

3 September 2024

IR-01-24-25448

James B

fyi-request-27731-4601a7eb@requests.fyi.org.nz

Tēnā koe James

Thank you for your Official Information Act 1982 (OIA) request of 21 July 2024 in which you requested information related to CommunityCam.

- 1) *The responses in IR1 indicate knowledge of CommunityCams privacy (2) and data storage policies (1) as of 06/09/21. Was NZ Police aware of a PIA/review being conducted by CommunityCam before 22 August 2022?*
 - a) *When did NZ Police become aware of the information provided in IR1?*
 - b) *Please provide information on how NZ Police came to the conclusion it did in IR1 when IR2 stated it held no information about the privacy policies or NZ Police's use of the site.*
 - c) *Please provide correspondence, memos, or other documentation regarding the privacy policies of <http://www.communitycam.co.nz/> and Police's use of the site as was available before 22/08/22.*
 - d) *Separately, please provide correspondence, memos, or other documentation regarding the privacy policies of <http://www.communitycam.co.nz/> and Police's use of the site after 22/08/22.*
 - e) *Has NZ Police completed a PIA for its use of CommunityCam? If so, please provide a copy and the date of initiation, completion, and scheduled review. If not, has NZ Police considered completing a PIA?*
 - f) *Please provide all documentation for the agreement of "Anton Maisey" to verify the confidentiality of CCTV footage uploaded to the site, as noted in the site FAQ under heading "Are NZ Police really the only ones who see my details?"*
 - g) *Please provide all information about the Police login page available at <https://www.communitycam.co.nz/police-login.cfm>, and the number of times it has been accessed if that information is available.*
 - h) *Please provide any MOU or similar contract NZ Police has with CommunityCam, if available.*

My response to each part of your request can be found below.

1. *The responses in IR1 indicate knowledge of CommunityCams privacy (2) and data storage policies (1) as of 06/09/21. Was NZ Police aware of a PIA/review being conducted by CommunityCam before 22 August 2022?*

No, and Police is not aware of one being conducted since.

- a) *When did NZ Police become aware of the information provided in IR1?*

Police National Headquarters

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

Police has held informal discussions with the website developer and owner on a number of occasions since the development of the website. This information was part of those discussions.

b) Please provide information on how NZ Police came to the conclusion it did in IR1 when IR2 stated it held no information about the privacy policies or NZ Police's use of the site.

I refer you to my answer in 1a).

c) Please provide correspondence, memos, or other documentation regarding the privacy policies of <http://www.communitycam.co.nz/> and Police's use of the site as was available before 22/08/22.

Two documents have been found within scope of your request. In 2021, Police completed a Technology Proposal Document and a New Technology Policy Risk Assessment. The purpose of these documents was to identify any risks and determine whether the continued use of CommunityCam would pose any issues to Police.

The Technology Proposal Document has been attached to this letter, and contains two redactions, under section 9(2)(a) of the OIA to protect the privacy of natural persons and section 9(2)(j) of the OIA to enable a Minister, department or organisation holding information to carry out commercial activities or negotiations.

Principle 5 of the New Technology Policy Risk Assessment has also been found within scope of your request. This part of the document has been extracted and can be found on the final page of the attached documentation.

One email has also been found within scope of your request and has been collated and attached as part of the two other identified documents. Please note that the email refers to the Technology Proposal Document which has been attached to this letter. Please note that there is a redaction under section 9(2)(a) of the OIA to protect the privacy of natural persons.

d) Separately, please provide correspondence, memos, or other documentation regarding the privacy policies of <http://www.communitycam.co.nz/> and Police's use of the site after 22/08/22.

There are no identified privacy policies found on CommunityCam's website, and thus no such correspondence, memos, or other documentation exists. Therefore, this part of your request has been refused under section 18(e) of the OIA as the information requested does not exist.

e) Has NZ Police completed a PIA for its use of CommunityCam? If so, please provide a copy and the date of initiation, completion, and scheduled review. If not, has NZ Police considered completing a PIA?

Police has not completed a PIA for CommunityCam. It was determined that because the technology is operated externally to Police, and that from the Police perspective there were no changes to the way that CCTV evidence is used (just a change in how it is collected from voluntary providers), there were no new privacy concerns, and a PIA was unnecessary.

Please note that Police do not 'own' CommunityCam and so it would be CommunityCam's obligation to complete a PIA rather than Police.

f) Please provide all documentation for the agreement of "Anton Maisey" to verify the confidentiality of CCTV footage uploaded to the site, as noted in the site FAQ under heading "Are NZ Police really the only ones who see my details?".

Anton's role with CommunityCam was to coordinate with the developer and assist getting the site approved by Police. Anton does not have any more access rights to the site than any other police officer. Anton still needs to enter the required pin code / password that would be required to access CCTV footage and then this is only made available to the requesting officer.

g) Please provide all information about the Police login page available at <https://www.communitycam.co.nz/police-login.cfm>, and the number of times it has been accessed if that information is available.

Police members are required to log on to this page using their own Police email address and individual password. Police login can only be accessed from a Police device. Police cannot log on from their home or external computers.

The number of times this is accessed is not captured, therefore, this part of your request has been refused under section 18(g) of the OIA as this information is not held.

h) Please provide any MOU or similar contract NZ Police has with CommunityCam, if available.

There is no MOU or similar contract between Police and CommunityCam, therefore this part of your request has been refused under section 18(e) of the OIA as the information requested does not exist.

For further information on how CommunityCam and Police interact, please contact Inspector Brett Callander at brett.callander@police.govt.nz who will be more than happy to show you how the CommunityCam website works from a Police perspective as well as the measures that are in place to ensure the privacy of the information that members of the public upload to the site.

You have the right, under section 28(3) of the OIA to ask the Ombudsman to review my decision if you are not satisfied with the way I have responded to your request. Information about how to make a complaint is available at: www.ombudsman.parliament.nz.

Nāku noa, nā



Phillip Taikato
Director Māori and Community Prevention Partnerships
New Zealand Police

Technology Proposal Document

Your name, role, contact details

Brett Callander

Manager Mental Health and Community Services

Community Partnership and Prevention

Iwi and Community

s.9(2)(a)

E Brett.Callander@police.govt.nz

Name of technology

Community Cam

Technology Description

What is the technology and how does it work? This should include an overview of the technical functionality, including a description of data sources where relevant. If the technology mainly relies on an algorithm to analyse data (e.g. to assess risk, make decisions, or produce recommendations for staff action) this should be specifically noted.

This technology creates a reporting system and receptacle for CCTV camera footage to be electronically shared between members of the public and NZ Police. The Community Cam website holds contact details (name, address, phone number) of those who have registered with them.

Community Cam allows members of the public to register their home / business CCTV cameras with Community Cam. Once their CCTV camera is registered those people can upload footage to Community Cam after reporting an incident to 105 / 111. They need to attach either an event number or a file number to their upload. Police staff can then go into Community Cam and download the footage straight onto a Police device without having to (1) arrange a time to meet the person holding the footage, (2) travel to the location of the CCTV camera base unit, and (3) either provide the appropriate data storage device or take one from the member of the public providing the footage.

Another Police use for Community Cam is the ability for Police to see what addresses have been registered with Community Cam and seek potential evidential footage from those cameras for relevant times/dates. Contact could be made, electronically, with a group of potential holders of evidence and the evidence collected without the officer leaving the station.

Necessity

What do Police need to be able to do (or do significantly better), that they can't do now? What existing policing capability gap is the technology intended to bridge? This should be a brief statement that describes an existing policing challenge or shortfall: for example, in meeting a public interest in, or expectation of, service delivery or harm prevention in a specific area.

As discussed above, this application will allow members of the public to provide Police with CCTV footage of potential incidents / crimes and faster access for Police to retrieve and view that footage.

Use case

What is the technology proposed to be used for? This should be a description of the specific purpose, or kinds of situations in which the technology is intended to be used (such as types of crime being investigated, or operational situations where the technology would be employed). This should include an outline of the proposed 'end state' deployment of the technology, as envisaged if a trial is successful.

Storage of evidential CCTV footage and then electronic collection of that footage by Police staff for any/all crime types. The footage may end up being used in court hearings.

Controls

How it is proposed to ensure that the technology is not used beyond its intended use case? This could include, for example, policy guidance, legislative or regulatory guidance, approvals processes, reporting and audits.

The developer of the website has put in place a number of safeguards;

- Members of the public must register to use the application
- Entry to the site requires both an email address and password to access
- Password protection that only allows registered Police staff access to the footage
- A 20-digit password that must be produced prior to Police staff downloading the footage

Proportionality

Can the proposed solution be justified against the impact on people's privacy or other rights/expectations of fairness (e.g. use of their data, surveillance of lawful activity, perceived 'targeting'); and in terms of the likely initial and ongoing financial/resourcing costs to Police (to the extent the approximate scale of such costs may be known)? Briefly describe any such impacts and costs and how they are justified, having regard to the above (necessity, use case, controls). Reference to the Principles below may help identify possible impacts.

Members of the public that register their cameras with Community Cam are doing so to provide Police with evidential footage when available. Further work needs to be done with the developer to ensure that processes are in place for Police staff to comply with all relevant privacy principles

Trial and evaluation proposal

What are the parameters for the proposed trial (for example, how many users/devices, in what locations, and for how long) and how is the trial is proposed to be evaluated? This should include a description of how the trial will be determined to be a success.

This application is already currently in use in Counties Manukau. There are around 265 CCTV cameras registered with Community Cam however when I accessed it today there were only 4 lots of footage uploaded.

How will the technology be funded?

Will this be funded within the Business Owner's allocated funding; or will this require an Investment Proposal through to Business Case? Advise options for the testing/trialling stage, and, should the technology be implemented, consider ongoing costs to maintain the technology.

s.9(2)(j) OIA

out of scope

Principle 5: Privacy

The technology incorporates privacy by design in data sourcing, use, retention and storage.

While the website provides access for Police to see what addresses have been registered as having CCTV, this information is not available to community members.

By registering on the site and uploading footage, users provide their consent for Police to access it.

There is an opportunity to improve the current process that is used for the storage of CCTV footage that is retrieved from Community Cam. Consideration needs to be given to the life cycle management of the footage and where it should be stored in the longer term (For example this could include software such as Evidence.com, which includes redaction tools).

Long-term data storage solutions and protocols have not yet been confirmed. In future, a data storage policy could be developed in conjunction to develop a more consistent approach to the storage of CCTV footage throughout the organisation. There is also a need for data retention protocols.

Privacy impacts have been considered and identified privacy risks mitigated.

No PIA has been undertaken. It was determined that it was unnecessary, given that the technology is operated externally and the change in practice does not give rise to new privacy concerns.

Automating the existing process could make it easier for unauthorised use of CCTV footage for personal reasons. It is recommended that Police audits suitable use of footage.

From: CALLANDER, Brett <Brett.Callander@police.govt.nz>
Sent: Wednesday, 21 July 2021 2:00 pm
To: GILMORE, Carla <Carla.Gilmore@police.govt.nz>
Cc: REGISTER, Brent <Brent.Register@police.govt.nz>
Subject: RE: Crime Prevention cameras CCTV in public

Hi Carla

Here is my attempt. Happy to add more or discuss if required.

Regards

Brett

From: GILMORE, Carla <Carla.Gilmore@police.govt.nz>
Sent: Wednesday, July 21, 2021 10:25 AM
To: CALLANDER, Brett <Brett.Callander@police.govt.nz>
Subject: RE: Crime Prevention cameras CCTV in public

Hi Brett,

Complete the attached proposal document. Just use the info that you have to hand – I'm not expecting you to go on an information and fact finding hunt since I have a reasonable knowledge of its use already. Then send it back to me. The attached principles are what underpin our decision making and compliance with the new technology policy.

From there it goes to the Emergent Tech working group which comprises of SME's for Security, Legal, Privacy, ICT, Risk and Assurance and we complete any required assessments (privacy, security, policy). Then the assessments with a cover page go off to Security Privacy Reference Group (SPRG) with recommendations.

Get in touch if you need any help.

Cheers,

Carla

Carla Gilmore
Inspector
National Lead : Emergent Technologies
S.9(2)(a) OIA
E carla.gilmore@police.govt.nz
