PRIVACY INTERNATIONAL

A Freedom of Information Case Study: Challenging "Neither Confirm Nor Deny"

August 2018

Contents

1. Introduction	03
2. IMSI Catchers	04
3. UK Police Use of IMSI Catchers	05
4. Privacy International Freedom of Information Requests	06
5. The Government’s Responses: “Neither Confirm Nor Deny”	07
6. Appeal to the Information Commissioner’s Office (ICO)	10
7. ICO Decisions	13
8. What Happens Next	17
References	18
Annex: History of a Freedom of Information Request to the Met	19

1. Introduction

The Information Commissioner’s Office (ICO) recently issued a series of decisions in Privacy International’s long-running battle for information about UK police acquisition of IMSI catchers and the regulatory and oversight regime governing their use. This case study provides an in-depth summary and analysis of this process.

In summary, Privacy International prevailed against police forces’ refusal to disclose information based on “neither confirm nor deny” (NCND) responses to our Freedom of Information (FOI) requests for the following categories of records: legislation, codes of practice, and marketing or other promotional materials related to IMSI catchers.

At the same time, the ICO dismissed Privacy International’s arguments that the police forces should not be allowed to rely on NCND to refuse FOI requests for several other categories of records related to IMSI catchers, including internal policy guidance as well as contracts and other records regarding the acquisition of this surveillance technology. Privacy International, represented by Liberty, is appealing this part of the ICO’s decisions to the First-tier Tribunal.

2. IMSI Catchers

IMSI catchers are a type of mobile phone surveillance technology, which mimic mobile phone base stations. By simulating base stations, IMSI catchers trick all mobile phones within a particular radius to connect to them. Once connected to an IMSI catcher, mobile phones reveal data that uniquely identifies them and therefore the mobile phone user. This identification process also allows IMSI catchers to determine the location of mobile phones (and their users). Some IMSI catchers can intercept or even manipulate communications or data, by editing or rerouting them. And some IMSI catchers can also block service to mobile phones within their range.

Where IMSI catchers intercept communications and data (such as calls, text messages, and internet data) transmitted from mobile phones, they pose the same privacy concerns as other methods of communications surveillance. But the interception of data that identifies mobile phones introduces a separate layer of privacy concerns. Mobile phones are uniquely and intimately tied to specific individuals. By combining this data with other information, the government can not only determine the identity of those individuals, but also track and profile them, including where they go, what they do and with whom they meet.

IMSI catchers are inherently indiscriminate surveillance tools, deceiving *all* mobile phones within their radius to identify themselves and reveal the personal data and location of their users. For that reason, IMSI catchers not only interfere with the rights to privacy and freedom of expression, but also pose a particular threat to the right to freedom of assembly and association. The government may, for example, use IMSI catchers at public gatherings, such as at a protest, to identify and collect the personal data of all those in attendance.

3. UK Police Use of IMSI Catchers

One of the earliest reports of UK police use of IMSI catchers dates back to 2011, when *The Guardian* published an article indicating that the Metropolitan Police Service (Met) had acquired an IMSI catcher from the Leeds-based company Datong plc.[1] Over the next few years, other media reports suggested the use of IMSI catchers throughout London.[2]

In October 2016, *The Bristol Cable* published an article citing to evidence indicating that, in addition to the Met, six other police forces have purchased IMSI catchers (Avon & Somerset, South Yorkshire, Staffordshire, Warwickshire, West Mercia and West Midlands).[3] In subsequent reporting by *The Guardian*, a number of policing officials attempted to reassure the public that they were subject to proper safeguards and oversight.[4] For example, the West Mercia Police and Crime Commissioner stated: “I am reassured on behalf of our local communities that the safeguards and processes in place will ensure this technology will be used appropriately and proportionately.” Similarly, the Staffordshire Police and Crime Commissioner stated: “[I]t is crucial that there are robust safeguards, framed by legislation, around this work, and there are.”

4. Privacy International Freedom of Information Requests

In November 2016, Privacy International submitted FOI requests to the police forces identified in the reporting by *The Bristol Cable* as well as to the Home Office and the National Police Chiefs’ Council (NPCC). The requests sought:

- Purchase orders, invoices, contracts, loan agreements, solicitation letters, correspondence with companies and other similar records regarding the acquisition of IMSI catchers;
- Marketing or promotional materials received by the police forces relating to IMSI catchers;
- All requests made to the police forces by companies or government agencies to keep confidential any aspect of the police forces’ possession and use of IMSI catchers, including any non-disclosure agreements;
- Legislation, codes of practice, policy statements, guides, manuals, memoranda, presentations, training materials or other records governing the use of IMSI catchers by the police forces, including restrictions on when, where, how and against whom they 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 IMSI catchers may be revealed to the public, criminal defendants, or judges.

5. The Government’s Responses: “Neither Confirm Nor Deny”

All of the bodies refused the request on grounds that they could “neither confirm nor deny” (NCND) whether they held the information requested because of a combination of the following FOIA exemptions:

- Section 23(5) – information directly or indirectly supplied by or which relates to a security body
- Section 24(2) – information whose exemption is required to safeguard national security
- Section 30(3) – information held for the purposes of investigations and proceedings or obtained from confidential sources
- Section 31(3) – information whose release would or would be likely to prejudice law enforcement

The responses across the public bodies were substantively similar, and in some instances, precisely parroted one another. Below is a detailed summary of one such response from the Met:

- The Met noted that section 23(5) (security bodies) is an absolute exemption but provided no further explanation as to how the FOI request related to this exemption.
- The Met noted that sections 24(2) (national security) and 31(3) (investigations and proceedings) are qualified exemptions subject to “a requirement to articulate the harm that would be caused in confirming or [denying] that the information is held.” In articulating the harm, the Met first stated that confirmation or denial “would in itself disclose exempt information” because “[s]tating information is held would confirm usage and the opposite if there is no such information.” Second, it observed that “[a]lthough the techniques are in the public domain, it is how and when they might be used, that are the sensitive issues” as they “could be deployed for more high profile sensitive operations, albeit not necessarily in the [Met] force area” and that NCND was “required to protect other forces that may use them.” Third, the Met indicated that confirmation “would reveal that the [Met] have access to sophisticated communications analysis techniques,” which would (i) limit operational capabilities as criminals/terrorists would gain a greater understanding of the [Met’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 [Met] may be aware of their presence and taking counter terrorist measures.” On the other hand, the Met submitted, denial “would reveal to those same individuals that their activities are unlikely to have been detected by the [Met]” and “may also suggest (whether correctly or not) the limitations of the [Met’s] capabilities in this area, which may further encourage criminal/terrorist activity by exposing a potential vulnerability.” Finally, the Met argued that the “detrimental effect is increased if the request is made to several different law enforcement bodies” by permitting “those intent on organised crime throughout the UK . . . to ‘map’ where the use of certain tactics are or are not deployed.” The Met continued that this “could lead to [individuals] moving their operations, destroying evidence, or avoiding those areas, ultimately compromising police tactics, operations and future prosecutions.”

- The Met further noted that sections 24(2), 30(3) (law enforcement) and 31(3) are qualified exemptions subject to a public interest test to determine whether the NCND response is appropriate.
    - For section 24(2), the Met stated that while “[t]he public is entitled to know where their public funds are being spent” and that “a better informed public can take steps to protect themselves”, confirming or denying “the use of specialist techniques could render Security measures less effective”, which could “compromise . . . ongoing or future operations to protect the security or infrastructure of the UK and increase the risk of harm to the public.”
    - For section 30(3), the Met stated that while “[t]he public are entitled to know what their public funds are spent on” and “[i]nvestigations may be closed and any proceedings may have been completed, which “may have been high profile and had national implications”, confirming or denying “the use of specialist techniques” would affect the Met’s “future law enforcement capabilities . . . and this would hinder the prevention and detection of crime.”
    - For section 31(3), the Met stated that while “[b]etter awareness may reduce crime or lead to more information from the public, and the public would be able to take steps to protect themselves” and that “[s] ome information is already in the public domain”, 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”, which would “impact on police resources, more crime would then be committed and individuals placed at risk.”

- The Met concluded that “the balancing test for confirming or denying whether any information is held regarding these techniques is not made out” for sections 24(2), 30(3) and 31(3). While acknowledging that “there is a public interest in the transparency of policing operations and in this case providing assurance that the [Met] is appropriately and effectively engaging with the threat posed by the criminal fraternity”, the Met asserted that “there is a very strong public interest in safeguarding both national security and the integrity of police investigations and operations in this area.” The Met also observed that “[t]here is also no requirement to satisfy any public concern over the legality of police operations and the tactics we may or may not use.” It submitted that it is subject to various oversight mechanisms and that its “accountability is therefore not enhanced by confirming or denying whether any information is held.”

Privacy International challenged the bodies’ reliance on NCND to refuse its requests by requesting an internal review. Upon internal review, each of the bodies upheld their initial decisions to rely on NCND to refuse the requests.

6. Appeal to the Information Commissioner’s Office (ICO)

Privacy International next challenged the bodies’ reliance on NCND by appealing to the ICO. Our arguments were as follows:

- Pursuant to international human rights law, the right to access information forms part of the right to freedom of expression. The European Court of Human Rights (ECtHR) affirmed this linkage in *Magyar Helsinki Bizottság v. Hungary* .[5] In assessing whether a denial of access to information constitutes an interference with the right to freedom of expression, the Court emphasised “whether the gathering of the information was . . . relevant [to] public debate” and “disclosure provides transparency on the manner of conduct of public affairs and on matters of interest for society as a whole and thereby allows participation in public governance by the public at large.” The Court also “attached particular weight to the applicant’s role . . . as a journalist or as a social watchdog or non-governmental organisation whose activities related to matters of public interest.” As a human rights organisation, Privacy International plays the role of a watchdog, similar to that played by the press. Indeed, in litigation before the ECtHR, the UK government has accepted that “NGOs engaged in the legitimate gathering of information of public interest in order to contribute to public debate may properly claim the same Art. 10 protections as the press.”[6] Privacy International seeks information about IMSI catchers in order to educate the public about the government’s use of this surveillance technology and its human rights implications, including for the rights to privacy, freedom of expression, and freedom of assembly and association.

- The request for legislation, codes of practice, policy guidance and other information governing the use of IMSI catchers should never be subject to NCND.

- The section 23(5) (security bodies) exemption is not applicable to our requests because the police forces failed to indicate whether the information requested was directly or indirectly supplied by a security body or how the requested information related, in any way, to a security body.

- The section 30(3) (investigations and proceedings) exemption is not applicable to our requests because the police forces failed to explain how the information requested was related to an investigation or proceeding or obtained from confidential sources. As a point of comparison, the Information Commissioner has found a request to fall within this exemption where it contained “a specific reference to a crime reference number which . . . related to the incident [the requestor] was asking about.”[7] By contrast, Privacy International’s request relates to the police forces’ acquisition of IMSI catchers and the regulatory and oversight regime governing their use and not to any specific investigations or proceedings (or to information obtained from confidential sources).

- The NCND position was not required to safeguard national security pursuant to the section 24(2) exemption, nor would confirming or denying the requested information be likely to prejudice law enforcement pursuant to the section 31(3) exemption. The police forces submitted, in their articulation of harm, that national security and law enforcement would be impacted by (1) at a general level, confirming or denying the use of “specialist techniques” and (2) at a specific level, indicating that a technique is used in one area but not in another. As to the first argument, none of the forces defined a “specialist technique” or why IMSI catchers constitute such a technique. Furthermore, it does not follow that confirming or denying that the police forces use a “specialist technique” reveals operationally sensitive information that would impact national security or law enforcement. In fact, the government has explicitly regulated or, in response to FOIA requests, disclosed information relating to a variety of what might also be considered “specialist techniques” – from hacking[8] to the use of equipment to extract data from mobile phones.[9] There is no reason that IMSI catchers should be afforded special protection. As to the second argument, it does not follow that determining which police forces use this technology could permit individuals to map or be aware of how operationally sensitive information is obtained. The police forces have a variety of investigative techniques and tools at their disposal and different police forces will obtain information in different ways.

- The public interest in disclosing the information requested outweighs the public interest in NCND such information pursuant to the section 24(2), 30(3) and 31(3) exemptions.
    - The police forces did not adequately recognise the public interest factors in favour of disclosure. In particular, the police forces failed to identify the strong public interest in information about methods of surveillance that have a profound impact on fundamental rights, including the rights to privacy, freedom of expression, and freedom of assembly and association. In particular, there is significant public interest in communications surveillance technologies, including IMSI catchers. Indeed, because IMSI catchers can indiscriminately collect data (by tricking all mobile phones within a given range to identify themselves and reveal their location), their use can interfere with the rights of many persons simultaneously. By relying on a NCND position, the police forces have hindered a fact-based public debate on IMSI catchers in particular and on police surveillance more broadly.
    - The police forces relied on a series of bare assertions – that confirming or denying “the use of specialist techniques could render Security measures less effective” and would “compromise law enforcement tactics” – as public interest factors in favour of NCND the requested information. As discussed above, the police forces have failed to demonstrate how confirming or denying the existence of the requested information would imperil national security or would be likely to prejudice law enforcement.

7. ICO Decisions

In July 2018, the ICO issued its decision notices with respect to the police forces. Below is a summary of its reasoning with respect to the Met, which is substantively similar to its reasoning across its other decisions.[10]

The Commissioner began by noting that the Met’s approach was to apply the exemptions across the information requested “in a ‘blanket fashion’ without, it would appear, any consideration of a more detailed breakdown of the different elements of the request.” The Commissioner then proceeded to consider the exemptions with respect to each category of the request.

The Commissioner held that several categories of information requested by Privacy International could not be subject to NCND by the police forces:

- *Marketing or promotional materials received by the police forces relating to IMSI catchers:* The Commissioner indicated that she could “not accept that any of the exemptions cited could properly attach to such material” as “[i]t is likely that the [Met] receives many approaches from suppliers trying to promote their products if they feel they may be of benefit to the police service.” She concluded that “[c]onfirmation or denial as to the receipt of such material does not reveal whether or not the [Met] actually purchased any equipment.”

- *Legislation and codes of practice:* The Commissioner began by noting that she had “invited the [Met] to revise its NCND position regarding these elements of the request, however, it declined to do so saying it wished to maintain its position.” She concluded that “[i]t is clear . . . that legislation either does or doesn’t exist and, if it does, it clearly cannot be exempt under FOIA as it would be statute which should be publicly available; this would be the same for codes of practice.”

The Commissioner upheld the NCND position for the remaining categories of records requested by Privacy International:

- Purchase orders, invoices, contracts, loan agreements, solicitation letters, correspondence with companies and other similar records regarding the acquisition of IMSI catchers;

- All requests by companies, or government agencies, to the police forces to keep confidential any aspect of the police forces’ possession and use of IMSI catchers, including any non-disclosure agreements;

- Policy statements, guides, manuals, memoranda, presentations, training materials or other records governing the use of IMSI catchers by the police forces.

The Commissioner did not provide further explanation as to why these specific categories of information were subject to the NCND exemptions, except as to “policy and guidance”, where she noted that “any confirmation or denial . . . would clearly indicate whether or not [IMSI catchers were] being used . . . because it would not exist unless there was a business requirement for it to have been created.” However, the Commissioner’s reasoning as to the application of the NCND exemptions was as follows:

- Section 23(5): The Commissioner emphasised that “[t]he equipment being considered here is covert surveillance equipment and, put simply, the Commissioner is trying to establish the likelihood as to whether or not the use of such equipment could ‘relate to’ any of the security bodies; this is all she is required to do.” She stated that the covert nature of the equipment makes it “considerably more likely to ‘relate’ to security bodies” and that “it could realistically be deployed in joint operations between the police service and security bodies.” She further indicated that “the conditions for any actual deployment of such equipment may therefore relate to practices developed by security bodies, eg terrorism operations.”

- Section 24(2): The Commissioner began by noting that “only a consistent use of a NCND response on matters of national security can secure its proper response” and therefore that “regard has to be given to the need to adopt a consistent NCND position and not simply to the consequences of confirming whether the specific requested information in this case is held or not.” She then relied on her decision with respect to the engagement of the section 23(5) exemption, where the determination “that section 23 is engaged” means “the potential involvement of a security body has already been satisfied.” Finally, the Commissioner essentially reiterated the Met’s arguments relating to harm, noting that “if it were the case that only a small number of forces had access to this type of equipment then it follows that those who do not are obviously more vulnerable to the types of crimes that could be subject to this type of surveillance if it were in use; this may in turn present a potential ‘green light’ to some criminals or terrorists to undertake certain crimes in particular force areas.” She continued that “[w]ere it the case that no forces had access to this equipment then confirming this would again show vulnerability and criminals would be more knowledgeable as to what means of communication were the least likely to be intercepted.” In terms of the public interest test, the Commissioner emphasised that “the current national security level of risk, which is set by the government, sits at severe” and concluded that it was “clearly the case that the public interest in confirming or denying whether information is held does not match the weight of the public interest in safeguarding national security by maintaining a consistent NCND stance.”

The Commissioner held that in light of her finding with respect to sections 23(5) and 24(2), she would not consider “the other exemption[s] cited” (i.e., sections 30(3) and 31(3)).

Home Office: Patchwork of Legislative Frameworks Govern IMSI Catchers

In May 2018, the Home Office wrote to Privacy International following the appeal to the ICO and indicated that it “wish[ed] to amend our original (neither confirm nor deny position” by “confirm[ing] that we do not hold any information considered within scope of the request.” The response further noted, however, that where there are “circumstances under which public authorities have an operational requirement to identify communications equipment, for example when an unknown piece of equipment is in close proximity to a public authority . . . a legal mechanism exists within the Investigatory Powers Act 2016 to support use of this capability.”

Liberty, now representing Privacy International in this matter, replied to the Home Office to seek clarification of its letter. First, it sought clarity as to how “an operational requirement to identify communications equipment” relates to the FOI request on IMSI catchers. Second, it sought clarity as to whether the Home Office’s position is that there is no legislation, codes of practice, or other policy guidance governing IMSI catchers; there is such legislation and it is the Investigatory Powers Act 2016 (IPA); and/or that there is other policy guidance held by other public authorities. Finally, the letter sought confirmation from the Home Office as to what searches it had conducted to reach the conclusion that it held no other information responsive to Privacy International’s request.

In July 2018, the Home Office responded to Liberty’s request for clarification. With respect to the “operational requirement to identify communications equipment”, the Home Office simply stated that “in order to provide a comprehensive response to your client, and given the nature of the request made, regard has been given to the broader question relating to the capability of public authorities to identify communications equipment.”

The Home Office also proceed to cite to other “relevant legislation governing the use of” IMSI catchers. Those pieces of legislation were:

- Part 3 of the Police Act 1997
- Chapter 7 of the Covert Surveillance and Property Interference Code of Practice
- Part 5 of the IPA
- Equipment Interference Code of Practice

Finally, the Home Office indicated that in conducting its search, “all relevant Home Office policy teams were consulted and each conducted thorough searches for any information held concerning” IMSI catchers.

In short, after 18 months of relying on a NCND position with respect to our request, the Home Office has amended that position to cite to two statutes and two codes of practice as relevant to police use of IMSI catchers.

National Police Chiefs’ Council: Dangerous U-Turn on FOIA

We have separately written about how the NPCC – during the course of our FOI request process – declared that it was not subject to FOIA.[11] This position ran counter to the NPCC’s long-standing practice, including with respect to our own request, to act as if it was subject to FOIA. In May 2018, Liberty, on behalf of Privacy International, wrote to the Home Office and Cabinet Office to request an immediate order designating the NPCC as a public authority subject to FOIA. In July 2018, the Cabinet Office informed Liberty[12] that it had laid a draft statutory instrument[13] before Parliament making such a designation.

8. What Happens Next

The police forces are required to confirm or deny whether they hold legislation, codes of practice, and brochures and other promotional materials related to IMSI catchers, and to either disclose this material or issue a refusal under a relevant FOIA exemption. Liberty and Privacy International will publish any materials disclosed and are prepared to challenge refusals that are not in compliance with FOIA. Privacy International, represented by Liberty, is also appealing those parts of the ICO’s decisions, which uphold the police forces’ NCND position with respect to other categories of records.

References

1 Ryan Gallagher & Rajeev Syal, “Met police using surveillance system to monitor mobile phones”, The Guardian, 30 October 2011, https://www.theguardian.com/uk/2011/oct/30/metropolitan-police-mobile-phone-surveillance.

2 Ben Bryant, “VICE News Investigation Finds Signs of Secret Phone Surveillance across London”, VICE News, 14 Jan. 2016, https://news.vice.com/article/vice-news-investigation-finds-signs-of-secret-phone-surveillance-across-london; Tom Cheshire, “Fake Mobile Phone Towers Operating in the UK”, Sky News, 9 June 2015, https://news.sky.com/story/fake-mobile-phone-towers-operating-in-the-uk-10356433.

3 Alon Aviram, “Revealed: Bristol’s police and mass mobile phone surveillance”, The Bristol Cable, 10 Oct. 2016, https://thebristolcable.org/2016/10/imsi/.

4 David Pegg & Rob Evans, “Controversial snooping technology ‘used by at least seven police forces’”, The Guardian, 10 Oct. 2016, https://www.theguardian.com/world/2016/oct/10/controversial-phone-snooping-technology-imsi-catcher-seven-police-forces/

5 Magyar Helsinki Bizottság v. Hungary, Grand Chamber, European Court of Human Rights, App. No. 18030/11, 8 Nov. 2016, available at https://privacyinternational.org/sites/default/files/2018-02/United%20Kingdom%E2%80%99s%20Observations%20on%20the%20Merits.pdf.

6 United Kingdom’s Observations on the Merits, 10 Human Rights Orgs. v. United Kingdom, European Court of Human Rights, App. No. 58170/13, 18 Apr. 2016, §6.1, available at https://privacyinternational.org/sites/default/files/2018-02/United%20Kingdom%E2%80%99s%20Observations%20on%20the%20Merits.pdf.

7 Information Commissioner’s Office, Decision Notice, Ref. FS50689520, 18 Dec. 2017, available at https://ico.org.uk/media/action-weve-taken/decision-notices/2017/2172938/fs50689520.pdf.

8 See Investigatory Powers Act 2016, Part 5; Equipment Interference Code of Practice, March 2018, available at https://assets.documentcloud.org/documents/4501821/Equipment-Interference-Code-of-Practice.pdf.

9 See Privacy International, “Digital stop and search: how the UK police can secretly download everything from your mobile phone”, Mar. 2018, available at https://privacyinternational.org/sites/default/files/2018-03/Digital%20Stop%20and%20Search%20Report.pdf.

10 Information Commissioner’s Office, Decision Notice, Ref. FS50728051, 10 July 2018, available at https://ico.org.uk/media/action-weve-taken/decision-notices/2018/2259450/fs50728051.pdf.

11 Scarlet Kim, “The NPCC is no longer open to public scrutiny – the Government must fix this loophole immediately”, Liberty, 22 June 2018, https://www.libertyhumanrights.org.uk/news/blog/npcc-no-longer-open-public-scrutiny-government-must-fix-loophole-immediately.

12 National police co-ordinating body to be opened up to public scrutiny following Liberty and Privacy International campaign, Liberty, 26 July 2018, https://www.libertyhumanrights.org.uk/news/press-releases-and-statements/national-police-co-ordinating-body-be-opened-public-scrutiny-0.

13 The Freedom of Information (Designation as Public Authority and Amendment) Order 2018, available at http://www.legislation.gov.uk/ukdsi/2018/9780111171158.

Annex: History of a Freedom of Information Request to the Met

PRIVACY INTERNATIONAL

Address: 62 Britton Street, London, EC1M 5UY, United Kingdom
Phone: +44 (0) 20 3422 4321
Website: www.privacyinternational.org

General enquiries
Metropolitan Police Service
New Scotland Yard
Broadway
London
SW1H 0BG

1 November 2016

Dear Freedom of Information Officer:

I am writing on behalf of Privacy International to seek records, pursuant to the Freedom of Information Act 2000, relating to the purchase and use of mobile phone surveillance equipment by the Metropolitan Police.

I refer, in particular, to the recent article written by the journalist collective The Bristol Cable “Revealed: Bristol’s police and mass mobile phone surveillance”.[1] The article makes reference to the purchase of equipment from the company CellXion by the Metropolitan Police under the item “CCDC” for the cost of £1,037,223.00. The article links to the original document disclosing the purchase, which can be found on the Metropolitan Police website.[2] The article also explains that the acronym “CCDC equipment” appears to refer to “covert communications data capture” as spelled out in the minutes of an Alliance Governance Group meeting in May 2016 between Warwickshire and West Mercia Police.[3]

I also refer to the 10 October 2016 article published by the Guardian “Controversial snooping technology ‘used by at least seven police forces’”.[4] That article reported that “surveillance technology that indiscriminately harvests information from mobile phones”, also “known as an IMSI catcher” is being “used by at least seven police forces across the country…according to police documents.” One of the forces understood to be using this technology is the Metropolitan Police.

[1] https://thebristolcable.org/2016/10/imsi/
[2] http://www.met.police.uk/foi/pdfs/lists_and_registers/corporate/contracts_over_%C2%A32500_q3_october2015_january2016.pdf
[3] https://thebristolcable.org/wp-content/uploads/2016/10/09-imsi-4.pdf
[4] https://www.theguardian.com/world/2016/oct/10/controversial-phone-snooping-technology-imsi-catcher-seven-police-forces?CMP=twt_gu

Privacy International requests the following records:

1. Purchase orders, invoices, contracts, loan agreements, solicitation letters, correspondence with companies and other similar records regarding the Metropolitan Police’s acquisition of CCDC equipment. Please include records of all purchase orders, invoices, contracts, agreements, and communications with CellXion.

2. Marketing or promotional materials received by the Metropolitan Police relating to CCDC equipment.

3. All requests by CellXion or any other corporation, or any government agency, to the Metropolitan Police to keep confidential any aspect of Metropolitan Police’s possession and use of CCDC equipment, including any non-disclosure agreements between Metropolitan Police and CellXion or any other corporation, or government agency, regarding the Metropolitan Police’s possession and use of CCDC equipment.

4. Legislation, codes of practice, policy statements, guides, manuals, memoranda, presentations, training materials or other records governing the possession and use of CCDC equipment by the Metropolitan 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.

Privacy International seeks records regardless of how CCDC equipment is identified. In this respect, Privacy International notes that CCDC equipment can be referred to using a range of other terms, including “IMSI Catchers”, “IMSI Grabbers”, “Cell site simulators” and “Stingrays”.

Please include copies of material that you hold either in the form of paper or electronic records, including emails. If possible, please provide all requested records in electronic format.

Upon locating the requested records, please contact us and advise us of any costs of providing copies, so that we may decide whether it is necessary to narrow our request.

We would appreciate a response as soon as possible and look forward to hearing from you shortly. Please furnish the requested records to:

Matthew Rice
Privacy International
62 Britton Street
London EC1M 5UY
matthew@privacyinternational.org

If any portion of this request is denied for any reason, please inform us of the reasons for the denial in writing and provide the name and address of the body to whom an appeal should be directed.

Please do not hesitate to contact me at 020 3422 4321 or matthew@privacyinternational.org if you have any questions about this request. Thank you for your prompt attention.

Sincerely,

Matthew Rice
Advocacy Officer

cc: Scarlet Kim
Legal Officer

From: **Scarlet** scarlet@privacyinternational.org
Subject: Fwd: FOIA Response
Date: 11 February 2018 at 12:31
To: Scarlet scarlet@privacyinternational.org



Begin forwarded message:

From: Matthew Rice <matthew@privacyinternational.org>
Subject: **Fwd: FOIA Response**
Date: 30 November 2016 at 10:23:44 GMT
To: Scarlet Kim <scarlet@privacyinternational.org>

Begin forwarded message:

From: catherine.carrington@met.police.uk
Subject: **FOIA Response**
Date: 29 November 2016 at 17:18:50 GMT
To: matthew@privacyinternational.org
Reply-To: foi@met.pnn.police.uk

Dear Mr Rice

Freedom of Information Request Reference No: 2016110000055

I respond in connection with your request for information which was received by the Metropolitan Police Service (MPS) on 08/11/2016. I note you seek access to the following information:

I am writing on behalf of Privacy International to seek records, pursuant to the Freedom of Information Act 2000, relating to the purchase and use of mobile phone surveillance equipment by the Metropolitan Police.

I refer, in particular, to the recent article written by the journalist collective The Bristol Cable “Revealed: Bristol’s police and mass mobile phone surveillance”. The article makes reference to the purchase of equipment from the company CellXion by the Metropolitan Police under the item “CCDC” for the cost of £1,037,223.00. The article links to the original document disclosing the purchase, which can be found on the Metropolitan Police website. The article also explains that the acronym “CCDC equipment” appears to refer to “covert communications data capture” as spelled out in the minutes of an Alliance Governance Group meeting in May 2016 between Warwickshire and West Mercia Police.

I also refer to the 10 October 2016 article published by the Guardian “Controversial snooping technology ‘used by at least seven police forces’”. That article reported that “surveillance technology that indiscriminately harvests information from mobile phones”, also “known as an IMSI catcher” is being “used by at least seven police forces across the country…according to police documents.” One of the forces understood to be using this technology is the Metropolitan Police.

Privacy International requests the following records:
1. Purchase orders, invoices, contracts, loan agreements, solicitation letters, correspondence with companies and other similar records regarding the Metropolitan Police’s acquisition of CCDC equipment. Please include records of all purchase orders, invoices, contracts, agreements, and communications with CellXion.
2. Marketing or promotional materials received by the Metropolitan Police relating to CCDC equipment.
3. All requests by CellXion or any other corporation, or any government agency, to the Metropolitan Police to keep confidential any aspect of Metropolitan Police’s possession and use of CCDC equipment, including any non-disclosure agreements between Metropolitan Police and CellXion or any other corporation, or government agency, regarding the Metropolitan Police’s possession and use of CCDC equipment.
4. Legislation, codes of practice, policy statements, guides, manuals, memoranda, presentations, training materials or other records governing the possession and use of CCDC equipment by the Metropolitan 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.

Privacy International seeks records regardless of how CCDC equipment is identified. In this respect, Privacy International notes that CCDC equipment can be referred to using a range of other terms

Privacy International notes that GCHQ equipment can be referred to using a range of other terms, including “IMSI Catchers”, “IMSI Grabbers”, “Cell site simulators” and “Stingrays”.
As per email dated 08/11/2016*: I would like my request for information to be within the search period of 1/8/2015 to 31/12/2015..*

DECISION
Section 1 of the Act places two duties on public authorities. Unless exemptions apply, the first duty at Section 1(1)(a) is to confirm or deny whether the information specified in a request is held. The second duty at Section 1(1)(b) is to disclose information that has been confirmed as being held. Where exemptions are relied upon Section 17 of the Act requires that we provide the applicant with a notice which: a) states that fact b) specifies the exemption(s) in question and c) states (if that would not otherwise be apparent) why the exemption applies.

The MPS can neither confirm nor deny that it holds information pertinent to this request as the duty in Section 1(1)(a) of the Act does not apply, by virtue of the following exemptions:

Section 23(5) Information relating to the Security bodies;
Section 24(2) National Security;
Section 30(3) Investigations;
Section 31(3) Law enforcement;

REASONS FOR DECISION
Section 23 is a class based absolute exemption and there is no requirement to consider the public interest test in this area.

Section 30 is a class based qualified exemption and consideration must be given as to whether there is a public interest in neither confirming nor denying the information exists is the appropriate response.

Sections 24 and 31 are prejudice based qualified exemptions and there is a requirement to articulate the harm that would be caused in confirming or nor that the information is held as well as carrying out a public interest test.

The overall harm for the NCND is as follows:
By confirming or denying that the MPS hold any information regarding these techniques would in itself disclose exempt information. Stating information is held would confirm usage and the opposite if there is no such information.

Although the techniques are in the public domain, it is how and when they might be used, that are the sensitive issues for the police service. These techniques could be deployed for more high profile sensitive operations, albeit not necessarily in the MPS force area, therefore the NCND is required to protect other forces that may use them.

Any disclosure under FOIA 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) the MPS may or may not deploy in specific circumstances would prejudice law enforcement. If the requested information was held by the MPS, confirmation of this fact would reveal that the MPS have 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 MPS'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 MPS may be aware of their presence and taking counter terrorist measures.

Conversely, if information was not held by the MPS, and a denial was issued, this would reveal to those same individuals that their activities are unlikely to have been detected by the MPS. It may also suggest (whether correctly or not) the limitations of the MPS'S 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 the MPS would substantially prejudice the ability of the MPS 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

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.

Please see the LEGAL ANNEX for the sections of the Act, and for a full explanation why the exemptions have been applied to this response.

This should not be taken as conclusive evidence that any information that would meet your request exists or does not exist.

Should you have any further enquiries concerning this matter, please contact me via email at foi@met.pnn.police.uk, quoting the reference number above.

Yours sincerely

Catherine Carrington
Privacy Advisor
Freedom of Information
Information Rights Unit (IRU)
Metropolitan Police Service (MPS)
PO Box 57192
London
SW6 1SF

LEGAL ANNEX

Section 17(1) of the Act provides:

(1) A public authority which, in relation to any request for information, is to any extent relying on a claim that any provision in part II relating to the duty to confirm or deny is relevant to the request or on a claim that information is exempt information must, within the time for complying with section 1(1), give the applicant a notice which-

(a) states the fact,
(b) specifies the exemption in question, and
(c) states (if that would not otherwise be apparent) why the exemption applies.

Section 23(5) of the Act provides:
Information supplied by, or relating to, bodies dealing with security matters.
(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).

Section 24(2) of the Act provides:
National security
(2)The duty to confirm or deny does not arise if, or to the extent that, exemption from section 1(1)(a) is required for the purpose of safeguarding national security.

Section 30(3) of the Act provides:
Investigations and proceedings conducted by public authorities
(3)The duty to confirm or deny does not arise in relation to information which is (or if it were held by the public authority would be) exempt information by virtue of subsection (1) or (2).

Section 31(3) of the Act provides:
Law enforcement
(3)The duty to confirm or deny does not arise if, or to the extent that, compliance with section 1(1)(a) would, or would be likely to, prejudice any of the matters mentioned in subsection (1).

Factors favouring confirming or denying whether any other information is held for Section 24
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 24
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 infra-structure 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 30
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 30
By confirming or denying the use of specialist techniques, the MPS’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 31
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 31
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 the MPS 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 MPS 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 Police and Criminal Evidence Act and the Regulation of Investigatory Powers Act and independent bodies such as Her Majesty’s Inspectorate of Constabulary, the Independent Police Complaints Commission 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 our 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.

COMPLAINT RIGHTS

Are you unhappy with how your request has been handled or do you think the decision is incorrect?

You have the right to require the Metropolitan Police Service (MPS) to review their decision.

Prior to lodging a formal complaint you are welcome to discuss the response with the case officer who dealt with your request.

Complaint

Complaint

If you are dissatisfied with the handling procedures or the decision of the MPS made under the Freedom of Information Act 2000 (the Act) regarding access to information you can lodge a complaint with the MPS to have the decision reviewed.

Complaints should be made in writing, within forty (40) working days from the date of the refusal notice, and addressed to:

FOI Complaint
Information Rights Unit
PO Box 57192
London
SW6 1SF
foi@met.police.uk

In all possible circumstances the MPS will aim to respond to your complaint within 20 working days.

The Information Commissioner

After lodging a complaint with the MPS if you are still dissatisfied with the decision you may make application to the Information Commissioner for a decision on whether the request for information has been dealt with in accordance with the requirements of the Act.

For information on how to make application to the Information Commissioner please visit their website at www.ico.org.uk. Alternatively, write to or phone:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
Phone: 0303 123 1113

Total Policing is the Met's commitment to be on the streets and in your communities to catch offenders, prevent crime and support victims. We are here for London, working with you to make our capital safer.

Consider our environment - please do not print this email unless absolutely necessary.

NOTICE - This email and any attachments may be confidential, subject to copyright and/or legal privilege and are intended solely for the use of the intended recipient. If you have received this email in error, please notify the sender and delete it from your system. To avoid incurring legal liabilities, you must not distribute or copy the information in this email without the permission of the sender. MPS communication systems are monitored to the extent permitted by law. Consequently, any email and/or attachments may be read by monitoring staff. Only specified personnel are authorised to conclude any binding agreement on behalf of the MPS by email. The MPS accepts no responsibility for unauthorised agreements reached with other employees or agents. The security of this email and any attachments cannot be guaranteed. Email messages are routinely scanned but malicious software infection and corruption of content can still occur during transmission over the Internet. Any views or opinions expressed in this communication are solely those of the author and do not necessarily represent those of the Metropolitan Police Service (MPS).

Find us at:

Facebook: Facebook.com/metpoliceuk
Twitter: @metpoliceuk

PRIVACY INTERNATIONAL

Address: 62 Britton Street, London, EC1M 5UY, United Kingdom
Phone: +44 (0) 20 3422 4321
Website: www.privacyinternational.org

FOI Complaint
Information Rights Unit
PO Box 57192
London
SW6 1SF

24 January 2017

Re: Freedom of Information Request Reference No. 2016110000055

A. Introduction

1. This is an appeal following a refusal to disclose information made by the Metropolitan Police Service on 29 November 2016. Privacy International respectfully requests an internal review of the decision.

2. Privacy International is a UK registered charity. The organisation’s mission is to defend the right to privacy and to fight unlawful surveillance and other intrusions into private life, with a focus on the technologies that enable these practices. In seeking the information requested, Privacy International seeks to bring greater accountability and transparency to surveillance practices.

B. Background

3. On 1 November 2016, Privacy International wrote to the Freedom of Information Officer seeking records, pursuant to the Freedom of Information Act 2000, relating to the purchase and use of mobile phone surveillance equipment by the Metropolitan Police. We directed you to an article making reference to the purchase of equipment from the company CellXion by the Metropolitan Police under the item “CCDC” for the cost of £1,037,223.00. The article explained that the acronym “CCDC” appeared to refer to “covert communications data capture” as spelled out in the minutes of an Alliance Governance Group meeting in May 2016 between Warwickshire and West Mercia Police.

4. The request also summarised another newspaper article, which referenced police use of surveillance technology known as IMSI catchers, which collect information from mobile phones. The article set out that it is understood that the Metropolitan Police is one of at least seven police forces across the country using this technology.

5. The request stated that CCDC equipment can be referred to using a range of other terms, including “IMSI Catchers”, “IMSI Grabbers”, “Cell site simulators” and “Stingrays”. For the purposes of this appeal, Privacy International refers to such equipment as “IMSI Catchers”.

6. Privacy International requested the following records:

“*1. Purchase orders, invoices, contracts, loan agreements, solicitation letters, correspondence with companies and other similar records regarding the Metropolitan Police’s acquisition of CCDC equipment. Please include records of all purchase orders, invoices, contracts, agreements, and communications with CellXion;*

2. Marketing or promotional materials received by the Metropolitan Police relating to CCDC equipment;

3. All requests by CellXion or any other corporation or any government agencies to the Metropolitan Police to keep confidential any aspect of the Metropolitan Police’s possession and use of CCDC equipment, including any non-disclosure agreements between the Metropolitan Police and CellXion or any other corporation or government agency regarding the Metropolitan Police’s possession and use of CCDC equipment;

4. Legislation, codes of practice, policy statements, guides, manuals, memoranda, presentations, training materials or other records governing the possession and use of CCDC equipment by the Metropolitan, 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.”

C. The Refusal

7. On 29 November 2016, the Privacy Advisor of the Metropolitan Police Freedom of Information, Information Rights Unit (“IRU”) refused the request. The refusal relied on ss.23(5), 24(2), 30(3), and 31(3) Freedom of Information Act 2000. The reasons given for the overall harm identified can be summarised as follows:

7.1 That confirming or denying that the Metropolitan Police holds information regarding these techniques would in itself disclose exempt information. Stating information is held would confirm usage and the opposite if there is no such information;

7.2 How and when the techniques might be used, are sensitive issues for the police service. These techniques could be deployed for more high profile sensitive

operations, albeit not necessarily in the Metropolitan Police force area, therefore the NCND is required to protect forces that may use them;

7.3 Any disclosure under the Freedom of Information Act 2000 is a disclosure to the world at large, and NCND use of specialist techniques which may or may not exist, and which (should they exist) the Metropolitan Police may or may not deploy in specific circumstances would prejudice law enforcement. If the requested information was held by the Metropolitan Police, confirmation of this fact would reveal that the Metropolitan Police have access to sophisticated communications analysis techniques. This would be damaging as it would:

7.3.1 Limit operational capabilities as criminals/terrorists would gain a greater understanding of the Metropolitan Police’s methods and techniques, enabling them to take steps to counter them; and

7.3.2 Provide an indication to any individual who may be undertaking criminal/terrorist activities that the Metropolitan Police may be aware of their presence and taking counter terrorist measures.

7.4 Conversely, if information was not held by the Metropolitan Police, and a denial was issued, this would reveal to those same individuals that their activities are unlikely to have been detected by the Metropolitan Police. It may also suggest (whether correctly or not) the limitations of the Metropolitan Police’s capabilities in this area, which may further encourage criminal/terrorist activity by exposing a potential vulnerability.

7.5 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 capacity by the Metropolitan Police would substantially prejudice the ability of the Metropolitan Police to police their area which would lead to a greater risk of the public.

7.6 Useful information to those committing crimes of drugs and terrorist activity who would be able to ‘map’ where the use of certain tactics are or are not deployed. Information could enable individuals to become aware of location-specific operations. This could lead to them moving their operations, destroying evidence, or avoiding those areas, ultimately compromising police tactics, operations and future prosecutions.

7.7 Very strong public interest in safeguarding both national security and the integrity of police investigations and operations in this area.

D. The Appeal

8. The reasons provided by the Metropolitan Police, as set out above, fail to justify the application of NCND in this case. This is for the following four reasons.

9. Firstly, the Metropolitan Police response is predicated on a series of non-sequiturs:

9.1 It simply does not follow that merely confirming or denying that a police force uses IMSI catchers would reveal operationally sensitive information about the scope of police activities and operations. This reasoning is not understood. It appears that the Metropolitan Police has confused consideration of “neither confirm nor deny” with consideration of the provision of information itself;

9.2 Equally, it does not follow that making the same request to multiple police forces could identify how individuals could map or be aware of how operationally sensitive information is obtained by the various police forces. Different police forces could obtain intelligence in multiple ways. Confirming or denying that a police force holds the requested information does not automatically reveal how tactics are deployed or what technical operations each force has;

9.3 It is not understood why revealing that a police force has sophisticated capabilities to analyse data would limit operational capabilities. The reasoning set out in paragraph 7.3, above, is nonsensical.

10. Secondly, it fails to have regard to obviously material considerations, including, but not limited to:

10.1 The fact that the Metropolitan Police’s purchase of IMSI catchers is already in the public domain, as set out in Privacy International’s original request;

10.2 The fact that the legislative provisions and/or policy guidance requested cannot conceivably fall within any exemption;

10.3 The significant public interest in the topic of IMSI catchers and the regulation of related communications surveillance technologies.

11. Thirdly, when considered forensically, the exemptions relied upon do not apply.

11.1 Under Section 23(5), there has to be a realistic possibility that a security body would be involved in the issue the request relates to in order for the exemption to apply. No such possibility has been set out. Any possibility that is particularised would be too remote to justify the application of this exemption;

11.2 Section 24(2) provides an exemption from the duty to confirm information is held, where the exemption is required for the purposes of safeguarding national security. Section 31(3) also provides an exemption where it is necessary for the prevention or detection of crime. No real reasons have been set out as to why either exemption applies. By way of example, it cannot seriously be suggested that it would damage national security and/or the prevention or detection of crime to confirm the existence of legislative powers and/or policy guidance;

11.3 Section 30(3) provides that the duty to confirm or deny does not arise in relation to information which is exempt information by virtue of subsection 30(1) or (2). Section 30(1) can only be claimed by public authorities that have a duty to investigate whether someone should be charged with an offence, or the power to conduct such investigations and/or institute criminal proceedings. Section 30(2) protects the identity of confidential sources, primarily to ensure informants are not deterred from supplying law enforcement agencies with valuable intelligence. The ICO Guidance makes it clear at §53 that the s.30 exemptions “*exist to ensure the effective investigation and prosecution of offences and the protection of confidential sources. They recognise the need to prevent disclosures that would prejudice either a particular investigation or set of proceedings, or the investigatory and prosecution processes generally, including any prejudice to future investigations and proceedings*.”[1] None of these matters have been addressed in the response to the request. There is no risk of prejudice to a specific investigation, there is no risk to informants, and there is no risk to confidential sources.

12. When considering whether or not any of these exemptions apply, it is necessary to have regard to the language and purpose of the Freedom of Information Act 2000. The language and purpose of the Act require exemptions to be narrowly construed:

12.1 The word “*required*” in s.1(1)(a) “*… means reasonably necessary. It is not sufficient for the information sought simply to relate to national security; there must be a clear basis for arguing that disclosure would have an adverse effect on national security before the exemption is engaged*”;[2]

12.2 It is therefore clear that a decision to “neither confirm nor deny” requires a clear justification and merits close scrutiny. This is because it flies in the face of the “*default setting*” in the Freedom of Information Act 2000, which is in favour of disclosure.[3] It also flies in the face of the Article 10 right to receive information, as recently confirmed by the European Court of Human Rights;[4]

[1] https://ico.org.uk/media/for-organisations/documents/1205/investigations-and-proceedings-foi-section-30.pdf
[2] *Philip Kalman v Information Commissioner and the Department of Transport* (EA/2009/111 8 July 2010).
[3] *Galloway v Information Commissioner v The Central and North West London NHS Foundation Trust* (2009) 108 BMLR 50, at §70.
[4] *Magyar Helsinki Bizottság v Hungary* (App. no. 18030/11).

12.3 This submission reflects the approach taken to “*neither confirm nor deny*” in parallel contexts. A decision to “*neither confirm nor deny*” “*… requires justification similar to the position in relation to public interest immunity ... It is not simply a matter of a governmental party to litigation hoisting the NCND flag and the court automatically saluting it*”.[5]

13. Fourthly, as regards the qualified exemptions relied upon, the public interest balancing exercise falls squarely in favour of disclosure:

13.1 No meaningful reasons have been provided as to why there is a public interest in neither confirming nor denying the matters requested in this request;

13.2 There is currently no evidence at all to suggest that the public interest will be harmed to any material extent by disclosure of the information sought;

13.3 The public interest in disclosure is real, it is important that the public are reassured that the measures used to safeguard national security are proportionate and effective;

13.4 No regard at all has been had to the public interest in the disclosure of the information requested. There is currently a wide-ranging public debate taking place on the ambit of privacy rights in the context of surveillance and technology. There has also been widespread coverage of the purchase and use of IMSI catchers by police forces across the country. In limiting its consideration of the public interest to “*the transparency of policing operations*”, the Metropolitan Police failed to have regard to obviously material considerations.

E. The Appeal

14. Privacy International respectfully requests the Metropolitan Police to re-consider the original request made for information as set out above.

Scarlet Kim
Legal Officer
Privacy International

cc: Matthew Rice
Advocacy Officer
Privacy International

[5] *Mohamed and another v Secretary of State for the Home Department* [2014] 1 WLR 4240, per Maurice Kay LJ, at §40.



Met HQ Strategy & Governance
Information Law & Security Group
Information Rights Unit
PO Box 57192
London
SW6 1TR

Telephone: 0207 161 3500
Facsimile: 0207 161 3503
Email: foi@met.police.uk

www.met.police.uk

Your ref:
Our ref: 2017010000924

13 June 2017

Dear Ms Kim

Freedom of Information Internal Review Reference No: 2017010000924

I write in connection with your correspondence dated 24/12/2017 in which you requested an internal review in relation to your request for information (ref: 2016110000055). The requested information was as follows:

> **‘Privacy International requests the following records:**
>
> **1. Purchase orders, invoices, contracts, loan agreements, solicitation letters, correspondence with companies and other similar records regarding the Metropolitan Police’s acquisition of CCDC equipment. Please include records of all purchase orders, invoices, contracts, agreements, and communications with CellXion.**
>
> **2. Marketing or promotional materials received by the Metropolitan Police relating to CCDC equipment.**
>
> **3. All requests by CellXion or any other corporation, or any government agency, to the Metropolitan Police to keep confidential any aspect of Metropolitan Police’s possession and use of CCDC equipment, including any non-disclosure agreements between Metropolitan Police and CellXion or any other corporation, or government agency, regarding the Metropolitan Police’s possession and use of CCDC equipment.**
>
> **4. Legislation, codes of practice, policy statements, guides, manuals, memoranda, presentations, training materials or other records governing the possession and use of CCDC equipment by the Metropolitan 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.

Privacy International seeks records regardless of how CCDC equipment is identified. In this respect, Privacy International notes that CCDC equipment can be referred to using a range of other terms, including “IMSI Catchers”, “IMSI Grabbers”, “Cell site simulators” and “Stingrays”.

As per email dated 08/11/2016: I would like my request for information to be within the search period of 1/8/2015 to 31/12/2015.’

DECISION

The Metropolitan Police Service (MPS) has completed its review and has decided to:

- Uphold the original decision

The MPS is not required to confirm or deny whether the requested information is held due to the following provisions of the Freedom of Information Act 2000:

- Section 17(1) - Refusal notice
- Section 23(5) - Information supplied by, or relating to bodies dealing with security matters
- Section 24(2) - National security
- Section 30(3) - Investigations and proceedings conducted by public authorities
- Section 31(3) - Law enforcement

REASON FOR DECISION

The Freedom of Information Act 2000 creates a statutory right of access to information held by public authorities. Section 1(1) of the act requires a public authority in receipt of a request to:

- Confirm whether they hold the requested information and if so,
- Communicate the requested information to the applicant.

Furthermore, the Freedom of Information Act is designed to place information into the public domain. Once access to information is granted to one person under the Act, it is then considered to be public information and would be communicated to any individual upon request. In accordance with this principle, the MPS operates an applicant-blind and motive-blind approach to FoIA requests and routinely publishes information disclosed under the Freedom of Information Act on the MPS Internet site[1].

The right of access to information is subject to a number of exemptions that are designed to enable public authorities to withhold information that is not suitable for release.

[1] http://www.met.police.uk/foi/disclosure/disclosure_log.htm

The duty to confirm or deny

The Information Commissioner’s Office (ICO) guidance titled ‘When to refuse to confirm or deny information is held’ states[2]:

> *‘In certain circumstances, even confirming or denying that requested information is held can reveal information that falls under an exemption. A public authority may be able to use an exemption to refuse to confirm whether or not it holds information, if either confirming or denying would reveal exempt information in itself.*
>
> *A neither confirm nor deny response is more likely to be needed for very specific requests than for more general or wide ranging requests.*
>
> *It can be important to use a neither confirm nor deny response consistently, every time a certain type of information is requested, regardless of whether the information is actually held or not. For this reason public authorities need to be alert to the possibility of receiving future requests for the same type of information when handling very specific or detailed requests.’*
>
> *‘There are situations where a public authority will need to use the neither confirm nor deny response consistently over a series of separate requests, regardless of whether it holds the requested information. This is to prevent refusing to confirm or deny being taken as an indication of whether information is held. Before complying with section 1(1)(a), public authorities should consider both whether any harm would arise from confirming that information is held and whether harm would arise from stating that no information is held. Otherwise, if the same (or same type of) requests were made on several occasions, a changing response could reveal whether information was held.’*

The ICO’s guidance further explains the harm in issuing a statement confirming or denying whether information is held and demonstrates the following:

- Exempt information may be revealed by:
  - Confirming information is held
  - Confirming information is not held
  - Inconsistently applying neither confirm nor deny (NCND) exemptions in response to the same or similar requests
- It is only necessary to demonstrate the harm in one of the above scenarios for an NCND response to be appropriate
- Cumulative prejudice may result from multiple disclosures
- It would be sufficient for a public authority to demonstrate that a confirmation or denial would be revealing to someone with specialist knowledge
- The wording of a request may determine whether an NCND response is appropriate.

The ICO guidance also states:

[2] https://ico.org.uk/media/for-organisations/documents/1166/when_to_refuse_to_confirm_or_deny_section_1_foia.pdf

‘The exact wording of the request for information is an important consideration when deciding whether a public authority should confirm or deny if it holds the requested information. The more specific the request, the more likely it is that a public authority will need to give a neither confirm nor deny response.’

The MPS needs to be alert to requests for certain types of information, such as requests directly or indirectly relating to law enforcement tactics and capabilities.

The MPS regularly receives requests for information that, if held, could disclose or infer policing tactics and capabilities which would be to the detriment of law enforcement. A hypothetical confirmation that such information is not held could also engage one or more FoIA exemptions.

In the circumstances of your request, a confirmation or denial statement would indirectly relate to law enforcement tactics and/or capabilities.

Due to the need for consistency when neither confirming nor denying whether information is held so as to protect policing information (E.g. Law enforcement tactics and capabilities) it is appropriate in the circumstances of your request for the MPS to neither confirm nor deny whether information is held

Any of the exemptions cited in response to your request (i.e. section 23(5), 24(2), 30(3) and 31(3)) would be sufficient on their own for the MPS to neither confirm nor deny whether the requested information is held. It is also pertinent to note that section 23(5) is a class-based, absolute exemption. Therefore, there is no requirement to demonstrate harm or consider the public interest in relation to section 23(5).

Please refer to the original MPS response to your request (ref:2016110000055) for a full public interest test and harm rationale.

Please note that the rationale presented above is in relation to the duty to confirm whether the information requested is held by the MPS. Therefore, this correspondence neither confirms nor denies whether or not the MPS holds the information requested.

Advice and Assistance

Please find attached ‘Appendix A’ for further guidance in relation to the duty to confirm or deny.

You may be interested in the following ICO decision notices that relate to similar FoIA requests where police forces have used ‘NCND’ exemptions in response to queries that are predicated upon directly or indirectly:

- confirming or denying the use of a potential policing tactic; and/or
- inferring policing capabilities:

ICO Decision Notice FS50622468 (relates to equipment interference)
https://ico.org.uk/media/action-weve-taken/decision-notices/2016/1624502/fs_50622468.pdf

ICO Decision Notice FS50459944 (relates to ‘silent’ SMS calls)
https://ico.org.uk/media/action-weve-taken/decision-notices/2013/825162/fs_50459944.pdf

ICO Decision Notice FS50263467 (relates to documents compiled by Special Branch)
https://ico.org.uk/media/action-weve-taken/decision-notices/2011/579404/fs_50263467.pdf

ICO Decision Notice FS50570727 (relates to RIPA authorisations)
https://ico.org.uk/media/action-weve-taken/decision-notices/2015/1431777/fs_50570727.pdf

The decision notices listed above may also answer the issues raised within your complaint correspondence dated 24/01/2017.

Although the MPS can neither confirm nor deny whether information is held in relation to your request, you may also be interested in the policies, legislation and codes of practice relevant to covert policing linked below:

MPS Surveillance Policy
https://beta.met.police.uk/globalassets/foi-media/policies/met-hq---portfolio--planning---surveillance-policy

MPS Covert Policing Standards Policy
https://beta.met.police.uk/globalassets/foi-media/policies/covert-policing-standards---policy

MPS Covert Policing Standards Policy – Equality Impact Assessment
https://beta.met.police.uk/globalassets/foi-media/policies/covert-policing-standards---equality-impact-assessment

Regulation of Investigatory Powers Act 2000 (RIPA)
http://www.legislation.gov.uk/ukpga/2000/23/contents

RIPA Codes
https://www.gov.uk/government/collections/ripa-codes

College of Policing Authorised Professional Practice (APP): Management of Police Information
https://www.app.college.police.uk/app-content/information-management/management-of-police-information/

Office of Surveillance Commissioners Procedures and guidance 2016
https://osc.independent.gov.uk/wp-content/uploads/2016/07/OSC-Procedures-Guidance-July-2016.pdf

Human Rights Act 1998
http://www.legislation.gov.uk/ukpga/1998/42/contents

Data Protection Act 1998
http://www.legislation.gov.uk/ukpga/1998/29/contents

Police Act 1997
http://www.legislation.gov.uk/ukpga/1997/50/contents

Criminal Procedure and Investigations Act 1996
http://www.legislation.gov.uk/ukpga/1996/25/contents

Police and Criminal Evidence Act 1984 (PACE)
http://www.legislation.gov.uk/ukpga/1984/60/contents

If you are dissatisfied with the outcome of this internal review you have the right to appeal the decision by contacting the Information Commissioner's Office (ICO) for a decision on whether the request for information has been dealt with in accordance with the requirements of the FOIA.

For information on how to make an application to the Information Commissioner please visit their website at www.ico.org.uk. Alternatively, write to or phone:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
Phone: 0303 123 1113

Yours sincerely

Brian Wilson
Information Law Advisor

LEGAL ANNEX

Section 1(1) (General right of access to information held by public authorities) of the Freedom of Information Act 2000 states:

(1) Any person making a request for information to a public authority is entitled—
(a) to be informed in writing by the public authority whether it holds information of the description specified in the request, and
(b) if that is the case, to have that information communicated to him.

http://www.legislation.gov.uk/ukpga/2000/36/section/1

Section 17(1) (Refusal of request) of the Freedom of Information Act 2000 states:

(1)A public authority which, in relation to any request for information, is to any extent relying on a claim that any provision of Part II relating to the duty to confirm or deny is relevant to the request or on a claim that information is exempt information must, within the time for complying with section 1(1), give the applicant a notice which—
(a) states that fact,
(b) specifies the exemption in question, and
(c) states (if that would not otherwise be apparent) why the exemption applies.

http://www.legislation.gov.uk/ukpga/2000/36/section/17

Section 23(1), (3) & (5) (Information supplied by, or relating to, bodies dealing with security matters) of the Act Freedom of Information Act 2000 states:

(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)

(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.

(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).

http://www.legislation.gov.uk/ukpga/2000/36/section/23

Section 24(1) & (2) (National Security) of the Freedom of Information Act 2000 states:

(1) 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.

(2) The duty to confirm or deny does not arise if, or to the extent that, exemption from section 1(1)(a) is required for the purpose of safeguarding national security.

http://www.legislation.gov.uk/ukpga/2000/36/section/24

Section 30(1)(a), 30(2) & 30(3) (Investigations) of the Freedom of Information Act 2000 states:

(1) Information held by a public authority is exempt information if it has at any time been held by the authority for the purposes of-
(a) any investigation which the public authority has a duty to conduct with a view to it being ascertained-
(i) whether a person should be charged with an offence, or
(ii) whether a person charged with an offence is guilty of it

(2) Information held by a public authority is exempt information if—
(a) it was obtained or recorded by the authority for the purposes of its functions relating to—
(i) investigations falling within subsection (1)(a) or (b),
(ii) criminal proceedings which the authority has power to conduct,
(iii) investigations (other than investigations falling within subsection (1)(a) or (b)) which are conducted by the authority for any of the purposes specified in section 31(2) and either by virtue of Her Majesty’s prerogative or by virtue of powers conferred by or under any enactment, or
(iv) civil proceedings which are brought by or on behalf of the authority and arise out of such investigations, and
(b) it relates to the obtaining of information from confidential sources.

(3) The duty to confirm or deny does not arise in relation to information which is (or if it were held by the public authority would be) exempt information by virtue of subsection (1) or (2).

http://www.legislation.gov.uk/ukpga/2000/36/section/30

Section 31(1)(a), 31(1)(b) and 31(3) (Law Enforcement) of the Freedom of Information Act 2000 states:

31 Law enforcement.(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,

(3)The duty to confirm or deny does not arise if, or to the extent that, compliance with section 1(1)(a) would, or would be likely to, prejudice any of the matters mentioned in subsection (1).

BEFORE THE INFORMATION COMMISSIONER

BETWEEN

PRIVACY INTERNATIONAL

Applicant

- and -

METROPOLITAN POLICE SERVICE

Respondent

GROUNDS OF APPEAL

I. Introduction and Summary

1. The Applicant is Privacy International, a registered UK charity, campaigning for the right to privacy.

2. On 1 November 2016, Privacy International wrote to the Metropolitan Police Service (“MPS”), Home Office, National Police Chiefs Council, National Crime Agency, South Yorkshire Police, Avon and Somerset Police and Crime Commissioner (“PCC”), Kent PCC, Staffordshire PCC, Warwickshire PCC, West Mercia PCC and West Midlands PCC, requesting information about the purchase and use of mobile phone surveillance equipment by the police forces and the regulatory and oversight regime governing the use of such equipment. This equipment can be referred to using a range of terms, including “Covert Communications Data Capture” (“CCDC”) equipment, “IMSI Catchers”, “IMSI Grabbers”, “Cell site simulators” and “Stingrays”. In these grounds, this equipment is hereafter referred to as “IMSI Catchers”. Privacy International’s initial request to the MPS is annexed to these grounds as Exhibit A.

3. On 29 November 2016, the MPS responded to the request by stating that it could neither confirm nor deny (“NCND”) whether it held the information requested pursuant to sections 23(5), 24(2), 30(3) and 31(3) of the Freedom of Information Act (“FOIA”) 2000. This response is annexed to these grounds as Exhibit B.

4. On 24 January 2017, Privacy International made a request for internal review of the MPS’s decision. This request is annexed to these grounds as Exhibit C.

5. On 13 June 2017, the MPS upheld its initial decision. This decision is annexed to these grounds as Exhibit D.

6. The MPS’s 13 June 2017 decision was wrong and/or unlawful in that it erred in concluding that:

    a. Legislation, policy guidance and other information governing the use of IMSI Catchers can be subject to an NCND position under a FOIA exemption;

    b. Sections 23(5) and 30(3) FOIA were engaged by the request;

    c. Confirming or denying the existence of the requested information was “required for the purpose of safeguarding national security” pursuant to section 24(2) FOIA;

    d. Confirming or denying the existence of the requested information would or would be likely to prejudice law enforcement pursuant to section 31(3) FOIA;

    e. In all the circumstances of the case, the public interest in neither confirming nor denying whether it held the information requested outweighs the public interest in disclosing the information pursuant to sections 24(2), 30(3) and 31(3) FOIA.

II. The Facts

A. Privacy International

7. Privacy International is a UK-registered charity. It was founded in 1990 as the first organisation to campaign at an international level on privacy issues. Its mission is to defend the right to privacy across the world, by investigating and challenging unlawful surveillance and other intrusions into private life by governments and corporations. Recent cases brought by Privacy International include a challenge to the lawfulness of the bulk interception of internet traffic by the UK security and intelligence services (*10 Human Rights Organisations v United Kingdom*, European Court of Human Rights, App. No. 24960/15) and a challenge to the blanket exemption of the Government Communications Headquarters under FOIA (*Privacy International v United Kingdom*, European Court of Human Rights, App. No. 60646/14).

8. Privacy International has played a long-standing role in campaigning on privacy and surveillance issues and has a particular interest in the purchase and use of mobile surveillance equipment by the police forces throughout the UK and in the regulatory and oversight regime that governs the use of such equipment.

B. IMSI Catchers

9. IMSI Catchers are surveillance devices used to collect mobile phone data and track individuals’ locations. IMSI stands for “International Mobile Subscriber Identity”, a

number unique to Subscriber Identification Module (“SIM”) cards.[1] Mobile phones communicate with a network of base stations, which enable the network provider to route calls, text messages and internet data to and from the mobile phone. IMSI Catchers function by impersonating a base station, tricking mobile phones into connecting to them. Once connected to an IMSI Catcher, mobile phones identify themselves by revealing their IMSI. This identification process also allows IMSI Catchers to determine the location of mobile phones. Some IMSI Catchers also have the capability to intercept data, including calls, text messages, and internet data, as well as block service, either to all mobile phones within their range or to select devices.

10. IMSI Catchers can interfere with the right to privacy in several ways. Where they intercept the data transmitted from mobile phones, such as calls, text messages, and internet data, they pose the same privacy concerns as traditional methods of communications surveillance.

11. The interception of IMSI/IMEI data can also raise several privacy concerns. A mobile phone is “*very intimately linked to a specific individual*”, meaning IMSI/IMEI data can also be tied to specific individuals.[2] By linking IMSI/IMEI data to other information, the government can not only determine the identity of individuals, but also track and profile those individuals. For example, by tracking IMSI/IMEI data across a number of locations, the government can create a profile of an individual’s activities and contacts.

12. The use of IMSI Catchers also raises particular concerns because of the indiscriminate nature by which they collect data. IMSI Catchers trick all mobile phones within a given range to identify themselves and reveal their location. Their use can therefore interfere with the privacy rights of many persons, including those who are not the intended targets of surveillance.

13. The indiscriminate nature by which IMSI Catchers collect data means that their use can also interfere with the rights to freedom of expression and to freedom of assembly and association. The police forces can use IMSI Catchers at gatherings of individuals, such as a protest, to identify those attending such gatherings.

14. Finally, the use of IMSI Catchers has a number of implications for the ability of individuals to maintain their anonymity, including when attending a gathering. There are inextricable linkages between anonymity, privacy, and freedom of expression.[3]

[1] IMSI Catchers typically also collect the “International Mobile Station Equipment Identifier” (“IMEI”) of mobile phones. The IMEI is unique to each mobile phone whereas the IMSI is unique to each SIM card.
[2] Article 29 Data Protection Working Party, Opinion 13/2011 on Geolocation Services on Smart Mobile Devices, 881/11/EN, 16 May 2011, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp185_en.pdf.
[3] *See* Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, U.N. Doc. A/HRC/29/32, 22 May 2015, available at http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/29/32; *see also* Written Submissions on Behalf of

15. There has been disquiet about the use of IMSI Catchers and speculation as to whether they are operational in the UK. IMSI Catchers have been reported in other countries in Europe, including Germany, where their use is regulated by federal law and subject to a series of safeguards. Those safeguards include requiring prior judicial authorisation for law enforcement agencies’ use of IMSI Catchers and only where there are grounds indicating that an individual has committed or is going to commit a specific serious crime and only to the extent necessary to determine that individual’s mobile IMSI/IMEI or whereabouts.[4] IMSI Catchers are also reported in use in the United States, where at the federal level, the Department of Justice has announced a policy requiring that all agencies obtain a search warrant supported by probable cause prior to using an IMSI Catcher.[5]

16. In 2014, the use of IMSI Catchers was described in a response in Hansard:

> “*Investigative activity involving interference with property or wireless telegraphy, such as International Mobile Subscriber Identity (IMSI) grabbers, is regulated by the Police Act 1997 and the Intelligence Services Act 1994 which set out the high level of authorisation required before the police or Security and intelligence agencies can undertake such activity. Use of these powers is overseen by the Intelligence Services Commissioner and the Office of Surveillance Commissioners. In any case involving the interception of the content of a communication, a warrant authorised by the Secretary of State under the Regulation of Investigatory Powers Act 2000 is required*.”[6]

17. On 10 October 2016, an article appeared in *The Bristol Cable* entitled: “Revealed: Bristol’s police and mass mobile phone surveillance.”[7] The article makes reference to the purchase of equipment from the company CellXion by the MPS under the item “CCDC” for the cost of £1,037,223. The article links to the original document disclosing the purchase, which at that time, could also be found on the MPS website.[8] The article also explains that the acronym “CCDC equipment” appears to refer to “covert communications data capture” as spelled out in the minutes of an Alliance Governance Group meeting in May 2016 between Warwickshire and West Mercia Police.[9]

18. On the same day, *The Guardian* published the article “Controversial snooping technology

---

Privacy International and Article 19, *Breyer v Germany*, European Court of Human Rights, App. No. 50001/12, 5 Sept. 2016.
[4] Section 100i of the *Criminal Procedure Code* (*Strafprozessordnung*, StPO) (Germany), available at https://www.gesetze-im-internet.de/englisch_stpo/englisch_stpo.html.
[5] 2015 U.S. Department of Justice Policy, available at https://www.justice.gov/opa/file/767321/download.
[6] Electronic Surveillance: Written question – HL2602, 3 Nov. 2014, available at http://www.parliament.uk/business/publications/written-questions-answers-statements/written-question/Lords/2014-11-03/HL2602.
[7] Alon Aviram, “Revealed: Bristol’s police and mass mobile phone surveillance,” The Bristol Cable, 10 Oct. 2016, https://thebristolcable.org/2016/10/imsi/.
[8] http://www.met.police.uk/foi/pdfs/lists_and_registers/corporate/contracts_over_%C2%A32500_q3_october2015_january2016.pdf
[9] https://thebristolcable.org/wp-content/uploads/2016/10/09-imsi-4.pdf

‘used by at least seven police forces’”.[10] The article reported that “*surveillance technology that indiscriminately harvests information from mobile phones*”, also “*known as an IMSI catcher*” is being “*used by at least seven police forces across the country…according to police documents*.” It further reported that the MPS was one of the “*forces understood to be using*” this technology.

19. The Investigatory Powers Act 2016 does not explicitly address the use of IMSI Catchers.

III. Procedural History

A. Request for Information

20. On 1 November 2016, Privacy International requested the following information from the MPS:

1. *Purchase orders, invoices, contracts, loan agreements, solicitation letters, correspondence with companies and other similar records regarding the Metropolitan Police’s acquisition of CCDC equipment. Please include records of all purchase orders, invoices, contracts, agreements, and communications with CellXion.*

2. *Marketing or promotional materials received by the Metropolitan Police relating to CCDC equipment.*

3. *All requests by CellXion or any other corporation, or any government agency, to the Metropolitan Police to keep confidential any aspect of Metropolitan Police’s possession and use of CCDC equipment, including any non-disclosure agreements between Metropolitan Police and CellXion or any other corporation, or government agency, regarding the Metropolitan Police’s possession and use of CCDC equipment.*

4. *Legislation, codes of practice, policy statements, guides, manuals, memoranda, presentations, training materials or other records governing the possession and use of CCDC equipment by the Metropolitan 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.*

[10] David Pegg & Rob Evans, “Controversial snooping technology ‘used by at least seven police forces,’” The Guardian, 10 Oct. 2016, https://www.theguardian.com/world/2016/oct/10/controversial-phone-snooping-technology-imsi-catcher-seven-police-forces.

B. The Refusal

21. On 29 November 2016, a Privacy Advisor in the Information Rights Unit for the MPS refused the request on grounds that it could NCND whether it held the information requested pursuant to sections 23(5), 24(2), 30(3), and 31(3) FOIA.

22. The reasons given for the overall harm identified for NCND were as follows:

    a. Confirming or denying that the MPS holds any information regarding these techniques would in itself disclose exempt information. Stating information is held would confirm usage and the opposite if there is no such information. Although the techniques are in the public domain, it is how and when they might be used, that are the sensitive issues for the police service. They could be deployed for high profile sensitive operations, albeit not in the MPS force area, therefore the NCND position is required to protect other forces that may use them.

    b. Any disclosure under FOIA 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) the MPS may or may not deploy in specific circumstances would prejudice law enforcement. If the requested information was held by the MPS, confirmation of this fact would reveal that the MPS 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 MPS’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 MPS may be aware of their presence and taking counter terrorist measures.

    c. Conversely, if information was not held by the MPS, and a denial was issued, this would reveal to those same individuals that their activities are unlikely to have been detected by the MPS. It may also suggest (whether correctly or not) the limitations of the MPS’s 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 capacity by forces would substantially prejudice the ability of the MPS to police their area which would lead to a greater risk to the public.

d. This detrimental effect is increased if the request is made to several law enforcement bodies as those committing crimes of drugs and terrorist activities would be able to ‘map’ where the use of certain tactics are or are not deployed. This could have the likelihood of identifying location-specific operations and could lead to them moving their operations, destroying evidence, or avoiding those areas, ultimately compromising police tactics, operations and future prosecutions.

e. 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.

23. With respect to the public interest test, the MPS indicated as factors favouring and against confirming or denying the existence of the requested information:

> “***Factors favouring confirming or denying whether any other information is held for Section 24***
> *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 24***
> *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 infra-structure 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 30***
> *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 30***
> *By confirming or denying the use of specialist techniques, the MPS’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 31***
> *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 31
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.”

24. The MPS acknowledged that while “*there is a public interest in the transparency of policing operations and in this case providing assurance that the MPS 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*.” Moreover, the MPS submitted that “*[a]s 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*” and that there is “*no requirement to satisfy any public concern over the legality of police operations and the tactics we may or may not use*.”

25. The MPS concluded that “*the balancing test for confirming or denying whether any information is held regarding these techniques is not made out*” and that “*[t]his argument is obviously transferable to all police tactics*.”

C. Request for Internal Review

26. On 24 January 2017, Privacy International challenged the refusal on five grounds.

27. First, Privacy International submitted that the MPS’s response was predicated on a series of *non-sequiturs*:

    a. It simply does not follow that merely confirming or denying that a police force uses IMSI catchers would reveal operationally sensitive information about the scope of police activities and operations. This reasoning is not understood. It appears that the MPS has confused consideration of NCND with consideration of the provision of information itself;

    b. Equally, it does not follow that making the same request to multiple police forces could allow individuals to map or be aware of how operationally sensitive information is obtained by the various police forces. Different police forces could obtain information in multiple ways. Confirming or denying that a police force holds the requested information does not automatically reveal how tactics are deployed or what technical operations each force has;

    c. It is not understood why revealing that a police force has sophisticated capabilities

to analyse data would limit operational capabilities. The reasoning set out in this respect is nonsensical.

28. Second, Privacy International submitted that the refusal failed to have regard to obviously material considerations, including, but not limited to:

    a. The fact that the MPS’s purchase of IMSI catchers is already in the public domain, as set out in Privacy International’s original request;

    b. The fact that the legislative provisions and/or policy guidance requested cannot conceivably fall within any exemption;

    c. The significant public interest in the topic of IMSI catchers and the regulation of related communications surveillance technologies.

29. Third, Privacy International submitted that when considered forensically, the exemptions relied upon do not apply:

    a. Under Section 23(5) FOIA, there has to be a realistic possibility that a security body would be involved in the issue the request relates to in order for the exemption to apply. No such possibility has been set out. Any possibility that is particularised would be too remote to justify the application of this exemption;

    b. Section 24(2) FOIA provides an exemption from the duty to confirm information is held, where the exemption is required for the purposes of safeguarding national security. Section 31(3) also provides an exemption where it is necessary for the prevention or detection of crime. No real reasons have been set out as to why either exemption applies. By way of example, it cannot seriously be suggested that it would damage national security and/or the prevention or detection of crime to confirm or deny the existence of legislative powers and/or policy guidance;

    c. Section 30(3) FOIA provides that the duty to confirm or deny does not arise in relation to information which is exempt information by virtue of sections 30(1) or (2). Section 30(1) can only be claimed by public authorities that have a duty to investigate whether someone should be charged with an offence, or the power to conduct such investigations and/or institute criminal proceedings. Section 30(2) protects the identity of confidential sources, primarily to ensure informants are not deterred from supplying law enforcement agencies with valuable intelligence. ICO guidance makes clear that the section 30 exemptions “*exist to ensure the effective investigation and prosecution of offences and the protection of confidential sources. They recognise the need to prevent disclosures that would prejudice either a particular investigation or set of proceedings, or the investigatory and prosecution processes generally, including any prejudice to future investigations*

and proceedings.”[11] None of these matters have been addressed in the response to the request. There is no risk of prejudice to a specific investigation, there is no risk to informants, and there is no risk to confidential sources.

30. Fourth, Privacy International submitted that as regards the qualified exemptions (*i.e.* sections 24(3), 30(3) and 31(3) FOIA) relied upon, the public interest balancing exercise fell squarely in favour of disclosure:

    a. No meaningful reasons have been provided as to why there is a public interest in neither confirming nor denying the matters requested in this request;

    b. There is currently no evidence at all to suggest that the public interest will be harmed to any material extent by disclosure of the information sought;

    c. The public interest in disclosure is real, it is important that the public are reassured that the measures used to safeguard national security are proportionate and effective;

    d. No regard at all has been had to the public interest in the disclosure of the information requested. There is currently a wide-ranging public debate taking place on the ambit of privacy rights in the context of surveillance and technology. There has also been widespread coverage of the purchase and use of IMSI Catchers by police forces across the country. In limiting its consideration of the public interest to “*the transparency of policing operations*”, the MPS failed to have regard to obviously material considerations.

31. Finally, Privacy International submitted that when relying upon the NCND position pursuant to one of the exemptions, it is necessary to have regard to the language and purpose of FOIA, which require exemptions to be narrowly construed:

    a. The word “*required”* in section 1(1)(a) FOIA “*…means reasonably necessary. It is not sufficient for the information sought simply to relate to national security; there must be a clear basis for arguing that disclosure would have an adverse effect on national security before the exemption is engaged*”;[12]

    b. It is therefore clear that a decision to NCND requires a clear justification and merits close scrutiny. This is because it flies in the face of the “*default setting*” in FOIA, which is in favour of disclosure.[13] It also flies in the face of the Article 10

[11] *See* Information Commissioner’s Office, Investigations and proceedings (section 30), Freedom of Information Act, §53, available at https://ico.org.uk/media/for-organisations/documents/1205/investigations-and-proceedings-foi-section-30.pdf.
[12] *Philip Kalman v Information Commissioner and the Department of Transport* (EA/2009/111 8 July 2010).
[13] *Galloway v Information Commissioner v The Central and North West London NHS Foundation Trust* (2009) 108 BMLR 50, at §70.

right to receive information, as recently confirmed by the European Court of Human Rights;[14]

c. This submission reflects the approach taken to NCND in parallel contexts. An NCND decision “*requires justification similar to the position in relation to public interest immunity...It is not simply a matter of a governmental party to litigation hoisting the NCND flag and the court automatically saluting it*”.[15]

D. Decision in Response to Request for Internal Review

32. On 13 June 2017, an Information Law Advisor at the MPS responded by upholding the original decision.

33. The Advisor cited from the ICO guidance on “When to refuse to confirm or deny information is held” and explained its NCND position as follows:

> “*The MPS needs to be alert to requests for certain types of information, such as requests directly or indirectly relating to law enforcement tactics and capabilities.*
>
> *The MPS regularly receives requests for information that, if held, could disclose or infer policing tactics and capabilities which would be to the detriment of law enforcement. A hypothetical confirmation that such information is not held could also engage one or more FOIA exemptions*.
>
> *In the circumstances of your request, a confirmation or denial statement would indirectly relate to law enforcement tactics and/or capabilities.*
>
> *Due to the need for consistency when neither confirming nor denying whether information is held so as to protect policing information (E.g. Law enforcement tactics and capabilities) it is appropriate in the circumstances of your request for the MPS to neither confirm nor deny whether information is held.*
>
> *Any of the exemptions cited in response to your request (i.e. section 23(5), 24(2), 30(3) and 31(3)) would be sufficient on their own for the MPS to neither confirm nor deny whether the requested information is held. It is also pertinent to note that section 23(5) is a class-based, absolute exemption. Therefore, there is no requirement to demonstrate harm or consider the public interest in relation to section 23(5).*”

34. The Advisor then indicated that Privacy International should “*refer to the original MPS*

[14] *Magyar Helsinki Bizottság v Hungary*, European Court of Human Rights, App. No. 18030/11, 8 Nov. 2016.
[15] *Mohamed and Another v Secretary of State for the Home Department* [2014] 1 WLR 4240, per Maurice Kay LJ, at §40.

response” to the request “*for a full public interest test and harm rationale*.”

IV. The Appeal

A. The Purpose of FOIA

35. The purpose of FOIA as part of the modern constitutional fabric of the law means that exemptions must be construed narrowly. To hold otherwise would fly in the face of FOIA, which is in favour of disclosure, and the right to receive information under Article 10 of the European Convention on Human Rights.

36. There is a high degree of consensus under international law that access to information is part of the right to freedom of expression. In particular, the Commissioner should have regard to the Grand Chamber decision in *Magyar Helsinki Bizottság v Hungary*.[16] That case concerned the rejection by the police of an access to information request submitted by the applicant, an NGO. The Court affirmed a right to access to information and emphasised the importance of this aspect of freedom of expression, which operates to provide transparency on the conduct of public affairs and on matters of society as a whole.[17]

37. The Court also emphasised the important role of watchdogs in a democracy in providing information of value to political debate and discourse. It explained the concept of a public watchdog as follows:

> *“167. The manner in which public watchdogs carry out their activities may have a significant impact on the proper functioning of a democratic society. It is in the interests of democratic society to enable the press to exercise its vital role of ‘public watchdog’ in imparting information on matters of public concern (see Bladet Tromsø and Stensaas, cited above, § 59), just as it is to enable NGOs scrutinising the State to do the same thing. Given that accurate information is a tool of their trade, it will often be necessary for persons and organisations exercising watchdog functions to gain access to information in order to perform their role of reporting on matters of public interest. Obstacles created in order to hinder access to information may result in those working in the media or related fields no longer being able to assume their ‘watchdog’ role effectively, and their ability to provide accurate and reliable information may be adversely affected (see Társaság, cited above, § 38).*

[16] *Magyar Helsinki Bizottság v Hungary*, European Court of Human Rights, App. No. 18030/11, 8 Nov. 2016.
[17] The right to access to information is also recognised by numerous other international human rights instruments and mechanisms. *See, e.g.*, Article 19, International Covenant on Civil and Political Rights; U.N. Human Rights Committee, General Comment No. 34, U.N. Doc. No. CCPR/C/GC/34, 12 Sept. 2011; U.N. Special Rapporteur on Freedom of Opinion and Expression, OSCE Representative on Freedom of the Media, OAS Special Rapporteur on Freedom of Expression, ACHPR on Freedom of Expression, Joint Declaration, 20 Dec. 2006; U.N. Special Rapporteur on Freedom of Opinion and Expression, OSCE Representative on Freedom of the Media, OAS Special Rapporteur on Freedom of Expression, Joint Declaration, 6 Dec. 2004.

168. Thus, the Court considers that an important consideration is whether the person seeking access to the information in question does so with a view to informing the public in the capacity of a public ‘watchdog’.”

38. As a human rights organisation, Privacy International plays the role of a watchdog, similar to that played by the press.[18] Indeed, in litigation before the European Court of Human Rights, the UK Government has accepted that “*NGOs engaged in the legitimate gathering of information of public interest in order to contribute to public debate may properly claim the same Art. 10 protections as the press.”*[19] Privacy International seeks to advance the right to privacy around the world, including in the UK. It carries out this work, in part, by conducting research on a variety of issues related to privacy and surveillance and publishing that research in multiple formats, including research reports, policy papers and blog posts. It seeks information about IMSI Catchers in order to educate the public about the government’s use of this surveillance technology and its human rights implications, including for the right to privacy.

39. It may also be useful in this respect to consider a comparative perspective. In the United States, a range of requests pursuant to federal and state freedom of information laws relating to law enforcement use and regulation of IMSI Catchers have successfully disclosed relevant records, including purchase records, product descriptions, non-disclosure agreements and policy guidance. These records were disclosed notwithstanding exemptions under the relevant laws protecting certain categories of information, including information classified to protect national security and information related to law enforcement techniques and procedures. A summary of these requests and the subsequent disclosure of records are annexed to these grounds as Exhibit E.

B. Section 23(5) FOIA

40. By virtue of section 23(5) FOIA 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, which was directly or indirectly supplied to the public authority by, or which relates to, any of the bodies specified in section 23(3).

41. In a recent decision relating to IMSI Catchers, the Commissioner held that in assessing the engagement of section 23(5), “*the balance of probabilities is the correct test to apply*”, meaning that “*the evidence must suggest to a sufficient degree of likelihood (rather than certainty) that any information falling within the scope of the request would relate to, or have been supplied by, a body specified in section 23(3)*”. The Commissioner proceeded to apply this test to *“the subject matter of the request – data capture from*

[18] *See Társaság a Szabadságjogokért v Hungary*, App. No. 37374/05, 14 April 2009.
[19] The United Kingdom’s Observations on the Merits, *10 Human Rights Organisations v United Kingdom*, App. No. 24960/15, 14 April 2016, §6.1.

mobile phones” and found it to be *“within the area of the work of bodies specified in section 23(3).*” The Commissioner continued that “*[t]his view is strengthened by the citation [from Hansard] which states that any use of IMSI technology would be regulated by the Police Act 1997 and the Intelligence Services Act 1994.”* The Commissioner further accepted that it was likely that “*if the information described in the request does exist, this would be a field of work which is likely to have been conducted in conjunction with, and with the knowledge, of other parties within the policing field, and that this type of work is likely to include security bodies*.” The Commissioner submitted that if “*the information requested is within what could be described as the ambit of security bodies' operations, section 23(5) is likely to apply*” and that *“[f]actors indicating whether a request is of this nature will include the functions of the public authority receiving the request, the subject area to which the request relates and the actual wording of the request*.” Finally, the Commissioner noted that “*there is clearly a close relationship between the police service and the security bodies*” and therefore, “*on the balance of probabilities, any information about its potential use of IMSI technology, if held, could be related to one of more bodies identified in section 23(3) of the FOIA*.”[20]

42. Privacy International respectfully submits that this decision should be distinguished and revisited on the following basis:

    a. Privacy International’s request includes *legislation, policy guidance and other information* governing the use of IMSI Catchers held by the MPS and therefore is not information falling within the area of the work of bodies specified in section 23(3) FOIA. As a threshold matter, these records, which relate to the legal basis for a public authority’s powers and activities and the rules governing those powers and activities, cannot be subject to NCND under any exemption. The principle of legality and the presumption of disclosure in FOIA must be properly considered and weighed against the position taken by the MPS;

    b. Privacy International’s request further seeks information relating to the use of IMSI Catchers *by police forces*. Just because IMSI Catchers may also be used by the bodies specified in section 23(3) is not enough for section 23(5) to be engaged. There are many techniques – ranging from the simple to the sophisticated – that both the police forces and the section 23(3) bodies may deploy. For that reason, the reliance on the argument that both the Police Act 1997 and the Intelligence Services Act 1994 cover a technique is meaningless. For example, both pieces of legislation authorise the power to interfere with property, which may include entry onto a property. A logical extension of this argument would engage section 23(5) for any technique covered by both

[20] ICO, Decision Notice, Ref. FS50665716, 13 June 2017, paras. 18-19, 21, 23-24, available at https://ico.org.uk/media/action-weve-taken/decision-notices/2017/2014285/fs50665716.pdf; *see also* ICO Decision Notice, Ref. FS50660527, 8 June 2017, paras. 16-19, 24-25 available at https://ico.org.uk/media/action-weve-taken/decision-notices/2017/2014349/fs50660527.pdf.

statutes. Similarly, reliance on the argument that there is a close relationship between the police forces and security bodies is dangerously vague. Indeed, a logical extension of that argument would engage section 23(5) for any technique deployed by the police forces. The MPS have made no attempt to indicate the circumstances in which police forces use IMSI Catchers, which could include ordinary law enforcement activities such as tracking a suspect for a variety of offences, and how those circumstances in any way relate to the section 23 bodies.

C. Section 24(2) FOIA

43. By virtue of section 24(2) FOIA, the duty to confirm or deny does not arise if, or to the extent that, exemption from section 1(1)(a) is required for the purpose of safeguarding national security.

44. With regards to section 24(2), the Commissioner has recently held in a decision on IMSI Catchers that consideration of this exemption is a “*two-stage process*”: first, the exemption must be engaged “*due to the requirement of national security*” and second, the exemption is “*qualified by the public interest, which means that the confirmation or denial must be provided if the public interest in the maintenance of the exemption does not outweigh the public interest in disclosure*.”[21]

45. The Commissioner has also previously held that *“this exemption should be interpreted so that it is only necessary for a public authority to show that either a confirmation or a denial of whether requested information is held would be likely to harm national security. The Commissioner interprets the phrase ‘required’ in the context of this exemption as ‘reasonably necessary’. In effect this means that there has to be a risk of harm to national security for the exemption to be relied upon, but there is no need for a public authority to prove that there is a specific, direct or imminent threat’.”*[22]

46. In the recent decision on IMSI catchers, the Commissioner found that there was some valid public interest in confirmation or denial and that this would increase public knowledge regarding the extent, or otherwise, of the use of IMSI catchers, by Nottinghamshire Police, which may give an indication regarding their use by the police service as a whole. However, the Commissioner determined that this interest was outweighed by that in safeguarding national security.[23]

i. Safeguarding National Security

[21] ICO, Decision Notice, Ref. FS50665716, 13 June 2017, para. 26; *see also* ICO Decision Notice, Ref. FS50660527, 8 June 2017, para 27.
[22] ICO, Decision Notice, Ref. FS50622468, 13 June 2016, para. 22, available at https://ico.org.uk/media/action-weve-taken/decision-notices/2016/1624502/fs_50622468.pdf.
[23] ICO, Decision Notice, Ref. FS50665716, 13 June 2017, paras. 29-30; *see also* ICO Decision Notice, Ref. FS50660527, 8 June 2017, paras. 30-31.

47. In the recent decision on IMSI Catchers, the Commissioner discussed the first prong of the section 24(2) FOIA exemption and relied heavily on the justification that because the Commissioner had already found section 23(5) to be engaged, section 24(2) would also be engaged, since “*a disclosure that touches on the work of the security bodies would consequentially undermine national security*.”[24]

48. As discussed above, in relation to the section 23(5) exemption, the request includes legislation, policy guidance and other information governing the use of IMSI Catchers by the MPS. These records, which relate to the legal basis for a public authority’s powers and activities and the rules governing those powers and activities, cannot be subject to NCND under any exemption. Moreover, the police forces could use IMSI Catchers in a wide range of operations, including for ordinary law enforcement activities, that bear no relation to the bodies specified in section 23(3). The MPS have made no attempt to indicate the circumstances in which police forces use IMSI Catchers and how those circumstances relate in any way to the section 23 bodies. It has therefore failed to demonstrate the engagement of either the section 23(5) or 24(2) exemption.

49. The MPS also base arguments around national security on skeletal assertions that national security would be impacted by (1) at a general level, confirming or denying the use of “*specialist techniques*” and (2) at a specific level, indicating that a technique is used one area but not in another area. Both arguments are baseless. As to the first argument, the MPS do not define a “specialist technique” and why IMSI Catchers constitute a specialist technique. Furthermore, it does not follow that merely confirming or denying that a police force uses IMSI Catchers reveals operationally sensitive information that would negatively impact national security. In fact, the government has willingly admitted and subjected to either public regulation or FOIA requests the use of a variety of what might also be considered “specialist techniques” – from hacking[25] to the use of equipment to physically extract mobile phone data.[26] There is therefore no reason that information governing the use of IMSI Catchers by police forces should be afforded special protection. As to the second argument, it does not follow that determining which police forces use this equipment could permit individuals to map or be aware of how operationally sensitive information is obtained, thereby negatively impacting national security. Different police forces will obtain information in many different ways.

ii. Public Interest Test

50. The original decision identified as the factor against confirming or denying the existence

[24] ICO, Decision Notice, Ref. FS50665716, 13 June 2017, para. 27; *see also* ICO Decision Notice, Ref. FS50660527, 8 June 2017, para. 29.
[25] *See* Part 5, Investigatory Powers Act; *see also* Equipment Interference: Draft Code of Practice.
[26] *See* Disclosure by the Metropolitan Police, https://www.met.police.uk/globalassets/foi-media/disclosure_2017/april_2017/information-rights-unit--mobile-phone-data-extraction-carried-out-at-local-police-station-and-hubs.

of the requested information that “*confirming or denying the use of specialist techniques could render [s]ecurity measures less effective*” and that “*[t]his 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*.” The Commissioner should not accept these bare assertions. As discussed above, the MPS has not clarified what constitutes a “specialist technique” or why confirming or denying the mere existence of such techniques generally or IMSI Catchers specifically could render security measures less effective. This position runs contrary to the government’s explicit regulation of other operational capabilities of the police forces of FOIA disclosures relating to such capabilities. Furthermore, the MPS has presented no evidence of risk to support its position.

51. The original decision only identified as a factor in favour of confirming or denying the existence of the requested information that “*[t]he public is entitled to know where its public funds are spent and a better informed public can take steps to protect themselves*”. The MPS has failed to consider that there is public interest in citizens being informed about methods of surveillance that could have a profound impact on their fundamental rights, including the rights to privacy, freedom of expression and freedom of assembly and association. In particular, there is significant public interest in the topic of IMSI Catchers and the regulation of related communication surveillance technologies. Indeed, because IMSI Catchers can indiscriminately collect data (by tricking all mobile phones within a given range to identify themselves and reveal their location), their use can interfere with the rights of many persons, including those who are not the intended targets of surveillance.

52. It is also worth considering that the European Court of Human Rights has placed particular emphasis on the public interest in the disclosure of matters of public concern. The Grand Chamber in *Magyar Helsinki Bizottság v Hungary* set out a number of relevant factors in its consideration of access to information under Article 10. These include:

    a. The purpose of the information being sought;
    b. The nature of information sought (i.e. the public interest);
    c. The role of the applicant;
    d. The availability of the information.

53. With respect to the public interest, the Court stated that “*the public interest relates to matters which affect the public to such an extent that it may legitimately take an interest in them, which attract its attention or which concern it to a significant degree, especially in that they affect the well-being of citizens of the life of the community*”.[27] As discussed above, IMSI Catchers engage the public interest because their use implicates the

[27] *Magyar Helsinki Bizottság v Hungary*, European Court of Human Rights, App. No. 18030/11, 8 Nov. 2016, para. 162.

fundamental rights of many citizens, Privacy International seeks this information in its role as a public watchdog, and it intends to use the information requested to educate the public about the use of IMSI Catchers and their human rights implications.

54. The *Magyar Helsinki Bizottság* decision’s reasoning on public interest effectively affirmed a prior decision in *Youth Initiative for Human Rights v Serbia*, which concerned an NGO that was monitoring the implementation of transitional laws in Serbia with a view to ensuring respect for human rights.[28] The applicant NGO requested the intelligence agency of Serbia to provide it with factual information concerning the use of electronic surveillance measures by that agency. The Court held that the NGO was involved in the legitimate gathering of information of public interest with the intention of imparting that information to the public and thereby contributing to the public debate.

55. As set out previously to the MPS and as explained above, the public interest balancing exercise falls squarely in favour of disclosure.

    a. No meaningful reasons have been provided as to why there is a public interest in neither confirming nor denying the information sought in this request;

    b. There is currently no evidence at all to suggest that the public interest will be harmed to any material extent by disclosure of the information sought;

    c. The public interest in disclosure is real, it is important that the public are reassured that the measures used to safeguard national security are necessary and proportionate as well as effective. Access to the information would allow for a fact-based public debate on surveillance measures. This has been hindered by the decision of the MPS to NCND the information in question.

    d. The applicant plays an important watchdog role and has requested the information as part of this function. Given the public interest nature of the issue on which Privacy International seeks to obtain information, its activities as a public watchdog warrant a high level of protection, and its role as a watchdog should be taken into account when evaluating the public interest in this matter.

    e. The fact that IMSI Catchers have been purchased by UK police forces is already in the public domain. The MPS have specifically been named in this regard.

[28] *Youth Initiative for Human Rights v Serbia*, European Court of Human Rights, App. No. 48135/06, 25 June 2013.

D. Section 30(3) FOIA

56. Pursuant to section 30(3) FOIA, the duty to confirm or deny does not arise if the information would be exempt by virtue of sections 30(1) or 30(2), which relate to information held for the purposes of investigations and proceedings or obtained from confidential sources.

57. The Commissioner has held that consideration of section 30(3) FOIA "*involves two stages; first, the information described in the request must fall within the classes described in sections 30(1) or 30(2). Secondly, the exemption is qualified by the public interest. This means that if the public interest in the maintenance of the exemption does not outweigh the public interest in confirming or denying whether information is held, then confirmation or denial must be provided*."[29]

i. Investigations, Proceedings and Confidential Sources

58. Again, as discussed above, in relation to the section 23(5) and 24(2) exemptions, the request includes legislation, policy guidance and other information governing the use of IMSI Catchers by the MPS. These records, which relate to the legal basis for a public authority's powers and activities and the rules governing those powers and activities, cannot be subject to NCND under any exemption.

59. The MPS has provided no explanation as to how the information requested falls within the categories of information described in sections 30(1) or 30(2) FOIA. As a point of comparison, the Commissioner has found a request to fall into such a category where it contained a "*specific reference to a crime reference number which…related to the incident he was asking about*."[30] By contrast, Privacy International's request neither contains references to nor relates to any investigations or proceedings (or, for that matter, to information obtained from confidential sources). Rather, the requested information relates to the purchase of IMSI Catchers and the regulatory and oversight regime governing their use.

ii. Public Interest Test

60. The original decision identified as the factor against confirming or denying the existence of the requested information that "*confirming or denying the use of specialist techniques*" would affect "*the force's future law enforcement capabilities…and…would hinder the prevention and detection of crime*". Notably, this factor says nothing about the effect of confirming or denying the existence of the requested information on investigations, proceedings or confidential informants, strengthening Privacy International's argument

[29] ICO, Decision Notice, Ref. FS50689520, 18 Dec. 2017, para. 17, available at https://ico.org.uk/media/action-weve-taken/decision-notices/2017/2172938/fs50689520.pdf.
[30] *Id*. at para. 20.

above that the MPS has failed to explain how the request falls within the section 30(1) or 30(2) FOIA categories of information.

61. Nevertheless, as with the factors against confirming or denying the existence of the requested information under section 24(2), the Commissioner should not accept such bare assertions. Again, the MPS has not clarified what constitutes a “specialist technique” or why confirming or denying the mere existence of such techniques generally or IMSI Catchers specifically in any way impact investigations, proceedings or information obtained from confidential informants. This position also runs contrary to the government’s explicit regulation of other operational capabilities of the police forces or FOIA disclosures relating to such capabilities. Furthermore, the MPS has presented no evidence of risk to support its position.

62. The original decision identified as factors in favour of confirming or denying the existence of the requested information that “*[t]he public are entitled to know what their public funds are spent on*” and that “*[i]nvestigations may be closed and any proceedings may have been completed, and the investigations may have been high profile and had national implications*.” As discussed above, the MPS has failed to consider that there is a public interest in citizens being informed about methods of surveillance that could have a profound impact on their fundamental rights, including the rights to privacy, freedom of expression and freedom of assembly and association.

63. Finally, as discussed above, it is also worth considering the European Court of Human Right’s recent jurisprudence on access to information under Article 10, which emphasises the public interest in disclosing matters of public concern, especially where they affect the rights of citizens.

64. Thus, as set out previously to the MPS and as explained above, the public interest balancing exercise falls squarely in favour of disclosure.

    a. No meaningful reasons have been provided as to why there is a public interest in neither confirming nor denying the information sought in this request;

    b. There is currently no evidence at all to suggest that the public interest will be harmed to any material extent by confirming or denying the existence of the information sought;

    c. The public interest in disclosure is real, it is important that the public are reassured that the measures used to safeguard national security are necessary and proportionate as well as effective. Access to the information would allow for a fact-based public debate on surveillance measures. This has been hindered by the decision of the MPS to NCND the information in question.

    d. The applicant plays an important watchdog role and has requested the

information as part of this function. Given the public interest nature of the issue on which Privacy International seeks to obtain information, its activities as a public watchdog warrant a high level of protection, and its role as a watchdog should be taken into account when evaluating the public interest in this matter.

e. The fact that IMSI Catchers have been purchased by UK police forces is already in the public domain. The MPS have specifically been named in this regard.

E. Section 31(3) FOIA

65. Pursuant to section 31(3) FOIA, the duty to confirm or deny does not arise if, or to the extent that, compliance with section 1(1)(a) would, or would be likely to, prejudice a range of matters related to law enforcement, including, *inter alia*, the prevention or detection of crime or the apprehension or prosecution of offenders.

66. The Commissioner has identified section 31(3) to be a “prejudice-based exemption” and that for this section to be engaged, “*three criteria must be met*:

- *Firstly, the actual harm which the public authority alleges would, or would be likely, to occur if the withheld information was disclosed – or in this case confirmation as to whether or not the requested information is held – has to relate to the applicable interests within the relevant exemption;*

- *Secondly, the public authority must be able to demonstrate that some causal relationship exists between the potential disclosure of the information being withheld – or the confirmation as to whether or not the requested information is held – and the prejudice which the exemption is designed to protect. Furthermore, the resultant prejudice which is alleged must be real, actual or of substance; and*

- *Thirdly, it is necessary to establish whether the level of likelihood of prejudice being relied upon by the public authority is met – ie, confirming or denying whether information is held disclosure ‘would be likely’ to result in prejudice or confirming or denying whether information is held ‘would’ result in prejudice. In relation to the lower threshold the Commissioner considers that the chance of prejudice occurring must be more than a hypothetical possibility; rather there must be a real and significant risk. With regard to the higher threshold, in the Commissioner’s view this places a stronger evidential burden on the public authority to discharge.*”[31]

[31] ICO, Decision Notice, Ref. FS50688200, 21 Nov. 2017, para. 21, available at https://ico.org.uk/media/action-weve-taken/decision-notices/2017/2172802/fs50688200.pdf.

i. Prejudice to Law Enforcement Matters

67. Again, as discussed above, in relation to the section 23(5), 24(2) and 30(3) FOIA exemptions, the request relates in part to legislation, policy guidance and information governing the use of IMSI Catchers by police forces. These records, which relate to the legal basis for a public authority’s powers and activities and the rules governing those powers and activities, cannot be subject to NCND under any exemption.

68. As with its arguments around the section 24(2) FOIA exemption, the MPS also base arguments around the 31(3) exemption on skeletal assertions that matters related to law enforcement would be prejudiced by (1) at a general level, confirming or denying the use of “*specialist techniques*” and (2) at a specific level, indicating that a technique is used in one area but not in another area. For the reasons discussed above – including the fact that the government has explicitly regulated other operational capabilities of the police forces or disclosed information relating to such capabilities via FOIA – these arguments fail to demonstrate any causal link between confirming or denying the existence of the requested information and the prejudice to law enforcement matters claimed. Furthermore, these arguments fail to demonstrate how the prejudice claimed is real, actual or of substance, let alone the likelihood that the claimed prejudice will be met.

ii. Public Interest Test

69. The original decision identified as the factors against confirming or denying the existence of the requested information that “*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*” and that this “*would impact on police resources, more crime would then be committed and individuals placed at risk*”. Again, the Commissioner should not accept such bare assertions. The MPS have not indicated why confirming or denying the mere existence of “*such techniques*” in general or IMSI Catchers specifically could render law enforcement less effective. This position runs contrary to the government’s explicit regulation of other operational capabilities of the police forces or FOIA disclosures relating to such capabilities. The MPS has further failed to clarify what it means by reference to the “partnership approach” and how such an approach would be undermined by confirming or denying the existence of the requested information. Finally, the MPS has presented no evidence of risk to support its position.

70. The original decision identified as the factors in favour of confirming or denying the existence of the requested information that “*[b]etter awareness may reduce crime or lead to more information from the public, and the public would be able to take steps to protect themselves*” and that “*[s]ome information is already in the public domain*.” As discussed above, the MPS has failed to consider that there is a public interest in citizens being informed about methods of surveillance that could have a profound impact on their fundamental rights, including the rights to privacy, freedom of expression and freedom of

assembly and association.

71. Finally, as discussed above, it is also worth considering the European Court of Human Right’s recent jurisprudence on access to information under Article 10, which emphasises the public interest in disclosing matters of public concern, especially where they affect the rights of citizens.

72. Thus, as set out previously to the MPS and as explained above, the public interest balancing exercise falls squarely in favour of disclosure.

    a. No meaningful reasons have been provided as to why there is a public interest in neither confirming nor denying the information sought in this request;

    b. There is currently no evidence at all to suggest that the public interest will be harmed to any material extent by confirming or denying the existence of the information sought;

    c. The public interest in disclosure is real, it is important that the public are reassured that the measures used to safeguard national security are necessary and proportionate as well as effective. Access to the information would allow for a fact-based public debate on surveillance measures. This has been hindered by the decision of the MPS to NCND the information in question.

    d. The applicant plays an important watchdog role and has requested the information as part of this function. Given the public interest nature of the issue on which Privacy International seeks to obtain information, its activities as a public watchdog warrant a high level of protection, and its role as a watchdog should be taken into account when evaluating the public interest in this matter.

    e. The fact that IMSI catchers have been purchased by UK police forces is already in the public domain. The MPS have specifically been named in this regard.

F. Conclusion

73. For the reasons set out above, the ICO is respectfully invited to allow this appeal and to issue a decision notice directing the MPS to comply with its obligations under section 1(1) FOIA and inform Privacy International whether it holds information of the description specified in the request and communicate that information.

12 February 2018

Ailidh Callander
Scarlet Kim

Privacy International

Reference: FS50728051

Freedom of Information Act 2000 (FOIA)

Decision notice

Date:	**10 July 2018**
Public Authority:	**Commissioner of the Metropolitan Police Service**
Address:	**New Scotland Yard** **Broadway** **London** **SW1H 0BG**
Complainant:	**Rosie Brighouse obo Privacy International**
Address:	**rosieb@libertyhumanrights.org.uk**

Decision (including any steps ordered)

1. The complainant has requested information about the purchase and use of Covert Communications Data Capture (“CCDC”) from the Metropolitan Police Service (the “MPS”). The MPS would neither confirm nor deny (“NCND”) whether it holds the requested information, citing the exemptions at sections 23(5) (information supplied by, or relating to, bodies dealing with security matters), 24(2) (national security) and 31(3) (law enforcement) of the FOIA for the request in its entirety.

2. In respect of parts (1) and (3) of the request the Commissioner’s decision is that sections 23(5) and 24(2) were cited correctly so the MPS was not obliged to confirm or deny whether the requested information is held; this is also her position in respect of some of part (4) of the request.

3. For part (2) of the request and the ‘legislation’ and ‘codes of practice’ elements of part (4) of the request, the Commissioner’s decision is that the exemptions were applied incorrectly. The MPS is required to confirm or deny whether this information is held and either disclose it or issue a fresh response compliant with section 17 of the FOIA.

4. The MPS must take these steps within 35 calendar days of the date of this decision notice. Failure to comply may result in the Commissioner

making written certification of this fact to the High Court pursuant to section 54 of the Act and may be dealt with as a contempt of court.

Background

5. The Commissioner is considering 9 related cases from this complainant in respect of similar information requests being made to different public authorities. They are dealt with under reference numbers FS50728051 to FS50728059 inclusive.

6. As the different authorities dealt with their requests within different time frames the Commissioner agreed to deal with the substantive complaint about all the requests outside of her usual 3 month deadline for accepting complaints. This agreement was made in advance, in May 2017, when some refusal notices / internal reviews were outstanding for some of the public authorities concerned.

Request and response

7. On 1 November 2016 the complainant wrote to the MPS and requested information in the following terms:

> *“I am writing on behalf of* [name removed] *to seek records … relating to the purchase and use of mobile phone surveillance equipment by the Metropolitan Police.*
>
> *I refer, in particular, to the recent article written by the journalist collective The Bristol Cable “Revealed: Bristol’s police and mass mobile phone surveillance”. The article makes reference to the purchase of equipment from the company CellXion by the Metropolitan Police under the item “CCDC” for the cost of £1,037,223.00. The article links to the original document disclosing the purchase, which can be found on the Metropolitan Police website* [no link found]*. The article also explains that the acronym “CCDC equipment” appears to refer to “covert communications data capture” as spelled out in the minutes of an Alliance Governance Group meeting in May 2016 between Warwickshire and West Mercia Police.*
>
> *I also refer to the 10 October 2016 article published by the Guardian “Controversial snooping technology ‘used by at least seven police forces’”. That article reported that “surveillance technology that indiscriminately harvests information from mobile phones”, also “known as an IMSI catcher” is being “used by at least seven police forces across the country…according to police*

Reference: FS50728051

documents.” One of the forces understood to be using this technology is the Metropolitan Police.

[Name removed] *requests the following records:*

1. Purchase orders, invoices, contracts, loan agreements, solicitation letters, correspondence with companies and other similar records regarding the Metropolitan Police’s acquisition of CCDC equipment. Please include records of all purchase orders, invoices, contracts, agreements, and communications with CellXion.

2. Marketing or promotional materials received by the Metropolitan Police relating to CCDC equipment.

3. All requests by CellXion or any other corporation, or any government agency, to the Metropolitan Police to keep confidential any aspect of Metropolitan Police’s possession and use of CCDC equipment, including any non-disclosure agreements between Metropolitan Police and CellXion or any other corporation, or government agency, regarding the Metropolitan Police’s possession and use of CCDC equipment.

4. Legislation, codes of practice, policy statements, guides, manuals, memoranda, presentations, training materials or other records governing the possession and use of CCDC equipment by the Metropolitan 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.

[Name removed] *seeks records regardless of how CCDC equipment is identified. In this respect,* [name removed] *notes that CCDC equipment can be referred to using a range of other terms, including “IMSI Catchers”, “IMSI Grabbers”, “Cell site simulators” and “Stingrays”.*

Please include copies of material that you hold either in the form of paper or electronic records, including emails. If possible, please provide all requested records in electronic format.

Upon locating the requested records, please contact us and advise us of any costs of providing copies, so that we may decide whether it is necessary to narrow our request”.

8. On 29 November 2016, the MPS responded. It would NCND holding the requested information, citing the exemptions at sections 23(5), 24(2), 30(3) and 31(3) of the FOIA.

9. On 24 January 2017 the complainant requested an internal review. This was provided by the MPS on 13 June 2017. It maintained its position.

10. During the Commissioner’s investigation, the MPS removed reliance on section 30(3).

Scope of the case

11. The complainant initially contacted the Commissioner on 17 May 2017. She advised of her intention to file a number of related complaints against different public authorities and requested a pause in the time limit for bringing such complaints.

12. Having received the necessary responses from all of the various public authorities, with the exception of two internal reviews, the complainant wrote to the Commissioner again on 12 February 2018 with her grounds of complaint in this case. She asked the Commissioner to consider the application of the exemptions cited.

13. The request in this case is similar to the requests for information which the Commissioner has considered under references FS50728052 to FS50728056 and FS50728059. The decision notice in this case is being issued at the same time as those cases, with this case taking the ‘lead’.

Reasons for decision

14. The MPS has provided most of its reasoning and evidence ‘in confidence’ to the Commissioner and she is unable to cite or comment directly about it in this decision notice. It has been taken into account in her deliberations.

15. She also notes that although the request itself is based on information that seems to have been in the public domain, that source information is no longer available. Whilst such information may possibly have been available at the time of the request, it is not there now and cannot be verified. Therefore, were it ever available, it has since been removed.

16. The Commissioner has been advised that no formal statements have been made by the MPS on this subject matter.

17. In its refusal notice the MPS explained its NCND position as follows:

Reference: FS50728051

“By confirming or denying that the MPS hold any information regarding these techniques would in itself disclose exempt information. Stating information is held would confirm usage and the opposite if there is no such information.

Although the techniques are in the public domain, it is how and when they might be used, that are the sensitive issues for the police service. These techniques could be deployed for more high profile sensitive operations, albeit not necessarily in the MPS force area, therefore the NCND is required to protect other forces that may use them.

Any disclosure under FOIA 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) the MPS may or may not deploy in specific circumstances would prejudice law enforcement. If the requested information was held by the MPS, confirmation of this fact would reveal that the MPS have 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 MPS'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 MPS may be aware of their presence and taking counter terrorist measures.

Conversely, if information was not held by the MPS, and a denial was issued, this would reveal to those same individuals that their activities are unlikely to have been detected by the MPS. It may also suggest (whether correctly or not) the limitations of the MPS'S 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 the MPS would substantially prejudice the ability of the MPS 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.

5

Reference: FS50728051



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”.

18. Whilst the Commissioner understands the rationale behind these arguments, and the others provided to her ‘in confidence’, she notes that the exemptions cited have all been done so in respect of all parts of the request in its entirety. The approach has therefore been to apply them in a ‘blanket fashion’ without, it would appear, any consideration of a more detailed breakdown of the different elements of the request.

19. Depending on the wording of a request, such an approach may be appropriate under some circumstances. However, the Commissioner considers that the request here is wide ranging and the exemptions appear to have been cited without full consideration as to where each applies.

20. Part (2) of the request seeks details regarding any marketing or promotional materials relating to CCDC equipment which the MPS may have received. The Commissioner does not accept that any of the exemptions cited could properly apply to such material. It is likely that the MPS receives many approaches from suppliers trying to promote their products if they feel they may be of benefit to the police service. Confirmation or denial as to the receipt of such material does not reveal whether or not the MPS actually purchased any equipment.

21. Some of part (4) of the request refers to legislation and codes of practice which would cover the use of CCDC. During her investigation the Commissioner invited the MPS to revise its NCND position regarding these elements of the request, however, it declined to do so saying it wished to maintain its position. It is clear to the Commissioner that

legislation either does or doesn’t exist and, if it does, it clearly cannot be exempt under FOIA as it would be statute which should be publically available; this would be the same for codes of practice. Furthermore, in her decision notice FS50660527[1] the Commissioner has already referred to a response on Hansard[2] which indicates the legislation that would support the use of IMSI equipment as follows:

> *“Investigative activity involving interference with property or wireless telegraphy, such as International Mobile Subscriber Identity (IMSI) grabbers, is regulated by the Police Act 1997 and the Intelligence Services Act 1994 which sets out the high level of authorisation required before the police or Security and intelligence agencies can undertake such activity. Use of these powers is overseen by the Intelligence Services Commissioner and the Office of Surveillance Commissioners. In any case involving the interception of the content of a communication, a warrant authorised by the Secretary of State under the Regulation of Investigatory Powers Act 2000 is required”.*

22. IMSI equipment would fall under the categorisation of CCDC and there is therefore clearly information in the public domain which evidences that its use is permitted by relevant legislation.

23. For these two elements of the request the Commissioner finds that none of the exemptions cited are appropriate and the MPS must confirm or deny whether any information is held. If information is held, it should either be disclosed or the MPS should issue a fresh response compliant with section 17 of the FOIA.

24. The Commissioner will next consider the application of sections 23 and 24 to the remaining parts of the request.

Section 23 – information supplied by, or relating to, bodies dealing with security matters
Section 24 – national security

25. The MPS explained that it was relying on sections 23(5) and 24(2) of FOIA as a basis to refuse to confirm or deny whether it holds any information falling within the scope of the request.

[1] https://ico.org.uk/media/action-weve-taken/decision-notices/2017/2014349/fs50660527.pdf
[2] http://www.parliament.uk/business/publications/written-questions-answers-statements/written-question/Lords/2014-11-03/HL2602

Reference: FS50728051

26. Sections 23(5) and 24(2) exclude the duty of a public authority to confirm or deny whether it holds information which, if held, would be exempt under section 23(1) or 24(1) respectively.

27. Information relating to security bodies specified in section 23(3) is exempt information by virtue of section 23(1). Information which does not fall under section 23(1) is exempt from disclosure under section 24(1), if it is required for the purpose of safeguarding national security.

28. By virtue of section 23(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 section 23(3). It is an absolute exemption requiring no public interest considerations. Put simply, if this exemption is engaged then this is sufficient then the MPS does not have to confirm or deny whether it holds the requested information.

29. By virtue of section 24(2) the duty to confirm or deny does not arise if, or to the extent that, exemption from section 1(1)(a) is required for the purpose of safeguarding national security.

30. The Commissioner does not consider the exemptions at sections 23(5) and 24(2) to be mutually exclusive and she accepts that they can be relied on independently or jointly in order to conceal whether or not one or more of the security bodies has been involved in an issue which might impact on national security. However, each exemption must be applied independently on its own merits. In addition, the section 24 exemption is qualified and is therefore subject to the public interest test.

31. The test as to whether a disclosure would relate to a security body is decided on the normal standard of proof, that is, the balance of probabilities. In other words, if it is more likely than not that the disclosure would relate to a security body then the exemption would be engaged.

32. From the above it can be seen that section 23(5) has a very wide application. If the information requested is within what could be described as the ambit of security bodies’ operations, section 23(5) is likely to apply. This is consistent with the scheme of FOIA because the security bodies themselves are not subject to its provisions. Factors indicating whether a request is of this nature will include the functions of the public authority receiving the request, the subject area to which the request relates and the actual wording of the request.

33. In disputing the citing of this exemption the complainant has argued as follows. Firstly, she notes that the request includes legislation, policy guidance and other information governing the use of CCDC by the MPS

which she does not consider to be information falling within the area of work of the bodies specified in section 23(3) FOIA. She says:

> *“As a threshold matter, these records, which relate to the legal basis for a public authority’s powers and activities and the rules governing those powers and activities, cannot be subject to NCND under any exemption. The principle of legality and the presumption of disclosure in FOIA must be properly considered and weighed against the position taken by the MPS”.*

34. The Commissioner has already accepted above that the MPS cannot rely on an exemption in respect of legislation or codes of practice.

35. Secondly, the complainant argues that the request seeks the use of CCDC by ‘police forces’ only and she therefore does not accept, just because it may be used by the bodies specified in section 23(3), that this gives sufficient grounds for section 23(5) to be engaged. She adds:

> *“There are many techniques – ranging from the simple to the sophisticated – that both the police forces and the section 23(3) bodies may deploy. For that reason, the reliance on the argument that both the Police Act 1997 and the Intelligence Services Act 1994 cover a technique is meaningless.*
>
> *For example, both pieces of legislation authorise the power to interfere with property, which may include entry onto a property. A logical extension of this argument would engage section 23(5) for any technique covered by both statutes.*
>
> *Similarly, reliance on the argument that there is a close relationship between the police forces and security bodies is dangerously vague. Indeed, a logical extension of that argument would engage section 23(5) for any technique deployed by the police forces. The MPS have made no attempt to indicate the circumstances in which police forces use IMSI Catchers, which could include ordinary law enforcement activities such as tracking a suspect for a variety of offences, and how those circumstances in any way relate to the section 23 bodies”.*

36. The Commissioner has already determined above that the MPS cannot rely on any exemption currently cited in respect of legislation and codes of practice. However, regarding the holding of policy and guidance, the Commissioner notes that any confirmation or denial as to the existence of this by the MPS would clearly indicate whether or not CCDC equipment was being used. This is essentially the case because it would not exist unless there was a business requirement for it to have been created.

Reference: FS50728051

37. The Commissioner agrees with the complainant in that there will be many policing techniques that are available for both the police service and the security bodies to use, however, she does not agree that relying on the Police Act 1997 and the Intelligence Services Act 1994 to cover a technique is meaningless. As mentioned in paragraph 21 above, the Commissioner has previously issued a decision notice about the purchase or rental of IMSI catchers in respect of a different public authority, this being the type of equipment which would fall under the description of CCDC. In that case, she noted that any use of IMSI technology would be regulated by the Police Act 1997 and the Intelligence Services Act 1994. Also in that case, she accepted that it is likely that, if the information described in that request did exist, this would be a field of work which is likely to have been done in conjunction with, and with the knowledge of, other parties within the policing field, and also that this type of work is likely to include security bodies.

38. The equipment being considered here is **covert** surveillance equipment and, put simply, the Commissioner is trying to establish the likelihood as to whether or not the use of such equipment could ‘relate to’ any of the security bodies; this is all she is required to do. As it is covert equipment, the Commissioner considers it is considerably more likely to ‘relate’ to security bodies and, if it is used, it could realistically be deployed in joint operations between the police service and security bodies. Furthermore, the conditions for any actual deployment of such equipment may therefore relate to practices developed by security bodies, eg terrorism operations.

39. Although not accepted by the complainant, in the Commissioner’s view the close relationship between the police service and the security bodies is not “*dangerously vague”* and there will clearly be an overlap in some of the work that is undertaken by these bodies. Although the complainant may believe that this means the police will always be able to cite section 23 and forego disclosure the Commissioner has no evidence to support this rationale. Where normal policing activity is under consideration a force will generally cite either section 30 (criminal investigations) or section 31 (law enforcement) to ‘protect’ any information it does not wish to disclose; there is no evidence to support the complainant’s belief that it will default to citing section 23. The request here concerns a covert surveillance technique which the Commissioner considers to be a subject matter which could readily touch on the type of work she would expect to relate to the security bodies rather than the police service in isolation.

40. In the Tribunal case *The Commissioner of Police of the Metropolis vs Information Commissioner* (EA/2010/0008) the argument was advanced that it was *highly likely* that any information held by the public authority that fell within the scope of the request would have been supplied to it by a section 23(3) body and, therefore, section 23(5) was engaged. The

counterargument was made that only certainty as to the source of the information would be sufficient. The Tribunal rejected this counterargument and stated:

> “[The evidence provided] *clearly establishes the **probability** that the requested information, if held, came through a section 23 body.”* (paragraph 20)

41. The approach of the Commissioner on this point is that she accepts the Tribunal view that the balance of probabilities is the correct test to apply. This means that for section 23(5) to be engaged, the evidence must suggest to a sufficient degree of likelihood (rather than certainty) that any information falling within the scope of the request would relate to, or have been supplied by, a body specified in section 23(3).

42. The test as to whether a disclosure would relate to a security body is decided on the normal standard of proof, that is, the balance of probabilities. In other words, if it is more likely than not that the disclosure would relate to a security body then the exemption would be engaged.

43. The Commissioner finds that on the balance of probabilities, information about this subject matter, ie the use of covert equipment, if held, could be related to one or more bodies identified in section 23(3). She therefore concludes that the exemption is engaged. As this is an absolute exemption no consideration of any public interest is necessary.

44. With regard to section 24(2), the Commissioner again considers that this exemption should be interpreted so that it is only necessary for a public authority to show either a confirmation or a denial of whether requested information is held would be likely to harm national security.

45. In relation to the application of section 24(2) the Commissioner notes that the First Tier Tribunal (Information Rights) has indicated that only a consistent use of a NCND response on matters of national security can secure its proper purpose. Therefore, in considering whether the exemption is engaged, and the balance of the public interest, regard has to be given to the need to adopt a consistent NCND position and not simply to the consequences of confirming whether the specific requested information in this case is held or not.

46. In the context of section 24, Commissioner accepts that withholding information in order to ensure the protection of national security can extend to ensuring that matters which are of interest to the security bodies are not revealed. Moreover, it is not simply the consequences of revealing whether such information is held in respect of a particular request that is relevant to the assessment as to whether the application of the exemption is required for the purposes of safeguarding national

security, but the need to maintain a consistent approach to the application of section 24(2).

47. The complainant has argued that:

> *“… police forces could use IMSI Catchers in a wide range of operations, including for ordinary law enforcement activities, that bear no relation to the bodies specified in section 23(3). The MPS have made no attempt to indicate the circumstances in which police forces use IMSI Catchers and how those circumstances relate in any way to the section 23 bodies. It has therefore failed to demonstrate the engagement of either the section 23(5) or 24(2) exemption”.*

48. As explained above, and in the wording of the request itself, IMSI equipment would fall under the category of ‘covert’ equipment. The Commissioner has also already determined above that section 23 is engaged so the potential involvement of a security body has already been satisfied. Furthermore, the MPS has not confirmed whether or not this equipment is being used so the circumstances for any such use is not at this stage relevant. The case being considered here is whether or not the MPS is entitled to maintain an NCND stance rather than to disclose any information which may, or may not, be held

49. The complainant has further argued that:

> *“The MPS also base arguments around national security on skeletal assertions that national security would be impacted by (1) at a general level, confirming or denying the use of “specialist techniques” and (2) at a specific level, indicating that a technique is used one area but not in another area. Both arguments are baseless. As to the first argument, the MPS do not define a “specialist technique” and why IMSI Catchers constitute a specialist technique. Furthermore, it does not follow that merely confirming or denying that a police force uses IMSI Catchers reveals operationally sensitive information that would negatively impact national security. In fact, the government has willingly admitted and subjected to either public regulation or FOIA requests the use of a variety of what might also be considered “specialist techniques” – from hacking to the use of equipment to physically extract mobile phone data. There is therefore no reason that information governing the use of IMSI Catchers by police forces should be afforded special protection. As to the second argument, it does not follow that determining which police forces use this equipment could permit individuals to map or be aware of how operationally sensitive information is obtained, thereby negatively impacting national security. Different police forces will obtain information in many different ways”.*

Reference: FS50728051

50. The government may have previously released details regarding the legislation of some specific ‘specialist techniques’ and this position may be less clear in respect of CCDC equipment. Such clarification may indeed be helpful but it is the role of government to legislate not the MPS. If the MPS does have its own guidance then revealing this would indicate that it does use CCDC equipment, which would go against the NCND stance it has adopted here. Also, if the use of such equipment were not fully legislated for, then this will be determined by the courts at some future date if evidence is gathered using this methodology.

51. Furthermore, the Commissioner does not accept that the provision of a confirmation or denial regarding the use of CCDC equipment would have no impact on the police service. For example, if it were the case that only a small number of forces had access to this type of equipment then it follows that those who do not are obviously more vulnerable to the types of crimes that could be subject to this type of surveillance if it were in use; this may in turn present a potential ‘green light’ to some criminals or terrorists to undertake certain types of crimes in particular force areas. Were it the case that no forces had access to this equipment then confirming this would again show vulnerability and criminals would be more knowledgeable as to what means of communication were the least likely to be intercepted. Were it the case that all forces had access to the same CCDC equipment then any vulnerability argument may be weakened, but the Commissioner does not know if this is the case and it is not a point which is under consideration in this investigation.

52. On this occasion the Commissioner is satisfied that complying with the requirements of section 1(1)(a) would be likely to reveal whether or not the security bodies were in any way involved in the subject matter which is the focus of this requests. The need for a public authority to adopt a position on a consistent basis is of vital importance in considering the application of an NCND exemption.

53. The Commissioner is satisfied that the public authority was entitled to rely on sections 23(5) and 24(2) in the circumstances of this case. She accepts that revealing whether or not information is held about CCDC would be likely to reveal whether information is held relating to the role of the security bodies. It would also undermine national security and for that reason section 24(2) also applies because neither confirming nor denying if additional information is held is required for the purpose of safeguarding national security.

54. As noted above section 24 is a qualified exemption. The complainant has argued that the public interest falls in favour of disclosure based on the following :

“(a) No meaningful reasons have been provided as to why there is a public interest in neither confirming nor denying the information sought in this request;
(b) There is currently no evidence at all to suggest that the public interest will be harmed to any material extent by disclosure of the information sought;
(c) The public interest in disclosure is real, it is important that the public are reassured that the measures used to safeguard national security are necessary and proportionate as well as effective. Access to the information would allow for a fact-based public debate on surveillance measures. This has been hindered by the decision of the MPS to NCND the information in question.
(d) The applicant plays an important watchdog role and has requested the information as part of this function. Given the public interest nature of the issue on which [name removed] *seeks to obtain information, its activities as a public watchdog warrant a high level of protection, and its role as a watchdog should be taken into account when evaluating the public interest in this matter.*
(e) The fact that IMSI Catchers have been purchased by UK police forces is already in the public domain. The MPS have specifically been named in this regard”.

55. The Commissioner would initially note that this decision concerns the upholding, or otherwise, of the duty to confirm or deny whether any information is held and not the actual disclosure of any information which may be held. Therefore, the argument presented at part (c) is not relevant – albeit it is noted that on one hand the complainant argues that the information should be disclosed as it is in the public interest for the public to be reassured regarding “*measures used to safeguard national security”* whereas, on the other hand, she argues that the exemption regarding national security is not engaged.

56. In respect of parts (a) and (b) of the complainant’s rationale, the Commissioner has addressed these points in her arguments above. She would also again like to stress that the confidential submissions provided by the MPS cannot be cited because of their nature, but they have still been taken into account.

57. The FOIA is applicant blind so the role of the requester is not relevant, thereby removing any reliance on the argument at (d).

58. In respect of the argument at (e), the Commissioner notes that the complainant has drawn attention to information in the public domain regarding the apparent purchase of IMSI equipment. However, as stated above, the Commissioner is advised that no such formal statements have been made by the MPS on this subject matter.

Reference: FS50728051

59. The Commissioner further notes that that the current national security level of risk, which is set by the government, sits at ‘severe’[3].

60. The Commissioner considers it to be clearly the case that the public interest in confirming or denying whether information is held does not match the weight of the public interest in safeguarding national security by maintaining a consistent NCND stance. This means that her conclusion is that the public interest in the maintenance of the exemption provided by section 24(2) outweighs the public interest in complying with the duty imposed by section 1(1)(a).

61. In view of this finding the Commissioner has not therefore considered the other exemption cited.

Other matters

62. Although it does not form part of this notice the Commissioner wishes to highlight the following matters of concern.

Internal review

63. The Commissioner cannot consider the amount of time it took a public authority to complete an internal review in a decision notice because such matters are not a formal requirement of the FOIA. Rather they are matters of good practice which are addressed in the code of practice issued under section 45 of the FOIA.

64. Part VI of the section 45 Code of Practice states that it is desirable practice that a public authority should have a procedure in place for dealing with complaints about its handling of requests for information, and that the procedure should encourage a prompt determination of the complaint. The Commissioner considers that these internal reviews should be completed as promptly as possible. While no explicit timescale is laid down by the FOIA, the Commissioner considers that a reasonable time for completing an internal review is 20 working days from the date of the request for review. In exceptional circumstances it may take longer but in no case should the time taken exceed 40 working days; it is expected that this will only be required in complex and voluminous cases.

65. Although she notes that there are sensitivities around this case because of the subject matter and the exemptions relied on, she is nevertheless

[3] https://www.gov.uk/terrorism-national-emergency

concerned that it took almost five months for an internal review to be completed.

66. The Commissioner would like to remind MPS that she routinely monitors the performance of public authorities and their compliance with the legislation. Records of procedural breaches are retained to assist the Commissioner with this process and further remedial work may be required in the future should any patterns of non-compliance emerge.

Reference: FS50728051

Right of appeal

67. Either party has the right to appeal against this decision notice to the First-tier Tribunal (Information Rights). Information about the appeals process may be obtained from:

    First-tier Tribunal (Information Rights)
    GRC & GRP Tribunals,
    PO Box 9300,
    LEICESTER,
    LE1 8DJ

    Tel: 0300 1234504
    Fax: 0870 739 5836
    Email: GRC@hmcts.gsi.gov.uk
    Website: www.justice.gov.uk/tribunals/general-regulatory-chamber

68. If you wish to appeal against a decision notice, you can obtain information on how to appeal along with the relevant forms from the Information Tribunal website.

69. Any Notice of Appeal should be served on the Tribunal within 28 (calendar) days of the date on which this decision notice is sent.

Signed .....

Carolyn Howes
Senior Case Officer
Information Commissioner’s Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Privacy International
62 Britton Street, London EC1M 5UY
United Kingdom

Phone +44 (0)20 3422 4321
www.privacyinternational.org
Twitter @privacyint

UK Registered Charity No. 1147471