Legal Officer,
Privacy International,
62 Britton Street,
LONDON.
EC1M 5UY.
Our Ref: AC/Alr

13th July 2017

Dear Sir / Madam,

Appeal re Freedom of Information Request Reference No: AC/AR – 2016-126 Request for an Internal Review

I write with reference to your request for an internal review dated 22 May 2017 following the Office of the Police and Crime Commissioner (OPCC) response to your freedom of information request dated 1 November 2016. Please find attached a report that has been completed by Warwickshire Legal Services (WLS) setting out the findings of the internal review that they have conducted on the OPCC's behalf.

The OPCC acknowledges that there has been a short delay in responding to Privacy International, however, we are aware that WLS has kept you informed and apologised for the delay. For the reasons set out in the report, the OPCC does not uphold your appeal, except in relation to one aspect of the fourth part of your request. If you are not satisfied with the outcome of the internal review you may appeal to the Information Commissioner's Office, at the following address:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Tel. 0303 123 1113
www.ico.org.uk

Yours sincerely,

Chief Executive
West Mercia Police & Crime Commissioner
Enc.

Internal Review Report – Freedom of Information Act 2000

Organisation: **West Mercia Office of the Police and Crime Commissioner ("the OPCC")**

Name of Requestor: **Mr Matthew Rice (request for Internal Review from Ms Scarlet Kim on behalf of Mr Rice)**

I have been instructed by the OPCC to undertake an internal review of the decision of the OPCC to not release information to Mr Rice following his request of 1st November 2016.

In undertaking this review, I have considered the request for information received on 1st November 2016, the OPCC's response of 20th December 2016 and the request for an internal review of 22nd May 2017. I have also viewed the information withheld by the OPCC, as well as the guidance on the following from the Information Commissioner's Office ("the ICO") as follows:

- Security Bodies (Section 23)
- Safeguarding National Security (Section 24)
- How Sections 23 and 24 Interact
- Law Enforcement (Section 31)
- Information in the Public Domain

How the request was dealt with

The OPCC received the request from Mr Rice on 1st November 2016. The request was for the following:

- Records relating to the purchase of "existing" Covert Communications Data Capture ("CCDC") equipment, referred to in a released copy of Alliance Government Group minutes, including purchase orders, invoices, contracts, loan agreements, solicitation letters, correspondence with companies and other similar records.
- Records relating to the purchase of replacement CCDC equipment, referred to in the Alliance Government Group minutes, including purchase orders, invoices, contracts, loan agreements, solicitation letters, correspondence with companies and other similar records.
- Records relating to the decision "to replace the existing CCDC equipment with a new supplier", referred to in the Alliance Government Group minutes, including any records referred to or consulted in reaching that decision.
- Legislation, codes of practice, policy statements, guides, manuals, memoranda, presentations, training materials or other records governing the use of CCDC equipment by Warwickshire Police, including restrictions on when, where, how, and against whom it may be used, limitations on retention and use of collected data, guidance on when a warrant or other legal process must be obtained, and rules governing when the existence and use of CCDC equipment may be revealed to the public, criminal defendants, or judges.

The response, sent out on 20th December 2016, made clear that in relation to the first three queries a Business Case document was held but nothing else, and that disclosure of the Business Case was exempt under section 24(1) and sections 31(a) & (b) of the Freedom of Information Act 2000 ("the Act"), on the grounds that (a) the document is a confidential strategic papers produced to evaluate the functionality and options in respect of existing and replacement CCDC equipment, and if disclosed would undermine national security; and (b) the disclosure of the document would prejudice the methods and strategies deployed or considered by the OPCC in relation to the prevention and detection of crime and the apprehension or prosecution of offenders. The response also went in some detail on the public interest test but considered that, on balance, the public interest in maintain national security and the prevention and detection of crime outweighed, in relation to release of this document, the public interest in how public funds are spent, whether measures in place to safeguarding national security are effective, and in ensuring that transparency exists and public bodies are held to account.

With regard to the final part of the request, s23(5) was utilised and therefore the existence of documentation was neither confirmed nor denied.

Analysis of Response

I note that the requests made were responded to, although extra time was required in order to deal with the public interest points raised, and that a letter was sent to explain this, ensuring that the legislation was complied with on this point.

The response did deal with all the requests, albeit that the only information actually revealed was that all the OPCC possessed was a copy of the Business Case. A thorough analysis is provided on the public interest point, although not in regard to why either national security or crime prevention / detection would be put at risk as a result of release of information.

Use of s23(5) allows for very little reasoning to be given as to why it is being used, other than to note that it is an absolute exemption.

Scope of this Internal Review

In relation to the first, second and third parts of the request, the request for an internal review focuses on two issues:

- That there must be a clear basis for arguing that disclosure would have an adverse effect on national security and that insufficient justification has been provided for utilising the exemption; and
- That the public interest balancing exercise falls in favour of disclosure.

In relation to the fourth part of the request, the concerns raised were that:

- Confirmation or denial of the existence of legislation, codes of practice, policy statements etc. would not reveal operationally sensitive information;
- There is a failure to have regard or give adequate weight to the fact that material is already in the public realm, that there is significant public interest in the area,

and that legislative provisions and/or policy guidance cannot conceivably fall within any exemption; and

- There has to be a realistic possibility that a security body would be involved in the issue for the exemption to apply.

Review of First, Second and Third Parts

National Security

Section 24(1) of the Freedom of Information Act 2000 states that "Information which does not fall within section 23(1) is exempt information if exemption from section 1(1)(b) is required for the purpose of safeguarding national security". As the request for the internal review makes clear, the words "required for the purpose of" are indeed critical when considering whether this exemption applies. The Information Commissioner's guidance on use of the exemption states as follows:

"The exemption applies where withholding the information is "required for the purposes of safeguarding national security". Required is taken to mean that the use of the exemption is reasonably necessary. "Required" is defined by the Oxford English Dictionary as 'to need something for a purpose' which could suggest the exemption can only be applied if it is absolutely necessary to do so to protect national security. However the Commissioner's interpretation is informed by the approach taken in the European Court of Human Rights where interference to human rights can be justified where it is 'necessary' in a democratic society for safeguarding national security. 'Necessary' in this context is taken to mean something less than absolutely essential but more than simply being useful or desirable, so we interpret 'required', in this context, as meaning 'reasonably necessary'."

Guidance from the Information Commissioner makes clear that this does not mean that there has to be a clear direct link to a specific threat to national security and neither does there have to be any evidence of an imminent terrorist attack happening as a result of releasing the information.

There is also a clear balancing exercise which needs to be taken between the public interest in open and transparent policing and avoiding unfettered surveillance, and also the public interest in being protected from terrorist and other national security threats. As the ICO states: "*The public are more likely to cooperate with security measures if they understand the need for them and, again, are satisfied that they are proportionate to the risks they are seeking to address. The public also have a natural concern that the measures in place to safeguard national security are effective*".

Conclusions

It is a difficult task to balance these issues, but having given this some considerable analysis my conclusion is that giving the public access to a document analysing both current and potential future CCPC capabilities and operational uses would raise a significant risk that it would both be seen by those who pose a threat to national security and would then be utilised to the detriment of the safety and security of British citizens.

Going into detail on why the exemption is required for national security purposes is impractical without releasing details of the information itself in order to explain. It is therefore not possible to say more than the analysis of the current system in the Business Case in terms of what they operationally allow the police to do, and what different options for future systems would allow, and how they work functionally, would give key knowledge to those who would seek to evade such systems and avoid coming to the attention of the police and other agencies who are entrusted with ensuring national security is protected. It is therefore concluded that there is indeed a clear basis for concluding that disclosure would have an adverse impact on national security.

The public interest case concerning the existence, deployment and functionality of CCPC equipment is indeed strong, but the public interest in protection from national security threats is, in my view, stronger. The risk to national security through the release of the Business Case is more than merely negligible and the consequence could be very significant. It is therefore my view that the public interest case for releasing the information does not outweigh the public interest in safeguarding national security to protect lives within the United Kingdom.

Prevention and Detection of Crime, & Apprehension or Prosecution of Offenders

Section 31(1)(a)&(b) of the Freedom of Information Act 2000 states as follows:

"(1) Information which is not exempt information by virtue of section 30 is exempt information if its disclosure under this Act would, or would be likely to, prejudice—

(a) the prevention or detection of crime,

(b) the apprehension or prosecution of offenders"

The wording under s31(1) is slightly different to s24(1), in that here it is must be demonstrated that disclosure "would, or would be likely to, prejudice" the function as opposed to the exemption being "required for the purpose of" the function. The Information Commissioner's guidance on use of s31(1) gives clear steps for a public body to go through when considering whether the exemption has been invoked:

"*The prejudice test involves a number of steps:*

- *One of the law enforcement interests protected by section 31 must be harmed by the disclosure.*
- *The prejudice claimed must be real, actual or of substance. Therefore, if the harm was only trivial, the exemption would not be engaged.*
- *The public authority must be able to demonstrate a causal link between the disclosure and the harm claimed.*
- *The public authority must then decide what the likelihood of the harm actually occurring is, i.e. would it occur, or is it only likely to occur?"*

"Deciding whether the prejudice would occur or is only likely to occur is important. The more certain the prejudice, the greater weight it will carry when considering the public interest. In this context the term "would prejudice" means that it has to be more probable than not that the prejudice would occur. "Would be likely to prejudice" is a

lower test; there must be a real and significant risk, even if risk of prejudice occurring is less than 50 per cent".

The Information Commissioner also provides guidance on the possibility of multiple disclosures forming a 'mosaic' effect as follows:

"*The prejudice test is not limited to the harm that could be caused by the requested information on its own. Account can be taken of any harm likely to arise if the requested information were put together with other information. This is commonly known as the 'mosaic effect'. As explained in the Information Commissioner's guidance information in the public domain, the mosaic effect usually considers the prejudice that would be caused if the requested information was combined with information already in the public domain.*

"However, some requests can set a precedent, i.e. complying with one request would make it more difficult to refuse requests for similar information in the future. It is therefore appropriate to consider any harm that would be caused by combining the requested information with the information a public authority could be forced to subsequently provide if the current requested was complied with. This is known as the precedent effect".

With regard to the public interest test, there is a very clear interest in ensuring that crime is prevented and detected, and that offenders are apprehended and prosecuted. As stated by the Information Commissioner:

"*The exemptions provided by sections 31(1)(a) and (b) very obviously serve to protect society from crime. The matters covered by some of the other exemptions can also prevent the disclosure of information that would facilitate or encourage criminal activity.*

There is a clear public interest in protecting society from the impact of crime. The greater the potential for a disclosure to result in crime, the greater the public interest in maintaining the exemption. The victims of crime can be both organisations and individuals. Although there is a public interest in protecting both, there is a greater public interest in protecting individuals from the impact of crime

Conclusions

For related reasons to those concerning national security, I consider that the information contained within the Business Case, concerning the operation and functionality of the CPCC system as well as potential options for the future, do indeed lead to the conclusion that release of the information would, or would be likely to, prejudice the prevention or detection of crime and the apprehension or prosecution of offenders.

I do not consider that release of the Business Case would lead to a mere theoretical prejudice. The information contained, in the hands of those who wish to evade law enforcement bodies, would make it easier to avoid attempts to undertake covert surveillance. Whilst I cannot be absolutely certain that crime prevention and detection,

and the apprehension and prosecution of offenders, would be adversely impacted by releasing details of the Business Case, I do consider that this is highly likely.

Again it is difficult to give full details of why the above is highly likely without revealing precisely the information that it is considered is exempt from release, but the contents of the Business Case would clearly be of significant use in the hands of those with relevant knowledge to ensure that criminal activity is not identified or located by the police, and that those concerned are able to evade capture as well, and ensure even if prosecution occurs that it is less likely that sufficient evidence will exist to lead to likely conviction.

There is therefore a high chance of such information being likely to prejudice prevention and detection of crime, as well as the apprehension and prosecution of offenders. The importance to the public interest of such steps, then I have concluded that that public interest in having knowledge of and understanding covert communications systems utilised by the police is outweighed by the public interest in prevention and detection of crime, as well as the apprehension and prosecution of offenders.

I therefore concluded that the exemptions in relation to the first, second and third parts of the request were correctly applied in relation to the only relevant information held by the OPCC, and that as a result the Business Case should not be released under s1 of the Freedom of Information Act 2000.

Review of Fourth Part

Section 23 of the Freedom of Information Act 2000 states as follows:

"(1) Information held by a public authority is exempt information if it was directly or indirectly supplied to the public authority by, or relates to, any of the bodies specified in subsection (3).

(2) A certificate signed by a Minister of the Crown certifying that the information to which it applies was directly or indirectly supplied by, or relates to, any of the bodies specified in subsection (3) shall, subject to section 60, be conclusive evidence of that fact.

(3) The bodies referred to in subsections (1) and (2) are—
- (a) the Security Service,
- (b) the Secret Intelligence Service,
- (c) the Government Communications Headquarters,
- (d) the special forces,
- (e) the Tribunal established under section 65 of the Regulation of Investigatory Powers Act 2000,
- (f) the Tribunal established under section 7 of the Interception of Communications Act 1985,
- (g) the Tribunal established under section 5 of the Security Service Act 1989,
- (h) the Tribunal established under section 9 of the Intelligence Services Act 1994,
- (i) the Security Vetting Appeals Panel,

(j) the Security Commission,
(k) the National Criminal Intelligence Service,
(l) the Service Authority for the National Criminal Intelligence Service,
(m) the Serious Organised Crime Agency,
(n) the National Crime Agency, and
(o) the Intelligence and Security Committee of Parliament.

(4) In subsection (3)(c) *"the Government Communications Headquarters"* includes any unit or part of a unit of the armed forces of the Crown which is for the time being required by the Secretary of State to assist the Government Communications Headquarters in carrying out its functions.

(5) The duty to confirm or deny does not arise if, or to the extent that, compliance with section 1(1)(a) would involve the disclosure of any information (whether or not already recorded) which was directly or indirectly supplied to the public authority by, or relates to, any of the bodies specified in subsection (3)".

The Information Commissioner's guidance on use of Section 23 makes clear that this is a very broadly based exemption. As stated:

"To engage section 23(1), the requested information simply has to have been supplied directly or indirectly by one of the named security bodies, or relate to one of those bodies. As it is a class based exemption there is no need for the disclosure to prejudice the work of those bodies in anyway. For the purpose of this guidance the exemption will be referred to as protecting "information relating to the security bodies"."

Making use of the 'neither confirm nor deny' rule engages a lot of the guidance given on section 23 and it is clear that this is another area in which the Information Commissioner considers that a broad approach should be taken to considering whether it is appropriate to use the NCND exemption:

"When considering the application of NCND provisions a public authority is not restricted to only considering the consequences of the actual response that it would be required to provide under s1(1)(a). For example, if it does hold the information the public authority is not limited to only considering what would be revealed by confirming that this is the case. It can also consider what would be revealed if it had to deny the information was held. It is sufficient to demonstrate that either a hypothetical confirmation or a hypothetical denial would engage the exemption.

"It is not necessary to show that both potential responses would engage the exemption.

"As with section 23(1), the term "relates to" is interpreted widely. This, together with the fact the exemption extends to information "not already recorded", means that it has the potential to be applied to a wide range of situations".

Moreover, the 'balance of probabilities' is engaged, as "a public authority can neither confirm nor deny that information is held, if this would disclose information relating to a security body. The term "would" is interpreted as meaning "more likely than not".

Conclusion

Firstly, it is worth noting that the request also included a request for 'legislation', and use the section 23(5) exemption is clearly not appropriate with regard to something that is produced and published by Parliament and Government in an open form. Relevant legislation, and anything else that is published in a public form, would fall under the section 21 exemption as being 'information accessible to the application by other means'.

In relation to anything that does not fall within the section 21 exemption, I conclude that it is appropriate to use the provisions of section 23(5) to neither confirm nor deny the existence of any such documentation. For reasons set out above, this is clearly a request about matters related to national security, and the whole of section 23 is an absolute exemption. In the request for an internal review it is stated that "confirmation or denial of the existence of legislation, codes of practice, policy statements etc. would not reveal operationally sensitive information", but section 23 applies to all information supplied directly or indirectly by, or relating to, the agencies set out in s23(3) and therefore the issue of whether or not information would be operationally sensitive is irrelevant.

As stated above, material already in the public realm is accessible by other means and there is no need to release it following an FOIA request. Public interest considerations also do not apply with regard to the use of section 23. With regard to there being a realistic possibility that a security body would be involved in the issue, given the nature of the CCDC equipment and the purposes for which it may be used, this is proven on the balance of probabilities.

I therefore consider that use of s23(5) was appropriate in relation to information not in the public domain within the fourth request.

In final conclusion I consider that the initial response to the Freedom of Information Act request was, subject to what I have put above with regard to legislation, an appropriate one to make and that the quoted exemptions do apply.

Warwickshire Legal Services