

**BEFORE THE INFORMATION COMMISSIONER**

**BETWEEN**

**PRIVACY INTERNATIONAL**

**Applicant**

**- and -**

**NATIONAL POLICE CHIEFS COUNCIL**

**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 National Police Chiefs Council (“NPCC”), Home Office, 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 NPCC is annexed to these grounds as Exhibit A.
4. On 1 December 2016, the NPCC responded to the initial request, by stating that it could neither confirm nor deny (“NCND”) whether it held the information requested by virtue of the exemptions contained in sections 23(5), 24(2), 30(3) and 31(3) Freedom of Information Act (“FOIA”) 2000. This response is annexed to these grounds as Exhibit B.
5. On 30 January 2017 Privacy International made a request for internal review of the decision. This request is annexed to these grounds as Exhibit C.
6. On 27 February 2017 the NPCC upheld its initial decision to NCND the information

sought in the request. However, in its response, the NPCC concluded that “*the s30 exemption, Investigations and Proceedings Conducted by Public Authorities, is not engaged in this case and . . . the neither confirm nor deny arguments around this exemption should therefore be excluded from the response.*” This decision is annexed to these grounds as Exhibit D.

7. The NPCC’s 27 February 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.<sup>1</sup> 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.<sup>2</sup> 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

---

<sup>1</sup> 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.

<sup>2</sup> 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](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp185_en.pdf).

inextricable linkages between anonymity, privacy, and freedom of expression.<sup>3</sup>

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.<sup>4</sup> 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.<sup>5</sup>

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.”*<sup>6</sup>

18. On 10 October 2016, an article appeared in the Bristol Cable entitled: “Revealed: Bristol’s police and mass mobile phone surveillance.”<sup>7</sup> 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 “Covert Communications Data Capture” (“CCDC”) equipment was discussed.

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

---

<sup>3</sup> 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](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.

<sup>4</sup> Section 100i of the *Criminal Procedure Code (Strafprozessordnung, StPO)* (Germany), available at [https://www.gesetze-im-internet.de/englisch\\_stpo/englisch\\_stpo.html](https://www.gesetze-im-internet.de/englisch_stpo/englisch_stpo.html).

<sup>5</sup> 2015 U.S. Department of Justice Policy, available at <https://www.justice.gov/opa/file/767321/download>.

<sup>6</sup> 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>.

<sup>7</sup> 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’<sup>8</sup>. 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.

### C. NPCC

21. The NPCC is a coordination body for law enforcement established in 2015. It replaced the Association of Chief Police Officers (“ACPO”). The NPCC was established by way of a legal agreement pursuant to section 22A of the Police Act 1996 (as amended), which enables chief officers of police and local policing to make an agreement about the discharge of officers and staff where it is in the interests of the efficiency and effectiveness of their own and other police force areas. The NPCC has a number of functions, which are set out in clause 7 of the legal agreement, including:

- a. The coordination of national operations including defining, monitoring and testing force contributions to the Strategic Policing Requirement working with the National Crime Agency where appropriate;
- b. The command of counter terrorism operations and delivery of counter terrorist policing through the national network as set out in the Counter Terrorism Collaboration Agreement;
- c. The co-ordination of the national police response to national emergencies and the co-ordination of the mobilisation of resources across force borders and internationally;
- d. The national operational implementation of standards and policy as set by the College of Policing and Government;
- e. Working with the College of Policing, to develop joint national approaches on criminal justice, value for money, service transformation, information management, performance management and technology.

22. As a coordinating body, the NPCC plays an important role in setting standards in policing and counter-terrorism operations. For this reason, public scrutiny and transparency of the NPCC is important.

---

<sup>8</sup> 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>.

23. Under section 5 FOIA, the Secretary of State can by order designate a body, which is not listed in Schedule 1 and cannot be added to that Schedule by order under section 4, as “*a public authority*” for the purposes of FOIA where it exercises “*functions of a public nature*”. The first order under section 5 in November 2011 designated ACPO (now the NPCC) as a public authority for the purposes of FOIA, in respect of specified functions. The Cabinet Office is responsible for updating Schedule 1 but the Information Commissioner can investigate whether or not a body is a public authority for the purposes of FOIA.<sup>9</sup>
24. The Commissioner therefore clearly has the power to investigate the NPCC either because it is already covered by Schedule 1 or due to its other powers to investigate whether the NPCC is a public authority for the purposes of FOIA.

### **III. Procedural History**

#### **A. Request for Information**

25. On 1 November 2016, Privacy International requested the following information from the NPCC:

*“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**

26. On 1 December 2016, the NPCC Freedom of Information Officer & Decision Maker refused the request on grounds that it could NCND whether it held the information requested. The NPCC’s NCND position relied on sections 23(5), 24(2), 30(3), and 31(3) FOIA.
27. The reasons given for the overall harm identified for NCND can be summarised as follows:
- a. That confirming or denying that the NPCC holds information regarding these techniques would in itself disclose exempt information. Stating information is

---

<sup>9</sup> See Information Commissioner’s Office, Public authorities under the Freedom of Information Act, available at <https://ico.org.uk/media/for-organisations/documents/1152/public-authorities-under-the-foia.pdf>.

held would confirm usage and the opposite if there is no such information;

- b. How and when the techniques might be used are sensitive issues for the police service. These techniques could be deployed for more high profile sensitive operations, albeit not necessarily by the force in our area, therefore the NCND is required to protect forces that may use them;
- c. Any disclosure under FOIA is a disclosure to the world at large, and NCND use of specialist techniques which may or may not exist, and which (should they exist) the police may or may not deploy in specific circumstances would prejudice law enforcement. If the requested information was held by the NPCC, confirmation of this fact would reveal that the police have access to sophisticated communications analysis techniques. This would be damaging as it would:
  - i. Limit operational capabilities as criminals/terrorists would gain a greater understanding of the police's methods and techniques, enabling them to take steps to counter them; and
  - ii. Provide an indication to any individual who may be undertaking criminal/terrorist activities that the police may be aware of their presence and taking counter terrorist measures.
- d. Conversely, if information was not held by the NPCC, and a denial was issued, this would reveal to those same individuals that their activities are unlikely to have been detected by the police. It may also suggest (whether correctly or not) the limitations of police capabilities in this area, which may further encourage criminal/terrorist activity by exposing a potential vulnerability.
- e. Disclosure of the information could confirm to those involved in criminality or terrorism that they are or have been the subject of such activity, allowing them to gauge the frequency of its use and to take measures to circumvent its use. Any compromise of, or reduction in technical capacity by the police would substantially prejudice their ability to police their areas which would lead to a greater risk to the public.
- f. The information could be useful to those committing crimes of drugs and terrorist activity who would be able to 'map' where the use of certain tactics are or are not deployed. This information could enable individuals to become aware of location-specific operations and could lead to them moving their operations, destroying evidence, or avoiding those areas, ultimately compromising police tactics, operations and future prosecutions.
- g. Any information identifying the focus of policing activity could be used to the advantage of terrorists or criminal organisations and information undermining the

operational integrity of these operations will adversely affect public safety and have a negative impact on both national security and law enforcement.

### **C. Request for Internal Review**

28. On 30 January 2017, Privacy International challenged the refusal on five grounds.
29. First, Privacy International submitted that the NPCC response was predicated on a series of *non-sequiturs*:
  - a. It simply does not follow that merely confirming or denying that a police force uses IMSI catchers would reveal operationally sensitive information about the scope of police activities. This reasoning is not understood. It appears that the NPCC has confused consideration of NCND with consideration of the provision of information itself;
  - b. Equally, it does not follow that making similar requests to multiple police forces could identify how individuals could map or be aware of how operationally sensitive information is obtained by the various police forces. Different police forces could obtain information in multiple ways. Confirming or denying that a police force holds the requested information does not automatically reveal how tactics are deployed or what technical operations each force has;
  - c. It is not understood why revealing that a police force has sophisticated capabilities to analyse data would limit operational capabilities. The reasoning set out in this respect is nonsensical.
30. Second, Privacy International submitted that the refusal failed to have regard to obviously material considerations, including, but not limited to:
  - a. The fact that the various police forces have purchased IMSI Catchers is already in the public domain, as set out in Privacy International's original request;
  - b. The fact that the legislative provisions and/or policy guidance requested cannot conceivably fall within any exemption;
  - c. The significant public interest in the topic of IMSI catchers and the regulation of related communications surveillance technologies.
31. Third, Privacy International submitted that when considered forensically, the exemptions relied upon do not apply:
  - a. Under Section 23(5) FOIA, there has to be a realistic possibility that a security body would be involved in the issue the request relates to in order for the



exemption to apply. No such possibility has been set out. Any possibility that is particularised would be too remote to justify the application of this exemption;

- b. Section 24(2) FOIA provides an exemption from the duty to confirm information is held, where the exemption is required for the purposes of safeguarding national security. Section 31(3) FOIA also provides an exemption where it is necessary for the prevention or detection of crime. No real reasons have been set out as to why either exemption applies. By way of example, it cannot seriously be suggested that it would damage national security and/or the prevention or detection of crime to confirm the existence of legislative powers and/or policy guidance;
- c. Section 30(3) FOIA provides that the duty to confirm or deny does not arise in relation to information that is exempt information by virtue of subsection 30(1) or (2). Section 30(1) can only be claimed by public authorities that have a duty to investigate whether someone should be charged with an offence, or the power to conduct such investigations and/or institute criminal proceedings. Section 30(2) protects the identity of confidential sources, primarily to ensure informants are not deterred from supplying law enforcement agencies with valuable intelligence. ICO guidance makes clear that the section 30 exemptions “*exist to ensure the effective investigation and prosecution of offences and the protection of confidential sources. They recognise the need to prevent disclosures that would prejudice either a particular investigation or set of proceedings, or the investigatory and prosecution processes generally, including any prejudice to future investigations and proceedings.*”<sup>10</sup> None of these matters have been addressed in the response to the request. There is no risk of prejudice to a specific investigation, there is no risk to informants, and there is no risk to confidential sources.

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

- a. No meaningful reasons have been provided as to why there is a public interest in neither confirming nor denying the matters requested in this request;
- b. There is currently no evidence at all to suggest that the public interest will be harmed to any material extent by disclosure of the information sought;
- c. The public interest in disclosure is real, it is important that the public are reassured that the measures used to safeguard national security are proportionate and effective;

---

<sup>10</sup> See Information Commissioner’s Office, Investigations and proceedings (section 30), Freedom of Information Act, §53, available at <https://ico.org.uk/media/for-organisations/documents/1205/investigations-and-proceedings-foi-section-30.pdf>.

- d. The refusal recognizes that “*The objectives of the FOIA are openness, transparency and accountability*” and that “*Greater transparency would better inform public debate on executive action for the collective good which may impact on individual liberties. The fact some relevant information is already in the public domain adds weight to the public interest in confirming or denying in this case.*” Despite these factors, the refusal finds that the “*evidence of harm above suggests strongly in favour of maintaining the exemptions.*” However, as previously stated, no evidence of harm was in fact provided.

33. 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”;<sup>11</sup>
- 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.<sup>12</sup> It also flies in the face of the Article 10 right to receive information, as recently confirmed by the European Court of Human Rights;<sup>13</sup>
- 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*”.<sup>14</sup>

#### **D. Decision in Response to Request for Internal Review**

34. On 27 February 2017, the NPCC responded by upholding its original decision. As a general matter, the NPCC submitted that “*adopting anything other than a neither confirm nor deny approach would potentially reveal exempt information*” and that the Police Service has adopted “*a neither confirm nor deny stance for the vast majority of forces.*”

---

<sup>11</sup> *Philip Kalman v Information Commissioner and the Department of Transport* (EA/2009/111 6 July 2010).

<sup>12</sup> *Galloway v Information Commissioner v The Central and North West London NHS Foundation Trust* (EA/2008/0036 20 March 2009).

<sup>13</sup> *Magyar Helsinki Bizottság v Hungary*, European Court of Human Rights, App. No. 18030/11, 8 November 2016.

<sup>14</sup> *Mohamed and another v Secretary of State for the Home Department* [2014] 1 WLR 4240, per Maurice Kay LJ, at §40.

The NPCC further submitted that confirming or denying the existence of the requested information “*would indicate one way or another whether the Police Service has access to and uses a specific tactical option*” and “*would clearly infer whether or not the tactical option . . . is in use across the service.*”

35. The NPCC held that the section 30 FOIA exemption “*is not engaged in this case*” and therefore excluded NCND arguments pursuant to this exemption from its response. However, it upheld the NCND arguments in the original decision as they related to sections 24(2) and 31(3) FOIA. The NPCC submitted that both exemptions were engaged as “*the request relates to covert technology which would, if held, be used to combat serious crime*”, which could include national security matters. It then proceeded to summarise the main arguments from the original decision.
36. In terms of the engagement of section 23(5) FOIA with respect to the NCND position, the NCND submitted that this exemption “*can be very broadly interpreted, especially in relation to the phrase ‘relates to’ and can cover information that has only loosely touched section 23 bodies.*” It concluded that “[g]iven the type of covert equipment under discussion, it is perfectly reasonable to assume that if information were held, there is the potential for s23 involvement”.

#### **IV. The Appeal**

##### **A. The Purpose of FOIA**

37. 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.
38. 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.<sup>15</sup>

---

<sup>15</sup> 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.

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

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

*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’.”*

40. 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.
41. 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**

42. 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).

43. 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.*”<sup>16</sup>

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

- a. The request relates to *legislation and/or policy guidance* governing the use of IMSI Catchers held by the NPCC 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 provisions and/or policy guidance, 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 NPCC;
- b. The request further relates to legislation and policy guidance governing the use of IMSI Catchers *by police forces*. Just because IMSI Catchers may also be used by

---

<sup>16</sup> 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-notice/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-notice/2017/2014349/fs50660527.pdf>.

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 the NPCC’s 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 NPCC 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 bodies.

## **B. Section 24(2) FOIA**

45. 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.
46. 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.*”<sup>17</sup>
47. 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.*”<sup>18</sup>
48. 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

---

<sup>17</sup> ICO, Decision Notice, Ref. FS50665716, 13 June 2017, para. 26; *see also* ICO Decision Notice, Ref. FS50660527, 8 June 2017, para 27.

<sup>18</sup> 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](https://ico.org.uk/media/action-weve-taken/decision-notices/2016/1624502/fs_50622468.pdf).

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.<sup>19</sup>

### **i. Safeguarding National Security**

49. 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.*”<sup>20</sup>
50. As discussed above, in relation to the section 23(5) exemption, the request relates to legislation and policy guidance governing the use of IMSI Catchers by police forces. Legislative provisions and/or policy guidance, 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 NPCC 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.
51. The NPCC also bases its arguments around national security on skeletal assertions that national security would be impacted by (1) at a general level, confirming or denying the use of “*specialist techniques*” and (2) at a specific level, indicating that a technique is used in one area but not in another area. Both arguments are baseless. First, the NPCC does not define a “specialist technique” and why IMSI Catchers constitute a specialist technique. Second, it simply does not follow that merely confirming or denying that a police force uses IMSI Catchers reveals operationally sensitive information that would negatively impact national security. In fact, the government has willingly admitted and subjected to either public regulation or FOIA requests the use of a variety of what might also be considered “specialist techniques” – from hacking<sup>21</sup> to the use of equipment to physically extract mobile phone data.<sup>22</sup> There is therefore no reason that the information related to the use of IMSI Catchers by police forces should be afforded special protection. Second, it does not follow that determining which police forces use this equipment could permit individuals to map or be aware of how operationally sensitive information is

---

<sup>19</sup> ICO, Decision Notice, Ref. FS50665716, 13 June 2017, paras. 29-30; *see also* ICO Decision Notice, Ref. FS50660527, 8 June 2017, paras. 30-31.

<sup>20</sup> ICO, Decision Notice, Ref. FS50665716, 13 June 2017, para. 27; *see also* ICO Decision Notice, Ref. FS50660527, 8 June 2017, para. 29.

<sup>21</sup> *See* Part 5, Investigatory Powers Act; *see also* Equipment Interference: Draft Code of Practice.

<sup>22</sup> *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](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).

obtained, thereby negatively impacting national security. Different police forces will obtain information in many different ways.

## ii. Public Interest Test

52. The original decision identified as the factor against confirming or denying the existence of the requested information that the “*use of specialist techniques could render security measures less effective*”. The ICO should not accept such a bare assertion. The NPCC has not clarified what constitutes a “specialist technique” or why confirming or denying the mere existence of such techniques in general or IMSI Catchers specifically could render security measures less effective. Furthermore, it has presented no evidence of risk to support this position.
53. The original decision only identified as a factor in favour of confirming or denying the existence of the requested information that “[t]he public is entitled to know where its public funds are spent and a better informed public can take steps to protect themselves”. The NPCC failed to consider that there is public interest in citizens being informed about methods of surveillance that could have a profound impact on their fundamental rights, including the rights to privacy, freedom of expression and freedom of assembly and association. In particular, there is significant public interest in the topic of IMSI catchers and the regulation of related communication surveillance technologies. Indeed, because IMSI Catchers can indiscriminately collect data (by tricking all mobile phones within a given range to identify themselves and reveal their location), their use can interfere with the rights of many persons, including those who are not the intended targets of surveillance.
54. 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.
55. 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*”.<sup>23</sup> As discussed

---

<sup>23</sup> *Magyar Helsinki Bizottság v Hungary*, European Court of Human Rights, App. No. 18030/11, 8 Nov. 2016, para. 162.



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.

56. 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.<sup>24</sup> 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.

57. As set out previously to the NPCC 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 NPCC 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.

---

<sup>24</sup> *Youth Initiative for Human Rights v Serbia*, European Court of Human Rights, App. No. 48135/06, 25 June 2013.

### C. Section 31(3) FOIA

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

59. 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.”<sup>25</sup>*

#### i. Public Interest Test

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

61. As with its arguments around the section 24(2) FOIA exemption, the NPCC also bases its arguments around the 30(3) exemption on skeletal assertions that matters related to law

---

<sup>25</sup> 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>.

enforcement would be prejudiced by (1) at a general level, confirming or denying the use of “specialist techniques” and (2) at a specific level, indicating that a technique is used in one area but not in another area. For the reasons discussed above, these arguments are baseless and therefore fail to demonstrate a causal link between confirming or denying the existence of the requested information and the prejudice claimed. Furthermore, these arguments fail to demonstrate how the prejudice claimed is real, actual or of substance, let alone the likelihood that the claimed prejudice will be met.

## **ii. Public Interest Test**

62. The original decision identified as the factor against confirming or denying the existence of the requested information that it “*would compromise law enforcement tactics and undermine the partnership approach which would hinder the prevention or detection of crime*”. As with the factor identified against confirming or denying the existence of the requested information under section 24(2), the ICO should not accept such bare assertions. The NPCC has not clarified why confirming or denying the mere existence of IMSI Catchers could render law enforcement less effective. It has also failed to explain what it means by “the partnership approach” or how such an “approach” would be impaired by disclosing the existence of the information sought in the request. Furthermore, it has presented no evidence of risk to support these positions.
63. The original decision identified as factors in favour of confirming or denying the existence of the requested information that “[*b*]etter awareness may reduce crime or lead to more information from the public, and the public would be able to take steps to protect themselves” and that “[*s*]ome information is already in the public domain.” As discussed above, the NPCC has failed to consider that there is public interest in citizens being informed about methods of surveillance that could have a profound impact on their fundamental rights, including the rights to privacy, freedom of expression and freedom of assembly and association.
64. 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.
65. Thus, as set out previously to the NPCC 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 NPCC 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**

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

Freedom of Information Officer  
National Police Chiefs Council (NPCC)  
1<sup>st</sup> Floor  
10 Victoria Street  
London SW1H 0NN

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".<sup>1</sup> 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.<sup>2</sup>

Specifically, the minutes record: "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'".<sup>3</sup> 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

---

<sup>1</sup> <https://thebristolcable.org/2016/10/imsi/>

<sup>2</sup> <https://thebristolcable.org/wp-content/uploads/2016/10/09-imsi-4.pdf>

<sup>3</sup> [https://www.theguardian.com/world/2016/oct/10/controversial-phone-snooping-technology-imsi-catcher-seven-police-forces?CMP=tw\\_t\\_gu](https://www.theguardian.com/world/2016/oct/10/controversial-phone-snooping-technology-imsi-catcher-seven-police-forces?CMP=tw_t_gu)

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 NPCC functions to develop joint national approaches on criminal justice, value for money, service transformation, information management, performance management and **technology**, 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](mailto: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



c/o PO BOX 481  
Fareham  
Hampshire  
PO14 9FS

Tel: 02380 478922

Email: [npcc.foi.request@cru.pnn.police.uk](mailto:npcc.foi.request@cru.pnn.police.uk)

01/12/2016

Dear Mr Rice

**FREEDOM OF INFORMATION REQUEST REFERENCE NUMBER: 000268/16**

Thank you for your request for information regarding CCDC technology which has now been considered.

**Applicant Question:**

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".<sup>1</sup> 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 record: "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'".<sup>3</sup> 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

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>

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 NPCC functions to develop joint national approaches on criminal justice, value for money, service transformation, information management, performance management and technology, 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".

### **NPCC Response:**

Section 17 of the Freedom of Information Act 2000 requires the NPCC, when refusing to provide information by way of exemption, to provide you with a notice which (a) states the fact, (b) specifies the exemption in question and (c) states why the exemption applies. In accordance with the Freedom of Information Act 2000 this letter acts as a refusal notice for those aspects of your request.

The NPCC can neither confirm nor deny whether we hold any information you have requested by virtue of the following exemptions:

Section 23(5) – Information supplied by, or concerning, certain security bodies  
Section 24(2) – National security  
Section 30(3) – Investigations and proceedings conducted by public authorities  
Section 31(3) – Law enforcement

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

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

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

The overall harm for the NCND is as follows:

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

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

Any disclosure under FOIA is a disclosure to the world at large, and confirming or denying the use of specialist techniques which may or may not exist, and which (should they exist) the police service may or may not deploy in specific circumstances would prejudice law enforcement. If the requested information were held by the NPCC, confirmation of this fact would reveal that the police has access to sophisticated communications analysis techniques. This would be damaging as it would (i) limit operational capabilities as criminals/terrorists would gain a greater understanding of the police's methods and techniques, enabling them to take steps to counter them; and (ii) provide an indication to any individual who may be undertaking criminal/terrorist activities that the police service may be aware of their presence and taking counter terrorist measures.

Conversely, if information were not held by the NPCC, and a denial were issued, this would reveal to those same individuals that their activities are unlikely to have been detected by the police. It may also suggest (whether correctly or not) the limitations of police capabilities in this area, which may further encourage criminal/terrorist activity by exposing a potential vulnerability. Disclosure of the information could confirm to those involved in criminality or terrorism that they are or have been the subject of such activity, allowing them to gauge the frequency of its use and to take measures to circumvent its use. Any compromise of, or reduction in technical capability by forces would substantially prejudice the ability of forces to police their areas which would lead to a greater risk to the public.

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

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

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

Factors favouring confirming or denying whether any other information is held for Section 24

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

Factors against confirming or denying whether any other information is held for Section 24

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

Factors favouring confirming or denying whether any other information is held for Section 30

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

Factors against confirming or denying whether any other information is held for Section 30

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

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

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

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

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

Balance test

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

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

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

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

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

Yours sincerely

Sherry Traquair  
Freedom of Information Officer & Decision Maker

[www.npcc.police.uk](http://www.npcc.police.uk)

## COMPLAINT RIGHTS

### Internal Review

If you are dissatisfied with the response you have been provided with, in compliance with the Freedom of Information legislation, you can lodge a complaint with NPCC to have the decision reviewed within 20 working days of the date of this response. The handling of your request will be looked at by someone independent of the original decision, and a fresh response provided.

It would be helpful, if requesting a review, for you to articulate in detail the reasons you are not satisfied with this reply.

If you would like to request a review, please write or send an email to NPCC Freedom of Information, c/o PO Box 481, Fareham, Hampshire, PO14 9FS.

If, after lodging a complaint with NPCC, you are still unhappy with the outcome, you may make an application to the Information Commissioner at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

# EXHIBIT C

NPCC Freedom of Information  
c/o PO Box 481  
Fareham  
Hampshire  
PO14 9FS

30 January 2017

Re: Freedom of Information Request Reference No. 000268/16

**A. Introduction**

1. This is an appeal following a refusal to disclose information made by the NPCC on 1 December 2016. Privacy International respectfully requests an internal review of the decision. Following correspondence NPCC extended time for the appeal until 31 January 2017.
2. Privacy International is a UK registered charity. The organisation's mission is to defend the right to privacy and to fight unlawful surveillance and other intrusions into private life, with a focus on the technologies that enable these practices. In seeking the information requested, Privacy International seeks to bring greater accountability and transparency to surveillance practices.

**B. Background**

3. On 1 November 2016, Privacy International wrote to the Freedom of Information Officer seeking records, pursuant to the Freedom of Information Act 2000, relating to the purchase and use of mobile phone surveillance equipment by 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 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.”*

**C. The Refusal**

7. On 1 December 2016, the Freedom of Information Officer & Decision Maker refused the request. The refusal relied on ss.23(5), 24(2), 30(3), and 31(3) Freedom of Information Act 2000. The reasons given for the overall harm identified can be summarised as follows:

- 7.1 That confirming or denying that the NPCC holds information regarding these techniques would in itself disclose exempt information. Stating information is held would confirm usage and the opposite if there is no such information;
- 7.2 How and when the techniques might be used, are sensitive issues for the police service. These techniques could be deployed for more high profile sensitive operations, albeit not necessarily in the force in our area, therefore the NCND is required to protect forces that may use them;
- 7.3 Any disclosure under the Freedom of Information Act 2000 is a disclosure to the world at large, and NCND use of specialist techniques which may or may not exist, and which (should they exist) the police may or may not deploy in specific circumstances would prejudice law enforcement. If the requested information was held by the NPCC, confirmation of this fact would reveal that the police have access to sophisticated communications analysis techniques. This would be damaging as it would:
- 7.3.1 Limit operational capabilities as criminals/terrorists would gain a greater understanding of the police’s methods and techniques, enabling them to take steps to counter them; and
- 7.3.2 Provide an indication to any individual who may be undertaking criminal/terrorist activities that the police may be aware of their presence and taking counter terrorist measures.
- 7.4 Conversely, if information was not held by the NPCC, and a denial was issued, this would reveal to those same individuals that their activities are unlikely to

have been detected by the police. It may also suggest (whether correctly or not) the limitations of the police's capabilities in this area, which may further encourage criminal/terrorist activity by exposing a potential vulnerability.

7.5 Disclosure of the information could confirm to those involved in criminality or terrorism that they are or have been the subject of such activity, allowing them to gauge the frequency of its use and to take measures to circumvent its use. Any compromise of, or reduction in technical capacity by the police would substantially prejudice the ability of their ability to police their area which would lead to a greater risk of the public.

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

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

#### **D. The Appeal**

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

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

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

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

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

10. Secondly, it fails to have regard to obviously material considerations, including, but not limited to:
  - 10.1 The fact that the various police forces have purchased IMSI catchers is already in the public domain, as set out in Privacy International's original request;
  - 10.2 The fact that the legislative provisions and/or policy guidance requested cannot conceivably fall within any exemption;
  - 10.3 The significant public interest in the topic of IMSI catchers and the regulation of related communications surveillance technologies.
11. Thirdly, when considered forensically, the exemptions relied upon do not apply.
  - 11.1 Under Section 23(5), there has to be a realistic possibility that a security body would be involved in the issue the request relates to in order for the exemption to apply. No such possibility has been set out. Any possibility that is particularised would be too remote to justify the application of this exemption;
  - 11.2 Section 24(2) provides an exemption from the duty to confirm information is held, where the exemption is required for the purposes of safeguarding national security. Section 31(3) also provides an exemption where it is necessary for the prevention or detection of crime. No real reasons have been set out as to why either exemption applies. By way of example, it cannot seriously be suggested that it would damage national security and/or the prevention or detection of crime to confirm the existence of legislative powers and/or policy guidance;
  - 11.3 Section 30(3) provides that the duty to confirm or deny does not arise in relation to information which is exempt information by virtue of subsection 30(1) or (2). Section 30(1) can only be claimed by public authorities that have a duty to investigate whether someone should be charged with an offence, or the power to conduct such investigations and/or institute criminal proceedings. Section 30(2) protects the identity of confidential sources, primarily to ensure informants are not deterred from supplying law enforcement agencies with valuable intelligence. The ICO Guidance makes it clear at §53 that the s.30 exemptions "*exist to ensure the effective investigation and prosecution of offences and the protection of confidential sources. They recognise the need to prevent disclosures that would prejudice either a particular investigation or set of proceedings, or the investigatory and prosecution processes generally, including any prejudice to future investigations and proceedings.*"<sup>1</sup> None of these matters have been addressed in the response to the request. There is no risk of prejudice to a

---

<sup>1</sup> <https://ico.org.uk/media/for-organisations/documents/1205/investigations-and-proceedings-foi-section-30.pdf>

specific investigation, there is no risk to informants, and there is no risk to confidential sources.

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

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

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

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

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

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

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

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

---

<sup>2</sup> *Philip Kalman v Information Commissioner and the Department of Transport* (EA/2009/111 8 July 2010).

<sup>3</sup> *Galloway v Information Commissioner v The Central and North West London NHS Foundation Trust* (2009) 108 BMLR 50, at §70.

<sup>4</sup> *Magyar Helsinki Bizottság v Hungary* (App. no. 18030/11).

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

13.4 The refusal recognizes that “*The objectives of the FOIA are openness, transparency and accountability*” and that “*Greater transparency would better inform public debate on executive action for the collective good which may impact on individual liberties. The fact some relevant information is already in the public domain adds weight to the public interest in confirming or denying in this case.*” Despite these factors, the refusal finds that the “*evidence of harm above suggests strongly in favour of maintaining the exemptions.*” However, as previously stated, no evidence of harm was in fact provided.

**E. The Appeal**

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

Scarlet Kim  
Legal Officer  
Privacy International

cc: Matthew Rice  
Advocacy Officer  
Privacy International

# EXHIBIT D

c/o PO BOX 481  
Fareham  
Hampshire  
PO14 9FS

Tel: 02380 478922  
Email: [npcc.foi.request@cru.pnn.police.uk](mailto:npcc.foi.request@cru.pnn.police.uk)

27/02/2017

Dear Mr Rice

**FREEDOM OF INFORMATION ORIGINAL REFERENCE NUMBER: 0268/16**  
**FREEDOM OF INFORMATION REQUEST INTERNAL REVIEW: 0023/17**

Please find below the response to your request for internal review which was submitted to the NPCC. For clarity, your original request number was 268/16.

**Original Question:**

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".

**Grounds for Appeal**

I have summarised your grounds for appeal, taken from your letter dated 30<sup>th</sup> January 2017, below:

- 9.1 Privacy International argues that the NPCC has confused considerations of 'neither confirm nor deny' with consideration of the provision of information itself.
- 9.2 Privacy International argues that making similar requests to different forces does not reveal how and which technical options may be deployed.
- 9.3 Privacy International argues that revealing police forces have sophisticated capabilities to analyse data would not limit operational capabilities.
- 10.1 Privacy International argues that some information is in the public domain.
- 10.2 Privacy International argues that the legislation means that policy and guidance cannot fall within any exemption.



- 10.3 Privacy International argues that there is a significant public interest in disclosure.
11. Privacy International argues that that 23(5), 24(2) and 30(3) are not engaged.
- 12.1 Privacy International argues that s24 is not engaged.
- 12.2 Privacy International argues that NCND merits close scrutiny because it contradicts the default setting in FOIA.
- 12.3 Privacy International argues that the decision to NCND requires justification similar to the position in relation to public interest immunity.
13. Privacy International argues that the public interest falls in favour of disclosure because no meaningful reasons provided why PIT upholds NCND, no evidence that public interest will be harmed by disclosure and arguments around public reassurance were not considered.

#### **NPCC Internal Review Response**

The first point to stress is that this Internal Review will deal only with considerations around the original neither confirm nor deny position articulated by the NPCC in its response dated 1<sup>st</sup> December 2016.

Please also note those grounds in your appeal letter that relate force-specific arguments will not be considered.

#### **Point 9.1**

The first point I would make in respect of 9.1 is that there is a clear difference in the Act between the provisions in s1(1)(a) – confirming or denying that information is held – and s(1)(1)(b) – providing a copy of the information. Most exemptions have a sub-section with the provision to neither confirm nor deny whether information is held if by confirming or denying exempt information would be revealed.

In this case, I would like to reassure you that the NPCC has a full understanding of the requirements under s1(1)(a) and s1(1)(b) of the Act and that there has been no confusion around the consideration of the NCND position with consideration of the provision of information itself. The NPCC is of the view that adopting anything other than a neither confirm nor deny approach in this case would potentially reveal exempt information. With this in mind, where there is prejudice or harm in confirming or denying information is held, there is no obligation on the part of the public authority to comply with s1(1)(a) of the Freedom of Information Act.

#### **Points 9.2 and 9.3**

Points 9.2 and 9.3 appear to relate to force-specific arguments and are therefore not considered in this Internal Review.

#### **Point 10.1**

Point 10.1 refers to the Privacy International argument that some information is in the public domain. Currently, with the exception of an erroneous disclosure, the Police Service has adopted a neither confirm nor deny stance for the vast majority of forces and the NPCC argues that this approach has not been undermined. For the NPCC to confirm or deny, therefore, whether any information is held relevant to your request would undermine the clear stance that has been adopted by forces and would also reveal exempt information into the public domain.



**Point 10.2**

In respect of point 10.2, the Privacy International argument focusses on the potential application of exemptions. However, the debate on which this Internal Review centres is around whether or not there is any harm in confirming or denying information is held ie. whether it is appropriate to comply with s1(1)(a). Confirming or denying that information is held in this case would indicate one way or another whether the Police Service has access to and uses a specific tactical option – if the NPCC were to confirm or deny that information were held, it would clearly infer whether or not the tactical option which is the focus of this request is in use across the service and likewise, a denial would indicate the opposite. The Police Service does not routinely create policies, guides, manuals, memoranda, presentations or training records for methods it does not use and as such, confirmation or denial by the NPCC would indicate one way or another whether this specific piece of equipment were in use by the Police Service.

As previously stated, where there is any harm in confirming or denying, an NCND position may be adopted within the parameters of the legislation.

**Point 10.3**

Point 10.3 relates to public interest arguments. Again, I must emphasise that the focus of this Internal Review is around the neither confirm nor deny position. As such, those qualified exemptions cited in respect of the NPCC response – s24, s30 and s31 - are all subject to public interest considerations around arguments but only on whether the NCND stance should be upheld.

Having considered the arguments, I can confirm that it is my belief that the s30 exemption, Investigations and Proceedings Conducted by Public Authorities, is not engaged in this case and that the neither confirm nor deny arguments around this exemption should therefore be excluded from the response. As such, I have overturned the original position adopted by the NPCC in respect of this exemption and removed it from consideration.

**Points 11 and 12.1**

Nevertheless, I fully support the remaining arguments around neither confirming nor denying in respect of s31 and s24. Point 11 and 12.1 relate to arguments as to whether or not these exemptions are engaged. As previously articulated, the original decision to apply s30 has been overturned. However, I uphold the application of the NCND elements of both the s24 and s31 exemptions.

Both exemptions are engaged as the request relates to covert technology which would, if held, be used to combat serious crime. This could include national security matters if information were held, hence the engagement of the NCND element of s24. Specialist capabilities, whatever they are, are deployed in crimes that warrant the cost and resources to deploy them. National security would undoubtedly be one of those reasons and confirmation or denial would affect the behaviour of any individuals monitored by the police and could have catastrophic consequences.

I have summarised the main arguments from your original response 268/16 in italics below and would re-iterate that I fully agree with the position adopted herein:

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

*Any disclosure under FOIA is a disclosure to the world at large, and confirming or denying the use of specialist techniques which may or may not exist, and which (should they exist) the Police Service may or may not deploy in specific circumstances would prejudice law enforcement. If the requested information were held by the NPCC, confirmation of this fact would reveal that the police has access to sophisticated communications analysis techniques. This would be damaging as it would (i) limit operational capabilities as criminals/terrorists would gain a greater understanding of the police's methods and techniques, enabling them to take steps to counter them; and (ii) provide an indication to any individual who may be undertaking criminal/terrorist activities that the Police Service may be aware of their presence and taking counter terrorist measures.*

*Conversely, if information were not held by the NPCC and a denial were issued, this would reveal to those same individuals that their activities are unlikely to have been detected by the police. It may also suggest (whether correctly or not) the limitations of police capabilities in this area, which may further encourage criminal/terrorist activity by exposing a potential vulnerability. Disclosure of the information could confirm to those involved in criminality or terrorism that they are or have been the subject of such activity, allowing them to gauge the frequency of its use and to take measures to circumvent its use. Any compromise of, or reduction in technical capability by forces would substantially prejudice the ability of forces to police their areas which would lead to a greater risk to the public.*

*This detrimental effect is increased if the request is made to several different law enforcement bodies. In addition to the local criminal fraternity now being better informed, those intent on organised crime throughout the UK will be able to make more informed decisions around whether certain tactics may or may not be deployed.*

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

	<b>Favouring upholding the NCND</b>	<b>Favouring confirmation or denial</b>
<b>S24</b>	<i>By confirming or denying the use of specialist techniques could render security measures less effective. This could lead to the compromise of ongoing or future operations to protect the security or infra-structure of the UK and increase the risk of harm to the public.</i>	<i>The public is entitled to know where its public funds are being spent and a better informed public can take steps to protect themselves.</i>
<b>S31</b>	<i>By confirming or denying whether such techniques were used would compromise law enforcement tactics and undermine the partnership approach which would hinder the prevention or detection of crime. This would impact on police resources, more crime would then be committed and individuals placed at risk.</i>	<i>Better awareness may reduce crime or lead to more information from the public, and the public would be able to take steps to protect themselves. Some information is already in the public domain.</i>

**Balance test**

*The security of the country is of paramount importance and the Police Service will not divulge whether information is or is not held if to do so could undermine national security or compromise law enforcement. Whilst there is a public interest in the transparency of policing operations and in*

*this case providing assurance that the Police Service is appropriately and effectively engaging with the threat posed by the criminal fraternity, there is a very strong public interest in safeguarding both national security and the integrity of police investigations and operations in this area.*

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

*There is also no requirement to satisfy any public concern over the legality of police operations and the tactics we may or may not use. Forces are already held to account by statute, for example the Police and Criminal Evidence Act and the Regulation of Investigatory Powers Act and independent bodies such as Her Majesty's Inspectorate of Constabulary, the Independent Police Complaints Commission and the Office of the Surveillance Commissioner. Accountability of the Police Service is therefore not enhanced by confirming or denying whether any information is held.*

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

In terms of the application of s23(5), this exemption is absolute – there is no requirement to either evidence harm or consider the PIT. This is also an exemption which when used in a substantive way can be very broadly interpreted, especially in relation to the phrase ‘relates to’ and can cover information that has only loosely touched section 23 bodies. Given the type of covert equipment under discussion, it is perfectly reasonable to assume that if information were held, there is the potential for s23 involvement.

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

#### **Point 12.2**

In terms of point 12.2, you are correct that the default setting in respect of FOI is to disclose information. However, this is always subject to first considering whether there is any harm in confirming or denying that any information is held. As previously emphasised, in this case, the NPCC is not considering disclosure *per se* but is focussing instead, quite permissibly within the Act, on whether or not there is any harm in confirming or denying that information is held.

The fact that the majority of exemptions have provision to neither confirm nor deny by virtue of a specific sub-section evidences clearly that legislators foresaw the need for this option and included it in the Act to ensure that public authorities would not be compromised where confirming or denying information were held might be prejudicial. Further explanation of this may be located within the ICO's guidance at the link below:

[https://ico.org.uk/media/for-organisations/documents/1166/when\\_to\\_refuse\\_to\\_confirm\\_or\\_deny\\_section\\_1\\_foia.pdf](https://ico.org.uk/media/for-organisations/documents/1166/when_to_refuse_to_confirm_or_deny_section_1_foia.pdf)

In respect of 12.3, public interest tests have been included, as required, in respect of upholding the neither confirm nor deny position. This meets the requirements under the legislation and adheres to ICO guidance on this subject. Further argument around whether or not NCND requires justification to the same level and degree as the public interest immunity fall outside of the scope of this Internal Review – the NPCC is in full compliance with the requirements laid down by the legislation and the ICO.

Point 13 refers again to public interest arguments around disclosure. In this case, your appeal can only centre on whether or not the NCND is appropriate and should or should not be upheld in this respect. Significant and detailed arguments have already been considered and presented in respect of why the NCND PIT upholds the original position. Further arguments around harm in disclosure unfortunately do not form part of the consideration in respect of this Internal Review. My only final comment is that the public interest is not considered to be what might interest the public but focusses instead in wider arguments around community benefit and other more generic considerations which are outlined in the ICO's guidance which may be located at the link below:

[https://ico.org.uk/media/for-organisations/documents/1183/the\\_public\\_interest\\_test.pdf](https://ico.org.uk/media/for-organisations/documents/1183/the_public_interest_test.pdf)

### **Further Information**

To address more generically some of the concerns you have raised about the application of the NCND principle in response to queries that are predicated upon directly or indirectly confirming or denying the use of a potential policing tactic and/or policing capabilities, I have provided links below to ICO Decision Notices on this subject:

ICO Decision Notice FS50622468:

[https://ico.org.uk/media/action-weve-taken/decision-notices/2016/1624502/fs\\_50622468.pdf](https://ico.org.uk/media/action-weve-taken/decision-notices/2016/1624502/fs_50622468.pdf)

ICO Decision Notice FS50459944:

[https://ico.org.uk/media/action-weve-taken/decision-notices/2013/825162/fs\\_50459944.pdf](https://ico.org.uk/media/action-weve-taken/decision-notices/2013/825162/fs_50459944.pdf)

ICO Decision Notice FS50263467:

[https://ico.org.uk/media/action-weve-taken/decision-notices/2011/579404/fs\\_50263467.pdf](https://ico.org.uk/media/action-weve-taken/decision-notices/2011/579404/fs_50263467.pdf)

ICO Decision Notice FS50570727:

[https://ico.org.uk/media/action-weve-taken/decision-notices/2015/1431777/fs\\_50570727.pdf](https://ico.org.uk/media/action-weve-taken/decision-notices/2015/1431777/fs_50570727.pdf)

### **Conclusion**

Overall, I have agreed with you that s30, Investigations and Proceedings Conducted by a Public Authority is not engaged in this case and have therefore overturned its application.

However, in respect of the other elements you have raised and which have been dealt with in detail in this response, I can confirm that I do not intend to overturn the original decision made by the NPCC Freedom of Information Officer and Decision-Maker. It is my decision that, with the exception of s30, the original decision be upheld.

If, after lodging a complaint with NPCC, you are still unhappy with the outcome, you may make an application to the Information Commissioner at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

Yours sincerely

**Rebecca Warhurst**  
**Deputy Manager**  
**National Police Freedom of Information & Data Protection Unit**  
**National Police Chiefs' Council**

[www.npcc.police.uk](http://www.npcc.police.uk)

# 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.<sup>1</sup> 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.”<sup>2</sup> 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.”<sup>3</sup> 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.<sup>4</sup>

---

<sup>1</sup> 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.

<sup>2</sup> NLRB v. Robbins Tire & Rubber Co., 437 U.S. 214, 242 (1978).

<sup>3</sup> 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)).

<sup>4</sup> 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.<sup>5</sup> The exemptions are:<sup>6</sup>

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<sup>7</sup>
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].”<sup>8</sup> 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)

---

<sup>5</sup> See 5 U.S.C. §552(b), (d); *see also* Chrysler Corp. v. Brown, 441 U.S. 281, 293 (1979).

<sup>6</sup> 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/>.

<sup>7</sup> 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.

<sup>8</sup> 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).<sup>9</sup> 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).<sup>10</sup>

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.<sup>11</sup> 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.<sup>12</sup> 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.<sup>13</sup> 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.*"<sup>14</sup> 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

---

<sup>9</sup> 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>.

<sup>10</sup> *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>.

<sup>11</sup> 5 U.S.C. § 552 (a)(3)(A).

<sup>12</sup> 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).

<sup>13</sup> 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>.

<sup>14</sup> 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”).<sup>15</sup> 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.<sup>16</sup> 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.<sup>17</sup> They further reveal that the FBI has been using IMSI Catchers since at least the mid-1990s,<sup>18</sup> 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.<sup>19</sup>

#### 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

---

<sup>15</sup> ACLU, *Stingray Tracking Devices: Who's Got Them?*, <https://www.aclu.org/issues/privacy-technology/surveillance-technologies/stingray-tracking-devices-whos-got-them>.

<sup>16</sup> *EPIC v. FBI – Stingray / Cell Site Simulator*, EPIC, <https://epic.org/foia/fbi/stingray/>.

<sup>17</sup> 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](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/>.

<sup>18</sup> Ryan Gallagher, *FBI Files / 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](http://www.slate.com/blogs/future_tense/2013/02/15/stingray_imsi_catcher_fbi_files_unlock_history_behind_cellphone_tracking.html).

<sup>19</sup> 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](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.<sup>20</sup> 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.<sup>21</sup>

### 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.<sup>22</sup> The request was sent to the FBI, DEA, ICE and the U.S. Marshals Service. The disclosed records include:<sup>23</sup>

- 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.<sup>24</sup>

## 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

---

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

<sup>21</sup> 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>.

<sup>22</sup> 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>.

<sup>23</sup> 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>.

<sup>24</sup> 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.<sup>25</sup> The records disclosed include:<sup>26</sup>

##### *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

---

<sup>25</sup> 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>.

<sup>26</sup> 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.<sup>27</sup>

## 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.<sup>28</sup>

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

---

<sup>27</sup> 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>.

<sup>28</sup> 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 times 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.<sup>29</sup>

### 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.<sup>30</sup> The MSP released records in two batches; those records include:<sup>31</sup>

- 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.<sup>32</sup> 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.<sup>33</sup>

6 February 2018

Privacy International

---

<sup>29</sup> *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>.

<sup>30</sup> *See MSP Stingray FOIA*, ACLU, <https://www.aclu.org/legal-document/msp-stingray-foia>.

<sup>31</sup> 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/>.

<sup>32</sup> 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/>.

<sup>33</sup> All of the disclosed records can be found at <https://www.documentcloud.org/public/search/projectid:%2031525-police-acquisitions-of-cell-phone-surveillance-devices>.