BEFORE THE INFORMATION COMMISSIONER

BETWEEN

PRIVACY INTERNATIONAL

Applicant

- and -

HOME OFFICE

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 Home Office, National Police Chiefs Council, National Crime Agency, Metropolitan Police, 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". For the purposes of these grounds, the equipment is hereafter referred to as "IMSI Catchers".

3. Privacy International's initial request to the Home Office is annexed to these grounds as Exhibit A.

4. On 13 March 2017, the Home Office responded to the initial request. In the response, the Home Office indicated that "*any police investigative activity involving interference with property or wireless telegraphy is regulated by the Police Act 1997, and subject to the Covert Surveillance and Property Interference Code of Practice*." The Home Office further indicated that for the remainder of the request it could neither confirm nor deny ("NCND") whether it held the information requested pursuant to sections 23(5), 24(2) and 31(3) Freedom of Information Act ("FOIA") 2000.. This response is annexed to these grounds as Exhibit B.

5. On 22 May 2017 Privacy International made a request for internal review of the decision. This request is annexed to these grounds as Exhibit C.

6. On 17 August 2017 the Home Office upheld its initial decision. This decision is annexed to these grounds as Exhibit D.

7. The Home Office's 17 August 2017 decision was wrong and/or unlawful, in that:

    a. It erred in concluding that section 23(5) FOIA was engaged by the request;

    b. It erred in concluding that its NCND position was "required for the purpose of safeguarding national security" pursuant to section 24(2) FOIA;

    c. It erred in concluding that confirming or denying the existence of the requested information would or would be likely to prejudice law enforcement pursuant to section 31(3) FOIA;

    d. It erred in concluding that, 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) and 31(3) FOIA.

II. The Facts

A. Privacy International

8. 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).

9. 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

10. 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.

11. 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.

12. 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.

13. 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.

14. 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.

15. 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

[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.

inextricable linkages between anonymity, privacy, and freedom of expression.[3]

16. 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]

17. 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]

18. On 10 October 2016, an article appeared in the Bristol Cable entitled: "Revealed: Bristol's police and mass mobile phone surveillance."[7] The article made reference to the minutes of an Alliance Governance Group meeting in May 2016 between Warwickshire and West Mercia Police in which the topic of CCDC equipment was discussed.

19. On the same day, the Guardian published the article "Controversial snooping technology

---

[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 Privacy International and Article 19, *Breyer v Germany*, European Court of Human Rights, App. No. 50001/12, 5 September 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 November 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 October 2016, https://thebristolcable.org/2016/10/imsi/.

'used by at least seven police forces'".[8] 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*."

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

III. Procedural History

A. Request for Information

21. On 1 November 2016, Privacy International requested the following information from the Home Office:

> "*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 NPCC, 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.*"

B. The Refusal

22. On 13 March 2017, a member of the Home Office Information Rights Team responded by stating:

> "*With regards to legislation and codes of practice, any police investigative activity involving interference with property or wireless telegraphy is regulated by the Police Act 1997, and subject to the Covert Surveillance and Property Interference Code of Practice. These are available at www.gov.uk.*"

The response further stated that it could NCND "*whether the Home Office holds any information within scope of the remainder of [the] request*" pursuant to sections 23(5), 24(2), 30(3), and 31(3) FOIA.

23. In an Annex to the response, the Home Office applied the public interest test with respect to sections 24(2) and 31(3) FOIA. With respect to considerations in favour of confirming or denying, the Home Office indicated:

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

"*In the interests of transparency and openness, it is accepted that there may be a general public interest in knowing what, if any, information the Home Office holds governing the use of Covert Communications Data Capture (CCDC) equipment in the United Kingdom.*

Confirming would serve to inform and educate the public about an issue related to national security and law enforcement. There is an interest in the public understanding the nature and extent of the department's interest in, and awareness of, communication technologies and their potential uses and effects."

24. With respect to considerations in favour of neither confirming nor denying, the Home Office indicated:

"*To provide a confirmation or denial would allow interested parties to determine the extent and scope of operational work by law enforcement. This would be prejudicial and detrimental to the overall effectiveness of work done by law enforcement agencies in tackling serious crime and protecting national security.*

Any response the Home Office might provide on this issue – be it a confirmation or denial – would be of significant value to criminal and terrorist groups who would be able to develop a greater understanding of law enforcement capabilities. A confirmation or denial would enable criminals and terrorists to gain an understanding of the nature, extent and investigative capabilities of law enforcement. This would allow such groups to build a picture of security measures or practices that might or might not be in place for protecting the UK. In turn, this would enable such groups to take steps to circumvent them.

Information that undermines the operational integrity of any such activities would adversely affect public safety and have a negative impact on both national security and law enforcement.

National security and law enforcement are of vital importance to protecting the UK. It is clearly not in the public interest to confirm or deny whether material is held that would benefit those who are intending to carry out criminal or terrorist activities to the detriment of the UK."

C. Request for Internal Review

25. On 22 May 2017, Privacy International challenged the response from the Home Office.

26. First, Privacy International indicated that "*[i]nsofar as the reference to the Police Act 1997 and the Covert Surveillance and Property Interference Code of Practice were intended to respond to the request for information relating to the regulatory regime in respect of ISMI catchers, the 13 March 2017 letter was woefully inadequate*." Privacy International further requested that the Home Office provide:

- Reference to the specific sections and/or paragraphs of the Police Act 1997 and the Covert Surveillance and Property Interference Code of Practice that the Home Office suggests regulates the use of ISMI catchers;

- An explanation, by reference to statute and/or publicly accessible policy guidance, as to:

    - What restrictions exist on when, where, how, and against whom ISMI catchers may be used;

    - What limitations exist on retention and use of collected data;

    - What guidance exists on when a warrant or other legal process must be obtained when the use of ISMI catchers may be sought;

    - What rules exist governing when the existence and use of ISMI catchers may be revealed to the public, criminal defendants, or judges.

27. Second, Privacy International noted that the Home Office response provides no explanation at all for its assertion of the NCND position pursuant to sections 23(5), 24(2) and 31(3) FOIA.

28. Third, Privacy International submitted that the reasons provided by the Home Office in respect of the public interest balancing test fail to justify the application of NCND for four reasons:

    a. First, the Home Office response was predicated on a series of *non-sequiturs*:

        i. It simply does not follow that merely confirming or denying that the Home Office holds information governing the use of IMSI catchers would reveal operationally sensitive information about the scope of police activities and operations. This reasoning is not understood. It appears that the Home Office has confused consideration of NCND with consideration of the provision of information itself;

        ii. It is not understood why revealing that the Home Office has information governing the use of sophisticated capabilities to collect data would limit operational capabilities. The reasoning set out in this respect is nonsensical.

    b. Second, the Home Office response failed to have regard to obviously material considerations, including, but not limited to:

        i. The fact that policy guidance and other records governing the use of IMSI Catchers cannot conceivably fall within any exemption;

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

c. Third, when considered forensically, the exemptions relied upon do not apply:

i. 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;

ii. 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 the existence of policy guidance and other records governing the use of IMSI Catchers;

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

i. 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;

ii. 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;

iii. 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.

29. 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. The language and purpose of FOIA require exemptions to be narrowly construed:

a. 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";[9]

b. It is therefore clear that an NCND decision 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.[10] It also flies in the face of the Article 10 right to receive information, as recently confirmed by the European Court of Human Rights;[11]

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*".[12]

D. Decision in Response to Request for Internal Review

30. On 17 August 2017, the Home Office upheld its decision.

31. With respect to Privacy International's requests for clarification regarding its reference to the Police Act 1997 and the Covert Surveillance and Property Interference Code of Practice, the Home Office acknowledged that "*neither the Police Act nor the code of practice is specific to any particular form of technology*" but submitted that "*Part 3 of the act and Chapter 7 of the code would be of particular relevance to anything that may interfere with property or wireless telegraphy*."

32. The Home Office further upheld its reliance on NCND pursuant to 23(5), 24(2) and 31(3) FOIA on the following grounds:

> "*Confirming or denying if any of the information within the scope of the request is held would (whether the information is held or not) reveal information relating to the role of the security bodies (section 23). The work of the security bodies – by their very nature – relates to the security of the UK (section 24), and in order to protect the security of the UK, security bodies work closely with other law enforcement agencies (section 31).*
>
> *Confirming or denying whether the information is held would undermine the techniques and capabilities used by such agencies (and security bodies) for the purposes of safeguarding the national security of the UK*."

---

[9] *Philip Kalman v Information Commissioner and the Department of Transport* (EA/2009/111 6 July 2010).
[10] *Galloway v Information Commissioner v The Central and North West London NHS Foundation Trust* (EA/2008/0036 20 March 2009).
[11] *Magyar Helsinki Bizottság v Hungary*, European Court of Human Rights, App. No. 18030/11, 8 November 2016.
[12] *Mohamed and another v Secretary of State for the Home Department* [2014] 1 WLR 4240, per Maurice Kay LJ, at §40.

33. Finally, the Home Office indicated its satisfaction with the "*public interest arguments in favour of confirming or denying whether the requested information is held, in the case of qualified exemptions*."

IV. The Appeal

A. The Purpose of FOIA

34. 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. There is a high degree of consensus under international law that access to information is part of the right to freedom of expression.

35. In particular, the Commissioner should have regard to the Grand Chamber decision in *Magyar Helsinki Bizottság v Hungary*. 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.[13]

36. 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*

[13] 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.

ability to provide accurate and reliable information may be adversely affected (see Társaság, cited above, § 38).

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'."

37. 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 technique and its human rights implications, including for the right to privacy.

38. 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.

A. Section 23(5) FOIA

39. 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).

40. 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 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*."[14]

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

    a. The request relates to *legislation, policy guidance and other information* governing the use of IMSI Catchers held by the Home Office and therefore is not information falling within the area of the work of bodies specified in section 23(3) FOIA. As a threshold matter, legislative provision, policy guidance and other information, 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 Home Office;

    b. The request further relates to legislation, policy guidance and other information governing the use of IMSI Catchers *by the 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 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 Home Office has 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

[14] 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.

bodies.

B. Section 24(2) FOIA

42. 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.

43. 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*."[15]

44. 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'. "*[16]

45. 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.[17]

i. Safeguarding National Security

46. 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*."[18]

---

[15] ICO, Decision Notice, Ref. FS50665716, 13 June 2017, para. 26; *see also* ICO Decision Notice, Ref. FS50660527, 8 June 2017, para 27.
[16] 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.
[17] ICO, Decision Notice, Ref. FS50665716, 13 June 2017, paras. 29-30; *see also* ICO Decision Notice, Ref. FS50660527, 8 June 2017, paras. 30-31.
[18] ICO, Decision Notice, Ref. FS50665716, 13 June 2017, para. 27; *see also* ICO Decision Notice, Ref. FS50660527, 8 June 2017, para. 29.

47. As discussed above, in relation to the section 23(5) exemption, the request relates to legislation, policy guidance and other 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. 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 Home Office has 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. The Home Office also bases its arguments around national security on skeletal assertions that "*confirming or denying whether the information is held would undermine the techniques and capabilities used by such agencies (and security bodies) for the purposes of safeguarding the national security of the UK*." It simply does not follow that merely confirming or denying that a police force uses certain "techniques and capabilities" more generally or IMSI Catchers specifically would reveal 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[19] to the use of equipment to physically extract mobile phone data.[20] There is therefore no reason that the information related to the use of IMSI Catchers by police forces should be afforded special protection.

ii. Public Interest Test

49. The original decision identified as the factor against confirming or denying the existence of the requested information that it "*would allow interested parties to determine the extent and scope of operational work by law enforcement*" and "*enable criminals and terrorists to gain an understanding of the nature, extent and investigative capabilities of law enforcement*." This would, in turn, "*allow such groups to build a picture of security measures or practices" and "take steps to circumvent them*." The result would be to undermine "*the operational integrity of any such activities*" and "*adversely affect public safety and have a negative impact on both national security and law enforcement*."

50. The ICO should not accept these bare assertions. As discussed above, it simply does not follow that merely confirming or denying that a police force uses certain "techniques and capabilities" more generally or IMSI Catchers specifically would reveal operationally sensitive information that would negatively impact national security. This position runs

[19] *See* Part 5, Investigatory Powers Act; *see also* Equipment Interference: Draft Code of Practice.
[20] *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.

contrary to the government's admission and public disclosure of information relating to the regulation of other operational capabilities of the police forces. Furthermore, it has presented no evidence of risk to support this position.

51. The original decision identified as factors in favour of confirming or denying the existence of the requested information that "*there may be a general public interest in knowing what, if any, information the Home Office holds governing the use of Covert Communications Data Capture (CCDC)*" and that doing so "*would serve to inform and educate the public about an issue related to national security and law enforcement*". The Home Office further indicated that "*[t]here is an interest in the public understanding the nature and extent of the department's interest in, and awareness of, communication technologies and their potential uses and effects*." The Home Office failed to consider that there is also 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*".[21] As discussed above, IMSI Catchers engage the public interest because their use implicates the 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.

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

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.[22] 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 Home Office 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 NCND 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 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 Home Office 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.

C. Section 31(3) FOIA

56. 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

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

detection of crime or the apprehension or prosecution of offenders.

57. 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.*"[23]

i. Prejudice to Law Enforcement Matters

58. Again, as discussed above, in relation to the section 23(5) and 24(2) FOIA exemptions, the request relates to legislation, policy guidance and other 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.

59. The Home Office bases its arguments around the 30(3) exemption on the statement that "*in order to protect the security of the UK, security bodies work closely with other law enforcement agencies (section 31)*." This argument fails to demonstrate any causal link between confirming or denying the existence of the requested information and the prejudice claimed. Further, 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.

[23] 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.

ii. Public Interest Test

60. The original decision identified the same factors against confirming or denying the existence of the requested information under section 31(3) as under section 24(2). As discussed above, the ICO should not accept these factors as asserted by the Home Office. It simply does not follow that merely confirming or denying that a police force uses certain "techniques and capabilities" more generally or IMSI Catchers specifically would reveal operationally sensitive information that would negatively impact law enforcement. This position runs contrary to the government's admission and public disclosure of information relating to the regulation of other operational capabilities of the police forces. Furthermore, the Home Office has presented no evidence of risk to support this position.

61. The original decision also identified the same factors in favour of confirming or denying the existence of the requested information under section 31(3) as under section 24(2). The Home Office therefore failed to again consider that there is also 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.

62. 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.

63. Thus, as set out previously to the Home Office 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 NCND 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 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 Home Office 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 warrants 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.

Conclusion

64. For the reasons set out above, the ICO is respectfully invited to allow this appeal and to issue a decision notice requesting the Home Office 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.

6 February 2018

Ailidh Callander
Scarlet Kim

Privacy International

EXHIBIT A

PRIVACY INTERNATIONAL

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

Freedom of Information Officer
Direct communications unit
Home Office
2 Marsham Street
London
SW1P 4DF

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 several police forces.

Alliance Governance Group Meeting Minutes

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 minutes of an Alliance Governance Group meeting in May 2016 between Warwickshire and West Mercia Police in which the topic of "Covert Communications Data Capture" (CCDC) equipment was discussed.[2]

Specifically, the minutes state: "Within the West Midlands region **both West Midlands and Staffordshire Police** have recently **purchased and operated 4G compatible CCDC equipment**." The Minutes then indicate that the following decision was made: "**Both PCCs [West Mercia and Warwickshire Police and Crime Commissioners] agreed to Replacing the existing [CCDC] equipment with a new supplier."**

Guardian Article

I also refer to the 10 October 2016 article published by the Guardian, "Controversial snooping technology 'used by at least seven police forces'".[3] 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." In addition to West Midlands, Staffordshire, West Mercia and

[1] https://thebristolcable.org/2016/10/imsi/
[2] https://thebristolcable.org/wp-content/uploads/2016/10/09-imsi-4.pdf
[3] https://www.theguardian.com/world/2016/oct/10/controversial-phone-snooping-technology-imsi-catcher-seven-police-forces?CMP=twt_gu

Warwickshire, the other forces understood to be using this technology include the Metropolitan Police Service, Avon and Somerset and South Yorkshire.

Record Requests

As the Home Office is responsible for policing across the country and the development of relevant policy and legislation in this area I believe you hold records relevant to the regulation of the use of CCDC equipment by police in the United Kingdom.

Privacy International requests the following records:

1. Legislation, codes of practice, policy statements, guides, manuals, memoranda, presentations, training materials or other records governing the use of CCDC equipment in the United Kingdom, 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

EXHIBIT B

Home Office

Information Rights Team
2 Marsham Street
London SW1P 4DF

020 7035 4848
(switchboard)

www.homeoffice.gov.uk

Mr Matthew Rice
Via email to:
matthew@privacyinternational.org

13 March 2017

Dear Mr Rice

Freedom of Information Act 2000 Request (Our Reference 41663)

Thank you for your email of 1 November 2016, in which you ask for the following information:

> *Legislation, codes of practice, policy statements, guides, manuals, memoranda, presentations, training materials or other records governing the use of CCDC equipment in the United Kingdom, 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.*

A full copy of your request can be found in **Annex A**. Your request has been handled as a request for information under the Freedom of Information Act 2000.

With regards to legislation and codes of practice, any police investigative activity involving interference with property or wireless telegraphy is regulated by the Police Act 1997, and subject to the Covert Surveillance and Property Interference Code of Practice. These are available at www.gov.uk.

We neither confirm nor deny whether the Home Office holds any information within scope of the remainder your request. Sections 23(5) (Information relating to security bodies), 24(2) (National security) and 31(3) (Law enforcement) absolve us from the requirement to say whether or not we hold information.

Section 23 relates to information supplied by, or relating to bodies dealing with security matters. This exemption applies to any information supplied directly by a security body and information originating from a security body that is provided by a third party. Section 23(5) is an absolute exemption, meaning information can be withheld automatically, without considering the public interest in favour of disclosure.

Section 24 and section 31 of the Act are qualified exemptions and require consideration of the public interest test. An explanation of the public interest test is set out in **Annex B**.

The response should not be taken as conclusive evidence that the information you have requested is or is not held by the Home Office.

If you are dissatisfied with this response you may request an independent internal review of our handling of your request by submitting a complaint within two months to the address below, quoting reference **41663**. If you ask for an internal review, it would be helpful if you could say why you are dissatisfied with the response.

Information Rights Team
Home Office
Third Floor, Peel Building
2 Marsham Street
London SW1P 4DF
Email: info.access@homeoffice.gsi.gov.uk

As part of any internal review the Department's handling of your information request will be reassessed by staff who were not involved in providing you with this response. If you remain dissatisfied after this internal review, you would have a right of complaint to the Information Commissioner as established by section 50 of the Freedom of Information Act.

Yours sincerely

S Mason
Information Rights Team
Switchboard 020 7035 4848 Email info.access@homeoffice.gsi.gov.uk

Annex A – FOI request

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 several police forces.

Alliance Governance Group Meeting Minutes

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 minutes of an Alliance Governance Group meeting in May 2016 between Warwickshire and West Mercia Police in which the topic of "Covert Communications Data Capture" (CCDC) equipment was discussed.

Specifically, the minutes state: "Within the West Midlands region **both West Midlands and Staffordshire Police** have recently **purchased and operated 4G compatible CCDC equipment**." The Minutes then indicate that the following decision was made: "**Both PCCs [West Mercia and Warwickshire Police and Crime Commissioners] agreed to Replacing the existing [CCDC] equipment with a new supplier.**"

Guardian Article

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." In addition to West Midlands, Staffordshire, West Mercia and Warwickshire, the other forces understood to be using this technology include the Metropolitan Police Service, Avon and Somerset and South Yorkshire.

Record Requests

As the Home Office is responsible for policing across the country and the development of relevant policy and legislation in this area I believe you hold records relevant to the regulation of the use of CCDC equipment by police in the United Kingdom.

Privacy International requests the following records:

> Legislation, codes of practice, policy statements, guides, manuals, memoranda, presentations, training materials or other records governing the use of CCDC equipment in the United Kingdom, 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

Annex B – Public Interest Test

Freedom of Information request from Matthew Rice (reference 41663)

Response

We neither confirm nor deny whether we hold the information that you have requested under section 23(5), 24(2) and 31(3) of the FOI Act.

Section 24(2) states:

> *(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 31(3) states:

> *(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).*

Public interest in relation to sections 24(2) and 31(3)

Section 17(3) of the Act requires us to conduct a Public Interest Test when considering the neither confirm nor deny provision of a qualified exemption. In applying this exemption, we are required to consider whether, in all the circumstances of the case, the public interest in neither confirming nor denying outweighs the public interest in disclosing whether the Home Office holds the information you have requested.

The 'public interest' is not the same as what interests the public. In carrying out a PIT, we consider the greater good or benefit to the community as a whole in saying whether information is held or not. The 'right to know' must be balanced against the need to enable effective government and to serve the best interests of the public. The FOI Act is 'applicant blind'. This means that we cannot, and do not, ask about the motives of anyone who asks for information. In providing a response to one person, we are expressing a willingness to provide the same response to anyone, including those who might represent a threat to the UK.

Considerations in favour of confirming or denying

In the interests of transparency and openness, it is accepted that there may be a general public interest in knowing what, if any, information the Home Office holds governing the use of Covert Communications Data Capture (CCDC) equipment in the United Kingdom.

Confirming would serve to inform and educate the public about an issue related to national security and law enforcement. There is an interest in the public understanding the nature and extent of the department's interest in, and awareness of, communication technologies and their potential uses and effects.

Considerations in favour of neither confirming nor denying

There is a strong public interest in not revealing whether or not the Home Office holds any documents governing the use of CCDC equipment in the United Kingdom.
To provide a confirmation or denial would allow interested parties to determine the extent and scope of operational work by law enforcement. This would be prejudicial and

detrimental to the overall effectiveness of work done by law enforcement agencies in tackling serious crime and protecting national security.

Any response the Home Office might provide on this issue – be it a confirmation or denial – would be of significant value to criminal and terrorist groups who would be able to develop a greater understanding of law enforcement capabilities. A confirmation or denial would enable criminals and terrorists to gain an understanding of the nature, extent and investigative capabilities of law enforcement. This would allow such groups to build a picture of security measures or practices that might or might not be in place for protecting the UK. In turn, this would enable such groups to take steps to circumvent them.

Information that undermines the operational integrity of any such activities would adversely affect public safety and have a negative impact on both national security and law enforcement.

National security and law enforcement are of vital importance to protecting the UK. It is clearly not in the public interest to confirm or deny whether material is held that would benefit those who are intending to carry out criminal or terrorist activities to the detriment of the UK.

Conclusions

We conclude that the public interest in maintaining the exclusion of the duty to confirm or deny outweighs the public interest in confirming or denying whether we hold the information in question.

Date 13 March 2017

EXHIBIT C

PRIVACY INTERNATIONAL

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

Information Rights Team
Home Office
Third Floor, Peel Building
2 Marsham Street
London SW1P 4DF

22 May 2017

Re: Freedom of Information Request Reference No. 41663

A. Introduction

1. This is an appeal following a refusal to disclose information made by the Home Office on 13 March 2017. Privacy International respectfully requests an internal review of the decision. Privacy International apologises that this request has been brought slightly outside the two-month time limit for requesting an internal review, but trusts that this short delay has not caused any possible prejudice to the Home Office.

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 use of mobile phone surveillance equipment by various police forces.

4. The application referred to an article making reference to minutes of an Alliance Governance Group meeting in May 2016 between Warwickshire and West Mercia police in which the topic of "Covert Communications Data Capture" (CCDC) equipment was discussed. The application also referred to an article in the Guardian reporting that IMSI catchers were being used by at least seven police forces across the country.

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:

"*Legislation, codes of practice, policy statements, guides, manuals, memoranda, presentations, training materials or other records governing the use of CCDC equipment in the United Kingdom, 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 Regulatory Regime

7. On 13 March 2017, a member of the Information Rights Team responded to our request. That response indicated that "[w]ith regards to legislation and codes of practice, any police investigative activity involving interference with property or wireless telegraphy is regulated by the Police Act 1997, and subject to the Covert Surveillance and Property Interference Code of Practice." The response then refused the remainder of the request, relying on ss.23(5), 24(2), and 31(3) Freedom of Information Act 2000.

8. Insofar as the reference to the Police Act 1997 and the Covert Surveillance and Property Interference Code of Practice were intended to respond to the request for information relating to the regulatory regime in respect of ISMI catchers, the 13 March 2017 letter was woefully inadequate. Please provide:

8.1 Reference to the specific sections and/or paragraphs of the Police Act 1997 and the Covert Surveillance and Property Interference Code of Practice that the Home Office suggests regulates the use of ISMI catchers;

8.2 Explain, by reference to statute and/or publicly accessible policy guidance:

8.2.1 What restrictions exist on when, where, how, and against whom ISMI catchers may be used;

8.2.2 What limitations exist on retention and use of collected data;

8.2.3 What guidance exists on when a warrant or other legal process must be obtained when the use of ISMI catchers may be sought;

8.2.4 What rules exist governing when the existence and use of ISMI catchers may be revealed to the public, criminal defendants, or judges.

D. The Refusal

9. No reasons at all are given for asserting that the absolute exemption in s.23 Freedom of Information Act 2000 or the qualified exemptions in ss.24 and 31 Freedom of Information Act 2000 apply.

10. The only reasons given are in respect of the application of the public interest balancing act under ss.24 and 31. Those reasons can be summarised as follows:

    10.1 That confirming or denying that the Home Office holds information governing the use of CCDC equipment would allow interested parties to determine the extent and scope of operational work by law enforcement. Stating information is held would therefore be prejudicial and detrimental to the overall effectiveness of work done by law enforcement agencies in tackling serious crime and protecting national security;

    10.2 Any response, be it a confirmation or denial, would be of significant value to criminal and terrorist groups who would be able to develop an understanding of the nature, extent and investigative capabilities of law enforcement. This information would allow these groups to build a picture of security measures or practices that might or might not be in place for protecting the UK, thereby enabling such groups to circumvent them;

    10.3 Information undermining the operational integrity of law enforcement activities would adversely affect public safety and have a negative impact on both national security and law enforcement.

E. The Appeal

11. The Home Office response to the request for information is wholly unreasoned. There is no explanation at all as to why the Home Office asserts that any exemption applies in this case.

12. The reasons provided by the Home Office in respect of the public interest balancing test, as set out above, fail to justify the application of NCND in this case. This is for the following four reasons.

13. Firstly, the Home Office response is predicated on a series of *non-sequiturs*:

    13.1 It simply does not follow that merely confirming or denying that the Home Office holds information governing the use of IMSI Catchers would reveal operationally sensitive information about the scope of police activities and operations. This reasoning is not understood. It appears that the Home Office

has confused consideration of "*neither confirm nor deny*" with consideration of the provision of information itself;

13.2 It is not understood why revealing that the Home Office has information governing the use of sophisticated capabilities to collect data would limit operational capabilities. The reasoning set out in paragraph 10.3, above, is nonsensical.

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

14.1 The fact that policy guidance and other records governing the use of IMSI Catchers cannot conceivably fall within any exemption;

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

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

15.1 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;

15.2 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 policy guidance and other records governing the use of IMSI Catchers;

16. 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:

16.1 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*";[1]

[1] *Philip Kalman v Information Commissioner and the Department of Transport* (EA/2009/111 8 July 2010).

16.2 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.[2] It also flies in the face of the Article 10 right to receive information, as recently confirmed by the European Court of Human Rights;[3]

16.3 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*".[4]

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

17.1 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;

17.2 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;

17.3 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.

F. The Appeal

18. Privacy International respectfully requests the Home Office to re-consider the original request made for information as set out above.

Scarlet Kim

Legal Officer
Privacy International

---

[2] *Galloway v Information Commissioner v The Central and North West London NHS Foundation Trust* (2009) 108 BMLR 50, at §70.
[3] *Magyar Helsinki Bizottság v Hungary* (App. no. 18030/11).
[4] *Mohamed and another v Secretary of State for the Home Department* [2014] 1 WLR 4240, per Maurice Kay LJ, at §40.

EXHIBIT D

Home Office

Performance and Risk Directorate
2 Marsham Street
London SW1P 4DF

0207 035 4848
(switchboard)

www.gov.uk

Scarlet Kim
Privacy International
62 Britton Street
London, EC1M 5UY

scarlet@privacyinternational.org

17 August 2017

Dear Ms Kim

Freedom of Information reference number: 41663 – internal review

I write further to my email of 19 July in which I provided an update on the progress of the internal review which you requested on 22 May.

I can now confirm that this review has been completed, and I have assessed the substance of the response provided to you. I can also confirm that I was not involved in the initial handling of your Freedom of Information (FOI) request.

This review is based solely on the provisions of the Freedom of Information Act 2000 (FOIA).

Your FOI request of 1 December 2016 asked for information governing the use of Covert Communications Data Capture (CCDC) equipment in the UK and can be seen in full at **Annex A**.

At this point I would like to offer my apologies for the time taken to respond to your internal review request. The Home Office always aims to reply to all internal review requests within a maximum of 40 working days, but this is not always possible despite our best efforts. I can understand your frustration at the time taken to respond, and am sorry for any inconvenience that may have been caused. Your patience throughout has been much appreciated.

The FOI response (which can be viewed at **Annex B**) provided information concerning the Police Act 1997 and the Covert Surveillance and Property Interference Code of Practice, but beyond this neither confirmed nor denied whether any of the information you requested was held by the Department, with reliance on the following exemptions:

- Section 23(5) – Information supplied by, or relating to, bodies dealing with security matters
- Section 24(2) – National security
- Section 31(3) – Law enforcement

Your internal review request can be viewed in full at **Annex C**, but the crux of your complaint is that you do not believe the neither confirm nor deny (NCND) approach was correct. You also ask for further detail in relation to the legislation and guidance on IMSI catchers, which I shall address first.

With reference to your question at paragraph 8, neither the Police Act nor the code of practice is specific to any particular form of technology. However, Part 3 of the act and Chapter 7 of the code would be of particular relevance to anything that may interfere with property or wireless telegraphy.

In relation to your complaint against the use of the NCND approach, I have considered the points you have raised and consulted with the responding unit and I am satisfied that the NCND approach was the correct approach in this instance.

Confirming or denying if any of the information within the scope of the request is held would (whether the information is held or not) reveal information relating to the role of the security bodies (section 23). The work of the security bodies – by their very nature – relates to the security of the UK (section 24), and in order to protect the security of the UK, security bodies work closely with other law enforcement agencies (section 31).

Confirming or denying whether the information is held would undermine the techniques and capabilities used by such agencies (and security bodies) for the purposes of safeguarding the national security of the UK.

I have also had sight of the public interest test arguments in favour of confirming or denying whether the requested information is held, in the case of qualified exemptions, and I am satisfied that they are valid and that the correct decision was reached.

You may be interested to know that the Information Commissioner has recently upheld this same approach on very similar subject matters. Decision notices FS50665716 and FS50660527 can be accessed via this link:
http://search.ico.org.uk/ico/search/decisionnotice?keywords=IMSI

Conclusion

I have concluded that the original FOI response was correct to rely on the cited exemptions, and that in all the circumstances of the case, the exclusion of the duty to neither confirm or deny outweighs the public interest in disclosing whether the Department holds the information in scope of your request.

This completes the internal review.

Yours sincerely

R Taylor
Information Rights Team

Annex A

Freedom of Information request – Matthew Rice (Privacy International) – 1 November 2016

PRIVACY INTERNATIONAL

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

Freedom of Information Officer
Direct communications unit
Home Office
2 Marsham Street
London
SW1P 4DF

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 several police forces.

Alliance Governance Group Meeting Minutes

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 minutes of an Alliance Governance Group meeting in May 2016 between Warwickshire and West Mercia Police in which the topic of "Covert Communications Data Capture" (CCDC) equipment was discussed.[2]

Specifically, the minutes state: "Within the West Midlands region **both West Midlands and Staffordshire Police** have recently **purchased and operated 4G compatible CCDC equipment**." The Minutes then indicate that the following decision was made: "**Both PCCs [West Mercia and Warwickshire Police and Crime Commissioners] agreed to Replacing the existing [CCDC] equipment with a new supplier."**

Guardian Article

I also refer to the 10 October 2016 article published by the Guardian, "Controversial snooping technology 'used by at least seven police forces'".[3] 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." In addition to West Midlands, Staffordshire, West Mercia and

[1] https://thebristolcable.org/2016/10/imsi/
[2] https://thebristolcable.org/wp-content/uploads/2016/10/09-imsi-4.pdf
[3] https://www.theguardian.com/world/2016/oct/10/controversial-phone-snooping-technology-imsi-catcher-seven-police-forces?CMP=twt_gu

Warwickshire, the other forces understood to be using this technology include the Metropolitan Police Service, Avon and Somerset and South Yorkshire.

Record Requests

As the Home Office is responsible for policing across the country and the development of relevant policy and legislation in this area I believe you hold records relevant to the regulation of the use of CCDC equipment by police in the United Kingdom.

Privacy International requests the following records:

1. Legislation, codes of practice, policy statements, guides, manuals, memoranda, presentations, training materials or other records governing the use of CCDC equipment in the United Kingdom, 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

Annex B

Freedom of Information response – 41663 - Information Rights Team – 13 March 2017

Home Office

Information Rights Team
2 Marsham Street
London SW1P 4DF

020 7035 4848
(switchboard)

www.homeoffice.gov.uk

Mr Matthew Rice
Via email to:
matthew@privacyinternational.org

13 March 2017

Dear Mr Rice

Freedom of Information Act 2000 Request (Our Reference 41663)

Thank you for your email of 1 November 2016, in which you ask for the following information:

> *Legislation, codes of practice, policy statements, guides, manuals, memoranda, presentations, training materials or other records governing the use of CCDC equipment in the United Kingdom, 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.*

A full copy of your request can be found in **Annex A**. Your request has been handled as a request for information under the Freedom of Information Act 2000.

With regards to legislation and codes of practice, any police investigative activity involving interference with property or wireless telegraphy is regulated by the Police Act 1997, and subject to the Covert Surveillance and Property Interference Code of Practice. These are available at www.gov.uk.

We neither confirm nor deny whether the Home Office holds any information within scope of the remainder your request. Sections 23(5) (Information relating to security bodies), 24(2) (National security) and 31(3) (Law enforcement) absolve us from the requirement to say whether or not we hold information.

Section 23 relates to information supplied by, or relating to bodies dealing with security matters. This exemption applies to any information supplied directly by a security body and information originating from a security body that is provided by a third party. Section 23(5) is an absolute exemption, meaning information can be withheld automatically, without considering the public interest in favour of disclosure.

Section 24 and section 31 of the Act are qualified exemptions and require consideration of the public interest test. An explanation of the public interest test is set out in **Annex B**.

The response should not be taken as conclusive evidence that the information you have requested is or is not held by the Home Office.

If you are dissatisfied with this response you may request an independent internal review of our handling of your request by submitting a complaint within two months to the address below, quoting reference **41663**. If you ask for an internal review, it would be helpful if you could say why you are dissatisfied with the response.

Information Rights Team
Home Office
Third Floor, Peel Building
2 Marsham Street
London SW1P 4DF
Email: info.access@homeoffice.gsi.gov.uk

As part of any internal review the Department's handling of your information request will be reassessed by staff who were not involved in providing you with this response. If you remain dissatisfied after this internal review, you would have a right of complaint to the Information Commissioner as established by section 50 of the Freedom of Information Act.

Yours sincerely

S Mason
Information Rights Team
Switchboard 020 7035 4848 Email info.access@homeoffice.gsi.gov.uk

Annex A – FOI request

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 several police forces.

Alliance Governance Group Meeting Minutes

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 minutes of an Alliance Governance Group meeting in May 2016 between Warwickshire and West Mercia Police in which the topic of "Covert Communications Data Capture" (CCDC) equipment was discussed.

Specifically, the minutes state: "Within the West Midlands region **both West Midlands and Staffordshire Police** have recently **purchased and operated 4G compatible CCDC equipment**." The Minutes then indicate that the following decision was made: "**Both PCCs [West Mercia and Warwickshire Police and Crime Commissioners] agreed to Replacing the existing [CCDC] equipment with a new supplier.**"

Guardian Article

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." In addition to West Midlands, Staffordshire, West Mercia and Warwickshire, the other forces understood to be using this technology include the Metropolitan Police Service, Avon and Somerset and South Yorkshire.

Record Requests

As the Home Office is responsible for policing across the country and the development of relevant policy and legislation in this area I believe you hold records relevant to the regulation of the use of CCDC equipment by police in the United Kingdom.

Privacy International requests the following records:

> Legislation, codes of practice, policy statements, guides, manuals, memoranda, presentations, training materials or other records governing the use of CCDC equipment in the United Kingdom, 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

Annex B – Public Interest Test

Freedom of Information request from Matthew Rice (reference 41663)

Response

We neither confirm nor deny whether we hold the information that you have requested under section 23(5), 24(2) and 31(3) of the FOI Act.

Section 24(2) states:

> *(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 31(3) states:

> *(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).*

Public interest in relation to sections 24(2) and 31(3)

Section 17(3) of the Act requires us to conduct a Public Interest Test when considering the neither confirm nor deny provision of a qualified exemption. In applying this exemption, we are required to consider whether, in all the circumstances of the case, the public interest in neither confirming nor denying outweighs the public interest in disclosing whether the Home Office holds the information you have requested.

The 'public interest' is not the same as what interests the public. In carrying out a PIT, we consider the greater good or benefit to the community as a whole in saying whether information is held or not. The 'right to know' must be balanced against the need to enable effective government and to serve the best interests of the public. The FOI Act is 'applicant blind'. This means that we cannot, and do not, ask about the motives of anyone who asks for information. In providing a response to one person, we are expressing a willingness to provide the same response to anyone, including those who might represent a threat to the UK.

Considerations in favour of confirming or denying

In the interests of transparency and openness, it is accepted that there may be a general public interest in knowing what, if any, information the Home Office holds governing the use of Covert Communications Data Capture (CCDC) equipment in the United Kingdom.

Confirming would serve to inform and educate the public about an issue related to national security and law enforcement. There is an interest in the public understanding the nature and extent of the department's interest in, and awareness of, communication technologies and their potential uses and effects.

Considerations in favour of neither confirming nor denying

There is a strong public interest in not revealing whether or not the Home Office holds any documents governing the use of CCDC equipment in the United Kingdom.
To provide a confirmation or denial would allow interested parties to determine the extent and scope of operational work by law enforcement. This would be prejudicial and

detrimental to the overall effectiveness of work done by law enforcement agencies in tackling serious crime and protecting national security.

Any response the Home Office might provide on this issue – be it a confirmation or denial – would be of significant value to criminal and terrorist groups who would be able to develop a greater understanding of law enforcement capabilities. A confirmation or denial would enable criminals and terrorists to gain an understanding of the nature, extent and investigative capabilities of law enforcement. This would allow such groups to build a picture of security measures or practices that might or might not be in place for protecting the UK. In turn, this would enable such groups to take steps to circumvent them.

Information that undermines the operational integrity of any such activities would adversely affect public safety and have a negative impact on both national security and law enforcement.

National security and law enforcement are of vital importance to protecting the UK. It is clearly not in the public interest to confirm or deny whether material is held that would benefit those who are intending to carry out criminal or terrorist activities to the detriment of the UK.

Conclusions

We conclude that the public interest in maintaining the exclusion of the duty to confirm or deny outweighs the public interest in confirming or denying whether we hold the information in question.

Date 13 March 2017

Annex C

Internal Review request – 41663 – Scarlet Kim (Privacy International) – 22 May 2017

PRIVACY INTERNATIONAL

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

Information Rights Team
Home Office
Third Floor, Peel Building
2 Marsham Street
London SW1P 4DF

22 May 2017

Re: Freedom of Information Request Reference No. 41663

A. Introduction

1. This is an appeal following a refusal to disclose information made by the Home Office on 13 March 2017. Privacy International respectfully requests an internal review of the decision. Privacy International apologises that this request has been brought slightly outside the two-month time limit for requesting an internal review, but trusts that this short delay has not caused any possible prejudice to the Home Office.

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 use of mobile phone surveillance equipment by various police forces.

4. The application referred to an article making reference to minutes of an Alliance Governance Group meeting in May 2016 between Warwickshire and West Mercia police in which the topic of "Covert Communications Data Capture" (CCDC) equipment was discussed. The application also referred to an article in the Guardian reporting that IMSI catchers were being used by at least seven police forces across the country.

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:

"*Legislation, codes of practice, policy statements, guides, manuals, memoranda, presentations, training materials or other records governing the use of CCDC equipment in the United Kingdom, 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 Regulatory Regime

7. On 13 March 2017, a member of the Information Rights Team responded to our request. That response indicated that "[w]ith regards to legislation and codes of practice, any police investigative activity involving interference with property or wireless telegraphy is regulated by the Police Act 1997, and subject to the Covert Surveillance and Property Interference Code of Practice." The response then refused the remainder of the request, relying on ss.23(5), 24(2), and 31(3) Freedom of Information Act 2000.

8. Insofar as the reference to the Police Act 1997 and the Covert Surveillance and Property Interference Code of Practice were intended to respond to the request for information relating to the regulatory regime in respect of ISMI catchers, the 13 March 2017 letter was woefully inadequate. Please provide:

8.1 Reference to the specific sections and/or paragraphs of the Police Act 1997 and the Covert Surveillance and Property Interference Code of Practice that the Home Office suggests regulates the use of ISMI catchers;

8.2 Explain, by reference to statute and/or publicly accessible policy guidance:

8.2.1 What restrictions exist on when, where, how, and against whom ISMI catchers may be used;

8.2.2 What limitations exist on retention and use of collected data;

8.2.3 What guidance exists on when a warrant or other legal process must be obtained when the use of ISMI catchers may be sought;

8.2.4 What rules exist governing when the existence and use of ISMI catchers may be revealed to the public, criminal defendants, or judges.

D. The Refusal

9. No reasons at all are given for asserting that the absolute exemption in s.23 Freedom of Information Act 2000 or the qualified exemptions in ss.24 and 31 Freedom of Information Act 2000 apply.

10. The only reasons given are in respect of the application of the public interest balancing act under ss.24 and 31. Those reasons can be summarised as follows:

    10.1 That confirming or denying that the Home Office holds information governing the use of CCDC equipment would allow interested parties to determine the extent and scope of operational work by law enforcement. Stating information is held would therefore be prejudicial and detrimental to the overall effectiveness of work done by law enforcement agencies in tackling serious crime and protecting national security;

    10.2 Any response, be it a confirmation or denial, would be of significant value to criminal and terrorist groups who would be able to develop an understanding of the nature, extent and investigative capabilities of law enforcement. This information would allow these groups to build a picture of security measures or practices that might or might not be in place for protecting the UK, thereby enabling such groups to circumvent them;

    10.3 Information undermining the operational integrity of law enforcement activities would adversely affect public safety and have a negative impact on both national security and law enforcement.

E. The Appeal

11. The Home Office response to the request for information is wholly unreasoned. There is no explanation at all as to why the Home Office asserts that any exemption applies in this case.

12. The reasons provided by the Home Office in respect of the public interest balancing test, as set out above, fail to justify the application of NCND in this case. This is for the following four reasons.

13. Firstly, the Home Office response is predicated on a series of *non-sequiturs*:

    13.1 It simply does not follow that merely confirming or denying that the Home Office holds information governing the use of IMSI Catchers would reveal operationally sensitive information about the scope of police activities and operations. This reasoning is not understood. It appears that the Home Office

has confused consideration of "*neither confirm nor deny*" with consideration of the provision of information itself;

13.2 It is not understood why revealing that the Home Office has information governing the use of sophisticated capabilities to collect data would limit operational capabilities. The reasoning set out in paragraph 10.3, above, is nonsensical.

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

14.1 The fact that policy guidance and other records governing the use of IMSI Catchers cannot conceivably fall within any exemption;

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

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

15.1 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;

15.2 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 policy guidance and other records governing the use of IMSI Catchers;

16. 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:

16.1 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*";[1]

[1] *Philip Kalman v Information Commissioner and the Department of Transport* (EA/2009/111 8 July 2010).

16.2 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.[2] It also flies in the face of the Article 10 right to receive information, as recently confirmed by the European Court of Human Rights;[3]

16.3 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*".[4]

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

17.1 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;

17.2 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;

17.3 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.

F. The Appeal

18. Privacy International respectfully requests the Home Office to re-consider the original request made for information as set out above.

Scarlet Kim

Legal Officer
Privacy International

---

[2] *Galloway v Information Commissioner v The Central and North West London NHS Foundation Trust* (2009) 108 BMLR 50, at §70.
[3] *Magyar Helsinki Bizottság v Hungary* (App. no. 18030/11).
[4] *Mohamed and another v Secretary of State for the Home Department* [2014] 1 WLR 4240, per Maurice Kay LJ, at §40.

Annex D

Further complaint procedure

This completes the internal review process by the Home Office. If you remain dissatisfied with the response to your FOI request, you have the right of complaint to the Information Commissioner at the following address:

The Information Commissioner
Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF

EXHIBIT E

A Comparative Perspective:
IMSI Catcher Freedom of Information Requests in the United States

I. Introduction

In the United States, a range of requests pursuant to federal and state freedom of information laws relating to law enforcement acquisition, use and regulation of IMSI Catchers have resulted in the disclosure of 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. Privacy International provides an overview of US freedom of information laws, a summary of these requests, and a summary of the records produced, which are publicly available. It believes that this comparative perspective may prove useful to the Information Commissioner in considering the refusals of the public bodies to confirm or deny the existence of records relating to the acquisition, use and regulation of IMSI Catchers in the UK.

II. A Summary of US Freedom of Information Laws

In the United States, the Freedom of Information Act ("FOIA"), which took effect in 1967, provides that any person has a right, enforceable in court, to obtain access to federal agency records, except to the extent that such records (or portions of them) are protected from public disclosure pursuant to an exemption or exclusion.[1] FOIA therefore established a statutory right of public access to information held by the Executive Branch in the federal government. The United States Supreme Court has explained that *"[t]he basic purpose of FOIA is to ensure an informed citizenry, vital to the functioning of a democratic society, needed to check against corruption and to hold the governors accountable to the governed*."[2] It has further submitted that FOIA is a "*means for citizens to know 'what their Government is up to*'" and that "*[t]his phrase should not be dismissed as a convenient formalism" but rather, "defines a structural necessity in a real democracy*."[3] Thus FOIA features "*broad provisions favouring disclosure, coupled with the specific exemptions*" reflecting the intent of Congress "'*to reach a workable balance between the right of the public to know and the need of the Government*'" to protect certain information.[4]

---

[1] 5 U.S.C. §552 (2006), amended by OPEN Government Act of 2007, Pub. L. No. 110-175, 121 Stat. 2524; *see also* DOJ Guide to the Freedom of Information Act (2009 edition), available at https://www.justice.gov/oip/doj-guide-freedom-information-act. Unlike the UK, which excludes certain bodies like the National Crime Agency and Government Communications Headquarters from the Freedom of Information Act 2000, no federal agency benefits from a similar blanket exclusion from FOIA. As a point of comparison, both the Federal Bureau of Investigation ("FBI") and the National Security Agency are subject to FOIA.

[2] NLRB v. Robbins Tire & Rubber Co., 437 U.S. 214, 242 (1978).

[3] NARA v. Favish, 541 U.S. 157, 171-72 (2004) (quoting DOJ v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 774 (1989)).

[4] John Doe Agency v. John Doe Corp., 493 U.S. 146, 152-53 (1989) (quoting H.R. Rep. No. 89-1497, at 6 (1966)); *see also* Dep't of the Air Force v. Rose, 425 U.S. 352, 361 (1976) (holding that "limited exemptions do not obscure the basic policy that disclosure, not secrecy, is the dominant objective of the Act").

FOIA articulates nine exemptions from disclosure, and they are generally discretionary, rather than mandatory, in nature.[5] The exemptions are:[6]

1. Information that is classified in the interest of national defence or foreign policy
2. Information related solely to the internal personnel rules and practices of an agency[7]
3. Information that is specifically exempted from disclosure by another federal law
4. Trade secrets and commercial or financial information obtained from a person and privileged or confidential
5. Privileged communications within or between agencies, such as those protected by attorney-work product privilege and attorney-client privilege
6. Information that, if disclosed, would constitute a clearly unwarranted invasion of personal privacy, such as personnel or medical files
7. Information compiled for law enforcement purposes that
    a. Could reasonably be expected to interfere with enforcement proceedings
    b. Would deprive a person of a right to a fair trial or impartial adjudication
    c. Could reasonably be expected to constitute an unwarranted invasion of personal privacy
    d. Could reasonably be expected to disclose the identity of a confidential source
    e. Would disclose techniques and procedures for law enforcement investigations or prosecutions or guidelines for investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law
    f. Could reasonably be expected to endanger the life or physical safety of any individual
8. Information that concerns the supervision of financial institutions
9. Geological and geophysical information on wells

In addition to exemptions, FOIA also articulates three narrow categories of exclusions for particularly sensitive law enforcement matters. These exclusions permit a federal law enforcement agency, in three exceptional circumstances, to "treat the records as not subject to the requirements of [FOIA]."[8] The exclusions are designed to protect the existence of:

1. An ongoing criminal law enforcement investigation when the subject of the investigation is unaware that it is pending and disclosure could reasonably be expected to interfere with enforcement proceedings
2. Informant records when the informant's status has not been officially confirmed (limited to criminal law enforcement agencies)

---

[5] *See* 5 U.S.C. §552(b), (d); *see also* Chrysler Corp. v. Brown, 441 U.S. 281, 293 (1979).
[6] For detail on the exemptions and general FOIA processes, see *Federal Open Government Guide*, RCFP (2009) https://www.rcfp.org/rcfp/orders/docs/HOW2FOI.pdf; *Freedom of Information Act Exemptions*, U.S. Dept. of Justice, 23 July 2014, https://www.justice.gov/sites/default/files/oip/legacy/2014/07/23/foia-exemptions.pdf/.
[7] This exemption covers both internal "housekeeping" or personnel documents that Congress determined were not within the public interest, and any documents that could be used to circumvent laws or gain unfair advantage over members of the public.
[8] 5 U.S.C. § 552(c)(1), (c)(2), (c)(3).

3. Foreign intelligence or counterintelligence, or international terrorism records when the existence of such records is classified (limited to the FBI)

Unlike the UK's Freedom of Information Act 2000, there are no provisions explicitly addressing a "neither confirm nor deny" response to an information request in the federal FOIA. However, the US government has sometimes taken the position that even confirming or denying the existence of information is necessary pursuant to two of the exemptions. This position is referred to as a "Glomar" response. First, agencies may assert that confirming or denying the existence of information could compromise national security (under the first exemption).[9] Second, agencies may assert that confirming or denying the existence of information relating to a person's involvement in a criminal investigation would constitute a violation of privacy (under the seventh exemption).[10]

Generally speaking, the FOIA process is as follows. An individual submits a written FOIA request, which must "*reasonably describe*" the records sought, to an agency's designated FOIA office.[11] The agency has 20 working days to make a determination on the request. A requester has the right to administratively appeal any adverse determination made on the initial request. The agency has 20 working days to make a determination on an administrative appeal.[12] A requester may thereafter seek to compel production of any requested records by filing a complaint in a United States federal district court.

States also have their own open records laws, which govern access to state agency records. While the specific provisions of these frameworks vary state by state, many of these frameworks mimic the purpose and structure of federal FOIA.[13] For example, the New York Freedom of Information Law ("FOIL") was intentionally "*patterned after the federal Freedom of Information Act, and accordingly, federal case law and legislative history on the scope of the federal act are instructive in interpreting New York's law, including its exemptions*."[14] Thus, FOIL similarly provides a right, enforceable in court, to obtain access to state agency records, except to the extent that such records (or portions of them) are protected from public disclosure pursuant to an exemption. Many of the exemptions are similar to those articulated in FOIA, including, *inter alia*, information specifically exempted from disclosure by another state or federal law; trade secrets; and information compiled for specified law enforcement purposes. The procedure for requesting records and challenging adverse

[9] Reporters Committee for Freedom of the Press, *Federal FOIA Appeals Guide*, Exemption 1, Pt. II.F, https://www.rcfp.org/federal-foia-appeals-guide/exemption-1/ii-appealing-agency%E2%80%99s-withholding-records-substantive-grou-10.
[10] *Id*. at Exemption 7, Pt. I.C.iii. https://www.rcfp.org/federal-foia-appeals-guide/exemption-7/ii-harm-disclosure/c-7c/iii-glomar-response.
[11] 5 U.S.C. § 552 (a)(3)(A).
[12] An agency's failure to comply with the time limits to respond to an initial request or an administrative appeal may be treated as "constructive exhaustion", entitling the requester to seek judicial review. *See* 5 U.S.C. § 552(a)(6)(C).
[13] A comprehensive guide to each state's open laws framework is available at Reporters Committee for a Free Press, *Open Government Guide*, https://www.rcfp.org/open-government-guide.
[14] Reporters Committee for Freedom of the Press, *New York – Open Government Guide*, Pt. II.A.1.c, https://www.rcfp.org/new-york-open-government-guide/ii-exemptions-and-other-legal-limitations/exemptions-open-records-s-3 (citing relevant New York case law in support of this statement).

determinations is also similar to that provided by FOIA, albeit with slightly different timelines for an agency's response.

III. FOIA Requests to Federal Agencies for IMSI Catcher Records

In the United States, a wide array of federal agencies deploy IMSI Catchers, including the FBI, the Drug Enforcement Administration ("DEA"), and Immigration and Customs Enforcement ("ICE").[15] Civil society organisations have managed to obtain information regarding these agencies' acquisition, use and regulation of IMSI Catchers through FOIA requests. Below, Privacy International summarises several of these requests and the information that was disclosed as a result. It is worth noting that none of the federal agencies subject to FOIA requests in the examples described below relied on a Glomar (*i.e.* NCND) response.

A. Electronic Privacy Information Center – FBI

In February 2012, the Electronic Privacy Information Center ("EPIC") submitted a FOIA request to the FBI seeking information concerning contracts relating to IMSI Catchers, technical specifications of IMSI Catchers, the legal basis for the use of IMSI Catchers, procedural requirements or guidelines for using IMSI Catchers, and Privacy Impact Assessments or Reports concerning the use of IMSI Catchers.[16] The FBI released documents in 13 batches, in part as a result of an EPIC suit to compel production. The disclosed records include internal DOJ guidance on IMSI Catchers, including procedures for loaning electronic surveillance devices to state police.[17] They further reveal that the FBI has been using IMSI Catchers since at least the mid-1990s,[18] has established a specialist mobile phone surveillance group called the "Wireless Intercept and Tracking Team", and uses other mobile phone surveillance devices, in addition to IMSI Catchers.[19]

B. American Civil Liberties Union of Northern California – Department of Justice

In April 2013, the American Civil Liberties Union ("ACLU") of Northern California submitted a FOIA request to the Department of Justice ("DOJ") seeking information about

---

[15] ACLU, *Stingray Tracking Devices: Who's Got Them?*, https://www.aclu.org/issues/privacy-technology/surveillance-technologies/stingray-tracking-devices-whos-got-them.
[16] *EPIC v. FBI – Stingray / Cell Site Simulator*, EPIC, https://epic.org/foia/fbi/stingray/.
[17] Ryan Gallagher, *FBI Documents Shine Light on Clandestine Cellphone Tracking Tool*, Slate, 10 Jan. 2013, http://www.slate.com/blogs/future_tense/2013/01/10/stingray_imsi_catcher_fbi_documents_shine_light_on_controversial_cellphone.html. All of the disclosed records are available on the EPIC website at *EPIC v. FBI – Stingray / Cell Site Simulator*, EPIC, https://epic.org/foia/fbi/stingray/.
[18] Ryan Gallagher, *FBI Files l History Behind Clandestine Cellphone Tracking Tool*, Slate, 15 Feb. 2013, http://www.slate.com/blogs/future_tense/2013/02/15/stingray_imsi_catcher_fbi_files_unlock_history_behind_cellphone_tracking.html.
[19] Ryan Gallagher, *FBI Files Reveal New Info on Clandestine Phone Surveillance Unit*, Slate, 8 Oct. 2013, http://www.slate.com/blogs/future_tense/2013/10/08/fbi_wireless_intercept_and_tracking_team_files_reveal_new_information_on.html.

the federal government's use of IMSI Catchers.[20] Following a suit to challenge DOJ's refusal to disclose the requested records, the court ordered the government to produce a portion of the requested records. The disclosed records include memos and "template" court applications that DOJ provides to federal prosecutors as well as procedures for the "Emergency Installation" of IMSI Catchers.[21]

C. American Civil Liberties Union – Various Federal Agencies

In November 2014, the ACLU sent a FOIA request to several federal law enforcement agencies seeking information concerning their use of IMSI Catchers mounted on aircraft to track and locate cell phones.[22] The request was sent to the FBI, DEA, ICE and the U.S. Marshals Service. The disclosed records include:[23]

- Contracts and other purchase records, which reveal that the U.S. Marshals Service spent more than $10 million in hardware and software purchases from Harris Corporation, the leading U.S. vendor of IMSI Catchers, from 2009 to 2014
- Policy directives from the U.S. Marshals Service Technical Operations Group, which discuss the rules for various kinds of electronic and aerial surveillance, although they do not clearly explain the rules applying to airborne IMSI Catchers
- Purchase records, which reveal that the DEA's El Paso Division purchased $412,871 in IMSI Catcher equipment in 2013

A similar request by the Electronic Frontier Foundation to the DOJ and the FBI also resulted in the disclosure of records. Those records include internal emails and presentations from the FBI, which contain discussions between FBI lawyers and the Operational Technology Division, which develops and oversees the FBI's surveillance techniques.[24]

IV. Freedom of Information Requests to State Agencies for IMSI Catcher Records

In addition to the federal agencies, a large number of state agencies also deploy IMSI Catchers. Civil society organisations and journalists have similarly managed to obtain

---

[20] *ACLU v. DOJ*, ACLU of Northern California, 13 Jan. 2016, https://www.aclunc.org/our-work/legal-docket/aclu-v-doj-stingrays.

[21] All of the disclosed records are available on the ACLU of Northern California website at Linda Lye, *New Docs: DOJ Admits that StingRays Spy on Innocent Bystanders*, ACLU of Northern California, Oct. 28, 2015, https://www.aclunc.org/blog/new-docs-doj-admits-stingrays-spy-innocent-bystanders.

[22] Nathan Freed Wessler, *ACLU Releases New FOIA Documents on Aerial Cell Phone Surveillance*, ACLU, 17 Mar. 2016, https://www.aclu.org/blog/privacy-technology/surveillance-technologies/aclu-releases-new-foia-documents-aerial-cell-phone.

[23] All of the disclosed records are available at Wessler, *ACLU Releases New FOIA Documents*, https://www.aclu.org/blog/privacy-technology/surveillance-technologies/aclu-releases-new-foia-documents-aerial-cell-phone.

[24] Andrew Crocker, *New FOIA Documents Confirm FBI Used Dirtboxes on Planes Without Any Policies or Legal Guidance*, Electronic Frontier Foundation, 9 Mar. 2016, https://www.eff.org/deeplinks/2016/03/new-foia-documents-confirm-fbi-used-dirtboxes-planes-without-any-policies-or-legal. All of the disclosed records are available at *US Marshals Airborne IMSI Catchers*, Electronic Frontier Foundation, https://www.eff.org/cases/us-marshals-airborne-imsi-catchers.

information regarding these agencies' acquisition, use and regulation of IMSI Catchers through FOIA requests. Below, Privacy International summarises several of these requests and the information that was disclosed as a result.

A. Florida

In 2014, the ACLU sent a request pursuant to the Florida Public Records Law to three dozen police and sheriffs' departments in Florida seeking information, *inter alia*, concerning the acquisition, use, and regulation of IMSI Catchers.[25] The records disclosed include:[26]

Florida Department of Law Enforcement ("FDLE")

- Documents revealing the FLDE has:
    - Spent more than $3 million on IMSI Catchers and related equipment since 2008
    - Signed agreements with at least 11 local and regional law enforcement agencies to permit them to use and share its IMSI Catchers
    - Identified 1,835 uses of IMSI Catcher equipment in Florida
- A confidentiality agreement between the FLDE and Harris Corporation

Tallahassee Police Department ("TPD")

- Documents revealing the TPD has:
    - Used IMSI Catchers in more than 250 investigations between 2007 and 2014, with robbery, burglary, and theft investigations representing nearly a third of the total
    - Permitted other police departments to use IMSI Catchers the TPD had borrowed from the FLDE
- The full investigative files from 11 cases where IMSI Catchers were used

Miami-Dade Police Department

- Purchase records for IMSI Catchers from Harris Corporation
- Documents indicating it has used IMSI Catchers in 59 closed criminal cases within a one-year period ending in May 2014

In general, the records disclosed revealed that in many investigations, the police failed to seek a court order to use an IMSI Catcher and, in circumstances where they did, they failed to seek a warrant (relying instead on a court order with a lower legal threshold). Furthermore, they revealed a pattern of secrecy, including concealing information about the use of IMSI Catchers in investigative files and court filings. None of the agencies produced any policies

[25] Nathan Freed Wessler, *ACLU-Obtained Documents Reveal Breadth of Secretive Stingray Use in Florida*, ACLU, 22 Feb. 2015, https://www.aclu.org/blog/free-future/aclu-obtained-documents-reveal-breadth-secretive-stingray-use-florida?redirect=blog/national-security-technology-and-liberty/aclu-obtained-documents-reveal-breadth-secretive-sting.

[26] All of the disclosed records are available at *Florida Stingray FOIA*, ACLU, 22 Feb. 2015, https://www.aclu.org/cases/florida-stingray-foia.

or guidelines governing their use of IMSI Catchers or restricting how and when they can be deployed.[27]

B. New York

In 2014, the New York Civil Liberties Union ("NYCLU") sent a FOIL request to the New York State Police and the Erie County Sheriff's Office seeking information, *inter alia*, concerning the acquisition, use, and regulation of IMSI Catchers. In 2014, it sent the same FOIL request to the New York City Police Department ("NYPD") and the Rochester Police Department ("RPD").

The records disclosed by the New York State Police include invoices and purchase orders for IMSI Catchers.[28]

The records disclosed by the Erie County Sheriff's Office following a lawsuit by the NYCLU include:

- Purchase orders
- A letter from the manufacturer of the IMSI Catcher
- A confidentiality agreement between the Sheriff's Office and the FBI, requiring the Sheriff's Office to maintain near total secrecy over Stingray records, including in court filings, unless the Office receives written consent from the FBI
- A procedural manual
- Summary reports of instances when the IMSI Catcher was used, revealing that the Sheriff's Office used Stingrays at least 47 times between 2010 and 2014 and only obtained a court order in one of those instances

It is worth noting that the court determined that the Sheriff's Office had "*no reasonable basis for denying access*" to the records sought by the NYCLU.

The records disclosed by the RPD include:

- Documents revealing that the RPD has spent approximately $200,000 since 2011 on IMSI Catcher hardware, software and training
- Correspondence between the RPD and Harris Corporation suggesting that IMSI Catchers may require costly yearly maintenance subscriptions to remain operational and revealing that Harris Corporation attempted to coax the RPD to spend approximately $388,000 to upgrade their existing IMSI Catcher in 2013
- A confidentiality agreement between the RPD and the FBI
- Surveillance policies, including instructions regarding use of its IMSI Catcher

[27] *See* Wessler, *ACLU-Obtained Documents Reveal Breadth of Secretive Stingray Use in Florida*, https://www.aclu.org/blog/free-future/aclu-obtained-documents-reveal-breadth-secretive-stingray-use-florida?redirect=blog/national-security-technology-and-liberty/aclu-obtained-documents-reveal-breadth-secretive-sting.

[28] All of the disclosed records are available at *Stingrays*, NYCLU, https://www.nyclu.org/en/stingrays.

- Documents revealing that the RPD used its IMSI Catcher 13 times between 2012 and 2015 and sought legal authorization approximately 69% of the time

The records disclosed by the NYPD include documents revealing that it used IMSI Catchers over 1,000 ties between 2008 and 2015 without a written policy and without obtaining a warrant (but rather a "pen register order" that requires the government to meet a lower legal threshold). The NYCLU is engaged in ongoing litigation against the NYPD to compel production of other records pursuant to its FOIL request.[29]

C. Michigan

In 2015, the ACLU of Michigan submitted a request pursuant to the Michigan Freedom of Information Act to the Michigan State Police ("MSP") seeking records, *inter alia*, concerning the acquisition, use, and regulation of IMSI Catchers.[30] The MSP released records in two batches; those records include:[31]

- Invoices, emails and other documents relating to the purchase and upgrade of IMSI Catcher equipment
- Documents revealing that IMSI Catchers were used in 128 cases ranging from homicide to burglary and fraud in 2014

D. CityLab

In 2016, the media outlet CityLab sent freedom of information requests to 50 of the largest police departments across the United States seeking information relating to the acquisition of mobile phone surveillance devices, including IMSI Catchers.[32] Of the 50 departments who received such requests, only eight claimed not to have acquired any of the mobile phone surveillance tools identified by CityLab; at least 12 admitted to having IMSI Catchers. CityLab also identified that departments with IMSI Catchers were largely seeking to improve their surveillance capabilities through upgrades to this equipment.[33]

6 February 2018 Privacy International

---

[29] *NYCLU Sues NYPD After It Refuses to Disclose Critical Information about Stingrays*, NYCLU, 19 May 2016, https://www.nyclu.org/en/press-releases/nyclu-sues-nypd-after-it-refuses-disclose-critical-information-about-stingrays.
[30] *See MSP Stingray FOIA*, ACLU, https://www.aclu.org/legal-document/msp-stingray-foia.
[31] All of the disclosed records can be found at *MSP Stingray FOIA – Initial Release*, ACLU, https://www.aclu.org/legal-document/msp-stingray-foia-initial-release and *MSP Stingray FOIA - Second Release*, ACLU, https://www.aclu.org/legal-document/msp-stingray-foia-second-release; *see also* Joel Kurth, *Michigan State Police Using Cell Snooping Devices*, The Detroit News, 22 Oct. 2015, http://www.detroitnews.com/story/news/local/michigan/2015/10/22/stingray/74438668/.
[32] George Joseph, *Cellphone Spy Tools Have Flooded Local Police Departments*, CityLab, 8 Feb. 2017, https://www.citylab.com/equity/2017/02/cellphone-spy-tools-have-flooded-local-police-departments/512543/.
[33] All of the disclosed records can be found at https://www.documentcloud.org/public/search/projectid:%2031525-police-acquisitions-of-cell-phone-surveillance-devices.