by optical character recognition software from license plate images. This string is accompanied by the vehicle/plate image from which it is derived, and associated time and location information. NZ Police ANPR units capture and process still images, not CCTV/video footage.	Refused [s18(e)]. Police's ANPR cameras have been acquired at various times, by individual Police districts, as additional 'one off' equipment purchases and/or acquired on a trial basis within the context of a pre-existing specialised emergency service vehicle equipment supplier relationship.	Refused [s18(e)]. Automatic number plate recognition is a conceptually simple process which is well established in the law enforcement context. The units were purchased from the supplier within an existing relationship and no specification of requirements was produced or necessary.	A number of documents which assess the current use of ANPR by Police and propose to update and rationalise governance and policy guidance currently exist in draft form. As these have not yet been finalised by relevant governance processes, they are withheld for the time being pursuant to section 9(2)(g)(i) of the Official Information Act 1982 in order to maintain the effective conduct of public affairs through the free and frank expression of opinions by or between officers and employees of any public service agency or organisation in the course of their duty. A document in support of this work was 'prepared for the consideration of the Organisational Capability Governance Group, entitled 'Automatic Number Plate Recognition Policy' (4 November 2020). This document is also withheld for the time being on the same grounds.	The Privacy Act 2020, New Zealand Police Code of Conduct and applicable policies apply generally. Search and Surveillance Act 2012 requirements may also apply depending on the circumstances. The New Zealand Police Instructions on Automatic Number Plate Recognition, and the associated 'Annex A: ANPR operations - approved deployment models', contain further information in respect of NZ Police ANPR deployment/use, and are attached in response to your request.	NZ Police operated ANPR cameras are deployed as part of planned District operations, and operated only by trained specialist staff. Use is therefore subject to standard operational review and managerial oversight processes. Data gathered auto deletes 48 hours after capture unless it is identified as being of specific evidential or investigative value and extracted from the system.	Data captured by the in-vehicle or fixed ANPR system is automatically compared in vehicle against the pre-loaded Vehicles of Interest number plate list. This list is principally comprised of the publicly available stolen vehicles list. The system generates real-time alerts to the system operator who can then manually alert the District Command Centre to determine any appropriate follow-up action such as tasking a Police unit to intercept the vehicle. The data captured during an in-vehicle deployment is then manually transferred from camera to local storage on return to base. All data is auto-deleted after 48 hours unless it is identified as being of specific evidential or investigative value and extracted from the system.	Refused [s18(e)]. This is a self-contained system, which does not have an associated data services contract.
ANPR 3rd party providers	National Prevention Centre	Auror Ltd and SaferCities (formerly Securegroup)	Auror; Vehicle Identification Broadcast Engine (VIBE)	Refused [s18(g)]. Police does not hold any information relating to secondary suppliers that may or may not contribute technology to vendor-proprietary software products. Retailers connected to VIBE may use a range of commercially available ANPR packages, however Police does not hold this information. VIBE only consumes standardised number plate information.	Refused [s18(e)]. ANPR, by definition, does not involve facial recognition. While 3rd party number plate information may be derived from CCTV systems or platforms which may or may not offer their commercial customers other image processing capabilities, only the number plate string is used by Police for ANPR matching against vehicles of interest (VOI). This string is accompanied by the vehicle/plate image from which it is derived and associated time and location information. To the extent that Police may hold information about other (non-ANPR) capabilities of 3rd party platforms, this information is withheld pursuant to section 9(2)(b)(ii), as its release would be likely unreasonably to prejudice the commercial position of the person who supplied or who is the subject of the information.	Refused [s18(e)]. New Zealand Police accesses the pre-existing commercial Auror retail crime prevention platform by agreement with Auror Ltd. No tender process was undertaken in respect of VIBE because the VIBE module was commissioned by Counties Manukau District as additional functionality for an existing proprietary software platform provided by Securegroup.	New Zealand Police accesses the pre-existing commercial Auror retail crime prevention platform by agreement with Auror Ltd and no requirements document exists. In respect of VIBE, a business case entitled 'Purchase of an Automatic Number Plate Recognition (ANPR) software database to receive ANPR data from existing 3rd party ANPR sites in the Counties Manukau District' was presented and approved at district level in June 2016. This document specifies the requirement sought to be acquired by engaging Securegroup to build an ANPR module (called the Vehicle Identification Broadcast Engine) onto its existing 3rd party CCTV aggregation platform. A copy of this document is attached in response to your request. Note that parts of this document have been redacted where the material contained does not relate to ANPR and is therefore outside the scope of your request, and for the reasons noted in the released document by reference to the relevant sections of the Official Information Act 1982.	As above.	The Privacy Act 2020, New Zealand Police Code of Conduct and applicable policies apply generally. Search and Surveillance Act 2012 requirements may also apply depending on the circumstances. VIBE generates automatic alerts to the system operator based on the uploaded Vehicles of Interest list (principally the publicly available stolen vehicle list), and the general legislative and policy framework described above applies. Access to more advanced ANPR search functions via the VIBE platform (for example, to try to locate a specific vehicle linked to a major crime or immediate threat to life) is governed by the same legislative framework (Privacy Act and Search and Surveillance Act), with additional policy, training and management controls. Only one member of New Zealand Police, holding the rank of Inspector, is currently able to initiate such ANPR searches. All searches are logged and auditable.	See response to question 9. Further, New Zealand Police's use of the Auror platform is subject to the terms of the access agreement. That agreement provides for audit of platform use (see clause 3(i)). While the content of this document is otherwise outside the scope of your request, as it has been previously released under the OIA, a copy of the agreement as previously released is attached for your information. Note that portions of this document have been redacted on the grounds provided by sections 6(c) and 9(2)(b)(ii) of the OIA.	Auror is a commercial product and not a New Zealand Police technology. Details of Auror Ltd's data storage arrangements are commercial to the company and to the extent that Police may hold this information it it withheld pursuant to section 9(2)(b)(ii), as its release would be likely unreasonably to prejudice the commercial position of the person who supplied or who is the subject of the information. VIBE data is aggregated and stored by SaferCities in New Zealand.	The response to question 11 also applies to this question. To the extent that New Zealand Police data is loaded to the Auror system, such as the publicly available stolen vehicle list (which is periodically uploaded), the agreement provides that Auror must not transfer Police data outside New Zealand except with the prior written consent of Police. Any transfer of Police data outside of New Zealand must be in accordance with the Privacy Act.
Body-worn cameras	Response & Operations (Equipment Capability); Evidence Based Policing Centre for research work	Refused s18(e). This information does not exist as Police has not procured this technology.	Refused s18(e). This information does not exist as Police has not procured this technology.	Refused s18(e). This information does not exist as Police has not procured this technology.	Refused s18(e). This information does not exist as Police has not procured this technology.	Refused s18(e). This information does not exist as Police has not specified a requirement for procurement of this capability.	Refused s18(e). This information does not exist as Police has not specified a requirement for procurement of this capability. Some high-level scoping of possible requirements associated with the potential acquisition of body-worn camera technology in the context of the Taser program has been done, and is contained in the documents provided in response to question 8 of this request.	See attached documents: - Police Executive Meeting paper PEM/13/78 (September 2013) on 'Taser Camera Systems' [redacted] - Initial concept paper CP00034 'On Body Camera Proof of Concept' (December 2014) [redacted] - 'Taser 7 and Associated Technology Briefing' (December 2018) [redacted] - ANZPAA briefing paper for 'Agenda Item - Body Worn Cameras' (November 2018) [redacted]	The Police Instructions on "Police filming and audio recording of operations and events" outline the legislative framework governing any possible use of body worn cameras. These instructions are attached in response to your request.	Refused s18(e). This information does not exist as Police has not procured this technology.	Refused s18(e). This information does not exist as Police has not procured this technology.	Refused s18(e). This information does not exist as Police has not procured this technology.
Digital Information Management	Information and Communication Technology Service Centre	Refused s18(e). This information does not exist as Police has not procured this technology.	Refused s18(e). This information does not exist as Police has not procured this technology.	Refused s18(e). This information does not exist as Police has not procured this technology.	Refused s18(e). This information does not exist as Police has not procured this technology.	A Market Research RFI was released via the publicly accessible Government Electronic Tenders Service (GETS) website on 2 July 2020. This RFI was designed to gather information about 'off the shelf' products available in the market, to inform further consideration of whether to proceed to development of a procurement proposal. A copy of the RFI document is attached in response to your request.	Potential requirements of a Digital Information Management solution were scoped, on a 'blue sky thinking' basis, in 2019 to provide a basis for the Market Research RFI. A document capturing those potential requirements was produced, entitled 'Digital Information Management Requirements' (dated Oct/Nov 2019). Those requirements were distilled into the requirements that were taken to market in the RFI. The initial requirements scoped were not confirmed business needs, but rather were designed to establish parameters to test the market. It was expected that market responses to the RFI, refined by further analysis of Police requirements, would inform development of a final requirements specification for any subsequent procurement proposal. As no decision has been made to proceed beyond the July 2020 RFI, a requirements specification for procurement has not yet been developed. Release of the potential/'draft' detailed requirements at this time would therefore have significant potential to compromise any potential future procurement process. The document 'Digital Information Management Requirements' (dated Oct/Nov 2019) is therefore withheld on the grounds provided by sections 9(2)(b)(ii) and 9(2)(g)(i) of the Official Information Act 1982: that release would be likely unreasonably to prejudice the commercial position of the person who supplied or who is the subject of the information; and in order to maintain the effective conduct of public affairs through the free and frank expression of opinions by or between officers and employees of any public service agency or organisation in the course of their duty. However, it may be helpful given your interest in the topic to confirm to you that this document does not contain any reference to facial recognition technology, and nor was facial recognition scoped as a potential or draft requirement.	The Market Research RFI, in effect, represents the near future strategic requirement, and is provided in response to this request. See in particular the diagram at paragraph 2.2.22 of that document. To the extent that the 'Digital Information Management Requirements' contains additional information of a similar but more detailed nature, this is withheld pursuant to sections 9(2)(b)(ii) and 9(2)(g)(i) of the Official Information Act 1982, for the reasons explained in response to question 7 of this request.	Refused s18(e). This information does not exist as Police has not procured this technology. However, it may be helpful to refer to paragraph 2.2.20 of the RFI for an overview of legislation that would be expected to be relevant to a Digital Information Management solution.	Refused s18(e). This information does not exist as Police has not procured this technology.	Refused s18(e). This information does not exist as Police has not procured this technology.	Refused s18(e). This information does not exist as Police has not procured this technology.