NEW ZEALAND
POLICE
Ngā Pirihimana o Aotearoa

27 May 2021

Phil Pennington
phil.pennington@rnz.co.nz
02102362890

Dear Phil

REQUEST FOR INFORMATION –REFERENCE: 01-21-14416

Thank you for your initial email request dated 4 May 2021 in which you requested:

"This OIA relates to NZP's approach to facial recognition and social media search or tracking tools or similar tools, noting NZP's stated desire to be open with the public about this.

Pls consider this request to cover any actual use of hi-tech tool/s involving the following suppliers/contractors by NZP or its employees or agents - but also extending to any trial of the technologies, and/or any consideration given to trialling them or using them RNZ requests NZP advise if NZP has a record since the start of 2019 of any use, or trial, or ongoing use or trial, of FR or socmed tools from the following entities, per entity (eg iFace – 'no', Clarifai – 'yes'); and where there is a record of this occurring, pls detail what tool is called, and how it is being used or trialled:

In facial recognition:

1. *iFace*
2. *Clarifai, including but not limited to Face Detection Model*
3. *Microsoft Azure, including but not limited to Azure Face and Azure Detect*
4. *Realnetworks*
5. *Idemia FACES*
6. *Ntech Labs*
7. *Safran Identity & Security*
8. *Megvii, including but not limited to Face++ or Face*
9. *Amazon Rekognition*
10. *Papillon*
11. *Thales LFIS and/or FRP Watch and/or FRP Verify and/or FRP Search expert and/or FRP SDK and/or FRP Mobile*
12. *SenseTime*

13. Cloudwalk Technology

In social media investigation / tracking:

1. Dataminr, including but not limited to First Alert
2. DataSift
3. Cobwebs Technologies
4. Palantir Gotham
5. Social Sentinel
6. DigitalStakeout
7. Babel Street, including but not limited to Babel X and/or Babel Box and/or Locate X
8. GeoDASH, including but not limited to Automated Policing System
9. Venntel
10. Factual / Foursquare"

I have considered your request in accordance with the Official Information Act 1982 (OIA).

Police undertake thousands of serious crime investigations each year that utilise a range of surveillance methodologies, techniques, equipment and people. These would include cases such as homicide, robberies, on-line exploitation of children, drug dealing and matters of national security to name but a few.

It is important that police on behalf of the community protect their methods as much as possible to ensure that criminals do not use publicly released information to hinder or defeat police investigations. Providing any such information to criminals would only harm the community and the public interest.

Between 2018 and 2020 the Cybercrime Unit had access to a social media tool that searched accessible and open source internet pages, for the purpose of assisting investigations.

Further details about this tool have been withheld pursuant to section 6(c) of the OIA, as the making available of the information is likely to prejudice the maintenance of law, including the prevention, investigation, and detection of offences and right to a fair trial.

In 2019 Police entered into an arrangement with a data analytics provider for the purpose of assisting the Operation Deans and Operation Whakahaumanu response to the March 15 terrorist attack. It was also used to provide Police responses to the Royal Commission of Inquiry into the terrorist attack on Christchurch masjidain.

Further details about this tool have been withheld pursuant to section 6(c) of the OIA; that the making available of the information is likely to prejudice the maintenance of law, including the prevention, investigation, and detection of offences and right to a fair trial.

Also post March 15, 2019, the National Intelligence Centre introduced software that searches accessible and open source internet pages including social media.

Open Source Intelligence (OSINT) collection is a term that is widely used internationally and within New Zealand Police.. Within Police it is used to describe information derived from publicly available online sources.

This tool is used by the OSINT team and Cybercrime Unit to collect information from online open sources to assist with investigations or support intelligence reports.

The OSINT team focuses on collections in line with national intelligence requirements such as public and staff safety priorities. The team provides support to intelligence and investigations groups across Police.

The OSINT support includes the collection of online publicly available information to assist with investigations and major events, as well as training and skills uplift for other Police Intelligence professionals.

The tool has been used by Police since November 2019.

Further details about this tool have been withheld pursuant to section 6(c) of the OIA; as the making available of the information is likely to prejudice the maintenance of law, including the prevention, investigation, and detection of offences and right to a fair trial.

In regard to your request to a yes / no answer to the list provided above, this part of your request is refused pursuant to section 6(c) of the OIA, as the making available of the information is likely to prejudice the maintenance of law, including the prevention, investigation, and detection of offences and right to a fair trial.

Police have disclosed some other tools in previous similar requests, as follows:

Signal is used by the National Command & Coordination Centre and to varying degrees across Police Districts. It is also used by teams in the National Intelligence Centre, including the OSINT team.

All three areas use Signal to surface social media posts as well as to identify trend information relating to public safety and criminal events

The Police Media and Communications team is currently considering the use of a social media tool, Zavy. The tool will allow the Marketing and Brand team to better understand the sentiment (tone) of the comments and engagements of posts on the official New Zealand Police social media pages. Understanding how our social media posts perform will help us understand what messages resonate with our followers.

Sprout Social is used is used by Police Media & Communications to show engagement and performance of online social media posts made by New Zealand Police on its own official social media pages.

Another tool, that allows for understanding attitudes, opinions, and general sentiment (through online channels – not just official New Zealand Police social media pages) is also being considered.

Maltego is used by Police Cybercrime Unit to query open source data and visualise it in graph form. It is particularly useful in mapping internet infrastructure.

Feedly is deployed by the OSINT team, and the Cybercrime Unit, who may decide to use it to collect information from online open source to assist with an investigation or support an intelligence report. The social media surveillance tool, searches exclusively across publicly available information and does not intercept communication or track individuals.

Please also note that the New Zealand Police will be proactively releasing its technology stocktake on the Police website in the next 4 weeks

If you are not satisfied with the response to your request, you have the right to refer the matter to the Ombudsman.

Yours sincerely

Detective Senior Sergeant Greg Dalziel
High Tech Crime Group
Police National Headquarters