

Our Ref: IM-FOI-2015-1186



Sir Stephen House QPM
Chief Constable

FREEDOM OF INFORMATION (SCOTLAND) ACT 2002

I refer to your recent request for information which has been handled in accordance with the Freedom of Information (Scotland) Act 2002.

In your request you asked:

Part one:

As raised in the Department of Health case (EA/2008/0018), it is important that the public have the opportunity to scrutinise procurement decisions, “showing who public money is being spent on a particular service or good, and how the supplier arrived at the price that is being charged.”

Furthermore, according to the Information Commissioner’s Guidelines, the public interest is served where access to the information would: “further the understanding of, and participation in the debate of issues of the day; facilitate the accountability and transparency of public authorities for decisions taken by them; facilitate accountability and transparency in the spending of public money; allow individuals to understand decisions made by public authorities affecting their lives and, in some cases, assist individuals in challenging those decisions; bring to light information affecting public security.”

In light of this, I would like to request the following:

- **From 1st January 2005, to the day this request is processed, contracts and purchase orders that contain the words: “IMSI catcher”, “cell site simulator”, “virtual base transceiver stations”, “mobile phone jammer”, or similar mobile phone surveillance and tracking devices held by Police Scotland.**
- **And all associated documents. I would expect this to include, but not limited to, any schedules, annexes, appendices, or other documents attached.**

Part two:

- **From 1st January 2005, to the day this request is processed, contracts and purchase orders between Police Scotland and the following companies: Datong plc, Cellxion, and Seven Technologies Group.**
- **And all associated documents. I would expect this to include, but not limited to, any schedules, annexes, appendices, or other documents attached.**

Part three:

I would also like the following information:

- **The number of times Police Scotland have used, or at least gained permission to use, “IMSI catchers”, “cell site simulators”, “virtual base transceiver stations”, “mobile phone jammers” or similar mobile phone surveillance and tracking devices. I would like a breakdown for the years 2015, 2014, 2013, 2012, 2011 and 2010.**

In terms of Section 18 of the Freedom of Information (Scotland) Act 2002 (the Act) Police Scotland can neither confirm nor deny that it holds the information requested by you. If held, the information would be considered exempt in terms of the following exemptions:

Section 31(1) – National security

Section 34(1) – Investigations and proceedings conducted by public authorities

Section 35(1) – Law enforcement

Any disclosure under FOISA is a disclosure to the world at large, and confirming or denying the use of specialist techniques which may or may not exist, and which (should they exist) Police Scotland may or may not deploy in specific circumstances would prejudice law enforcement. If the requested information were held by Police Scotland, confirmation of this fact would reveal that the Service has access to sophisticated communications analysis techniques. This would be damaging as it would:

- (i) limit operational capabilities as criminals/terrorists would gain a greater understanding of the police's methods and techniques, enabling them to take steps to counter them; and
- (ii) provide an indication to any individual who may be undertaking criminal/terrorist activities that the police service may be aware of their presence and taking counter terrorist measures.

Conversely, if Police Scotland confirmed that no information were held, this would reveal to those same individuals that their activities are unlikely to have been detected by the police. It may also suggest (whether correctly or not) the limitations of police capabilities in this area, which may further encourage criminal/terrorist activity by exposing a potential vulnerability. Disclosure of the information could confirm to those involved in criminality or terrorism that they are or have been the subject of such activity, allowing them to gauge the frequency of its use and to take measures to circumvent its use. Any compromise of, or reduction in technical capability by Police Scotland would substantially prejudice the ability of the Service to police their area, which would lead to a greater risk to the public.

This detrimental effect is increased if the request is made to several different law enforcement bodies. In addition to the local criminal fraternity now being better informed, those intent on organised crime throughout the UK will be able to ‘map’ where the use of certain tactics are or are not deployed. This can be useful information to those committing crimes of drugs and terrorist activities.

For example, to state that no information is held in one area and then exempt information held in another, would itself provide acknowledgement that the technique has been used at that second location. This could have the likelihood of identifying location-specific operations, enabling individuals to become aware of whether their activities have been detected. This in turn could lead to them moving their operations, destroying evidence, or avoiding those areas, ultimately compromising police tactics, operations and future prosecutions.

Any information identifying the focus of policing activity could be used to the advantage of terrorists or criminal organisations. Information that undermines the operational integrity of these activities will adversely affect public safety and have a negative impact on both national security and law enforcement.

Factors favouring confirming or denying whether any other information is held for Section 31 (National Security):

The public is entitled to know where their public funds are being spent and a better informed public can take steps to protect themselves.

Factors against confirming or denying whether any other information is held for Section 31:

By confirming or denying the use of specialist techniques could render security measures less effective. This could lead to the compromise of ongoing or future operations to protect the security or infrastructure of the UK and increase the risk of harm to the public.

Factors favouring confirming or denying whether any other information is held for Section 34 (Investigations):

The public are entitled to know what their public funds are spent on. Investigations may be closed and any proceedings may have been completed, and the investigations may have been high profile and had national implications.

Factors against confirming or denying whether any other information is held for Section 34:

By confirming or denying the use of specialist techniques, Police Scotland's future law enforcement capabilities would be affected and this would hinder the prevention and detection of crime.

Factors favouring confirming or denying whether any other information is held for Section 35 (Law Enforcement):

Better awareness may reduce crime or lead to more information from the public, and the public would be able to take steps to protect themselves. Some information is already in the public domain.

Factors against confirming or denying whether any other information is held for Section 35:

By confirming or denying whether such techniques were used would compromise law enforcement tactics and undermine the partnership approach which would hinder the prevention or detection of crime. This would impact on police resources, more crime would then be committed and individuals placed at risk.

Balance test:

The security of the country is of paramount importance and Police Scotland will not divulge whether information is or is not held if to do so could undermine national security or compromise law enforcement. Whilst there is a public interest in the transparency of policing operations and in this case providing assurance that the police service is appropriately and effectively engaging with the threat posed by the criminal fraternity, there

is a very strong public interest in safeguarding both national security and the integrity of police investigations and operations in this area.

As much as there is public interest in knowing that policing activity is appropriate and balanced in matters of national security this will only be overridden in exceptional circumstances.

There is also no requirement to satisfy any public concern over the legality of police operations and the tactics we may or may not use. Forces are already held to account by statute, for example the Criminal Procedure (Scotland) Act 1995 and the Regulation of Investigatory Powers Act and independent bodies such as Her Majesty's Inspectorate of Constabulary in Scotland, the Police Investigations and Review Commissioner and the Office of the Surveillance Commissioner. Our accountability is therefore not enhanced by confirming or denying whether any information is held.

Therefore it is my opinion that for these issues the balancing test for confirming or denying whether any information is held regarding these techniques is not made out. This argument is obviously transferable to all police tactics.

None of the above can be viewed as an inference that the information you seek does or does not exist.

Should you require any further assistance concerning this matter please contact me directly on 0131 311 3901 quoting the reference number given.

If you are not satisfied with the way in which your request has been dealt with, you are entitled in the first instance, and within 40 working days of receiving this response, to request a review of the decision. Should you wish to do so, contact details are; FOI Central Processing Unit, Police Scotland, Clyde Gateway, 2 French Street, Dalmarnock, G40 4EH - foi@scotland.pnn.police.uk

If you remain dissatisfied following the outcome of that review, you are thereafter entitled to apply to the Scottish Information Commissioner within six months for a decision. Contact details are; Office of the Scottish Information Commissioner, Kinburn Castle, Doubledykes Road, St Andrews, Fife, KY16 9DS - enquiries@itspublicknowledge.info

Should you wish to appeal against the Scottish Information Commissioner's decision, there is an appeal to the Court of Session on a point of law only.

Yours sincerely,

Gabriella Trybalska
Information Management