BEFORE THE INFORMATION COMMISSIONER

BETWEEN

PRIVACY INTERNATIONAL

Applicant

- and -

STAFFORDSHIRE POLICE AND CRIME COMMISSIONER

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

3. On 15 December 2017, Privacy International submitted grounds of appeal to the Commissioner, following the Staffordshire PCC's failure to respond to the initial request for information. Those grounds are annexed to these grounds as Exhibit B.

4. On 8 January 2018, the Commissioner issued a decision notice finding that the Staffordshire PCC had breached sections 1(1) and 10(1) of the Freedom of Information Act ("FOIA") 2000 by failing "*to provide a valid response to the request within 20 working days*." The Commissioner further directed the Staffordshire PCC "*to comply with the request or to issue a valid refusal notice as set out in section 17*" within 35 calendar days of the decision notice. This decision notice is annexed to these grounds as Exhibit C.

5. On 9 February 2018, the Staffordshire PCC responded to the request by stating that it could neither confirm nor deny ("NCND") whether it held the information requested pursuant to sections 23(5), 24(2) and 31(3) FOIA. This response is annexed to these grounds as Exhibit D.

6. On 12 February 2018, the Senior Case Officer of the Information Commissioner's Office ("ICO") indicated that the Commissioner would accept a complaint against the Staffordshire PCC's decision without a further internal review, given the length of time between the initial request for information and the decision by Staffordshire PCC. This correspondence is annexed to these grounds as Exhibit E.

7. The Staffordshire PCC's 9 February 2018 decision was wrong and/or unlawful in that it erred in concluding that:

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

    b. Sections 23(5) was engaged by the request;

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

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

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

II. The Facts

A. Privacy International

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

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

B. IMSI Catchers

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

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

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

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

14. The indiscriminate nature by which IMSI Catchers collect data means that their use can also interfere with the rights to freedom of expression and to freedom of assembly and

[1] IMSI Catchers typically also collect the "International Mobile Station Equipment Identifier" ("IMEI") of mobile phones. The IMEI is unique to each mobile phone whereas the IMSI is unique to each SIM card.
[2] Article 29 Data Protection Working Party, Opinion 13/2011 on Geolocation Services on Smart Mobile Devices, 881/11/EN, 16 May 2011, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp185_en.pdf.

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

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

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

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

18. On 10 October 2016, an article appeared in *The Bristol Cable* entitled: "Revealed: Bristol's police and mass mobile phone surveillance."[7] The article makes reference (and links) to the minutes of an Alliance Governance Group meeting in May 2016 between

---

[3] *See* Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, U.N. Doc. A/HRC/29/32, 22 May 2015, available at http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/29/32; *see also* Written Submissions on Behalf of Privacy International and Article 19, *Breyer v Germany*, European Court of Human Rights, App. No. 50001/12, 5 Sept. 2016.

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

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

[6] Electronic Surveillance: Written question – HL2602, 3 Nov. 2014, available at http://www.parliament.uk/business/publications/written-questions-answers-statements/written-question/Lords/2014-11-03/HL2602.

[7] Alon Aviram, "Revealed: Bristol's police and mass mobile phone surveillance," The Bristol Cable, 10 Oct. 2016, https://thebristolcable.org/2016/10/imsi/.

Warwickshire and West Mercia Police in which the topic of "Covert Communications Data Capture" ("CCDC") equipment was discussed.[8] Specifically, those minutes state: "*Within the West Midlands region both West Midlands and Staffordshire Police have recently purchased and operated 4G compatible CCDC equipment*."

19. On the same day, *The Guardian* published the article "Controversial snooping technology 'used by at least seven police forces'".[9] The article reported that "*surveillance technology that indiscriminately harvests information from mobile phones*", also "*known as an IMSI catcher*" is being "*used by at least seven police forces across the country…according to police documents*."

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

III. Procedural History

A. Request for Information

21. On 1 November 2016, Privacy International requested the following information from the Staffordshire PCC:

    1. *Records relating to the purchase of CCDC equipment, referred to in the Alliance Government Group minutes…, including purchase orders, invoices, contracts, loan agreements, solicitation letters, correspondence with companies and other similar records.*

    2. *Records relating to the "robust safeguards" and "legislation" to govern the use of CCDC equipment by Staffordshire Police that [the Staffordshire PCC] referred to in the Guardian article…*

    3. *Any other records, including legislation, codes of practice, policy statements, guides, manuals, memoranda, presentations, training materials or other records governing the possession and use of CCDC equipment by Staffordshire Police, including restrictions on when, where, how and against whom it may be used, limitations on retention and use of collected data, guidance on when a warrant or other legal process must be obtained, and rules governing when the existence and use of CCDC equipment may be revealed to the public, criminal defendants, or judges.*

[8] https://thebristolcable.org/wp-content/uploads/2016/10/09-imsi-4.pdf
[9] David Pegg & Rob Evans, "Controversial snooping technology 'used by at least seven police forces,'" The Guardian, 10 Oct. 2016, https://www.theguardian.com/world/2016/oct/10/controversial-phone-snooping-technology-imsi-catcher-seven-police-forces.

B. The Refusal

22. On 9 February 2018, following Privacy International's appeal to the Commissioner and the Commissioner's issuance of a decision notice, the Staffordshire PCC refused the request on grounds that it could NCND whether it held the information requested pursuant to sections 23(5), 24(2) and 31(3) FOIA. On 12 February 2018, the Senior Case Officer of the ICO indicated that the Commissioner would accept a complaint against the Staffordshire PCC's decision without a further internal review, given the length of time between the initial request for information and the decision by the Staffordshire PCC.

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

    a. By confirming or denying that the PCC 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.

    b. Any disclosure under FOIA is a disclosure to the world at large, and confirming or denying the use of specialist techniques which may or may not exist, and which (should they exist) the police service may or may not deploy in specific circumstances would prejudice law enforcement. If the requested information was held by the PCC, 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 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.

    c. Conversely, if information was not held by the PCC, 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. 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.

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

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

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

> "***Factors favouring confirming or denying whether any other information is held for Section 24***
> *The public is entitled to know where 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 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.*
>
> ***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.*"

25. The Staffordshire PCC acknowledged that while "*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." Moreover, the PCC submitted that "*[a]s much as there is public interest in knowing that policing activity is appropriate and balanced in matters of national security this will only be overridden in exceptional circumstances*" and that there is "*no requirement to satisfy any public concern over the legality of police operations and the tactics we may or may not use*."

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

IV. The Appeal

A. The Purpose of FOIA

27. 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.

28. There is a high degree of consensus under international law that access to information is part of the right to freedom of expression. In particular, the Commissioner should have regard to the Grand Chamber decision in *Magyar Helsinki Bizottság v Hungary*.[10] 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.[11]

29. 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*

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

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'."

30. As a human rights organisation, Privacy International plays the role of a watchdog, similar to that played by the press.[12] Indeed, in litigation before the European Court of Human Rights, the UK Government has accepted that "*NGOs engaged in the legitimate gathering of information of public interest in order to contribute to public debate may properly claim the same Art. 10 protections as the press.*"[13] Privacy International seeks to advance the right to privacy around the world, including in the UK. It carries out this work, in part, by conducting research on a variety of issues related to privacy and surveillance and publishing that research in multiple formats, including research reports, policy papers and blog posts. It seeks information about IMSI Catchers in order to educate the public about the government's use of this surveillance technology and its human rights implications, including for the right to privacy.

31. 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 F.

B. Section 23(5) FOIA

32. 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

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

relates to, any of the bodies specified in section 23(3).

33. 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 or more bodies identified in section 23(3) of the FOIA*."[14]

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

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

    b. Privacy International's request further seeks information relating to the use of IMSI Catchers *by police forces*. Just because IMSI Catchers may also be used

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

by the bodies specified in section 23(3) is not enough for section 23(5) to be engaged. There are many techniques – ranging from the simple to the sophisticated – that both the police forces and the section 23(3) bodies may deploy. For that reason, the reliance on the argument that both the Police Act 1997 and the Intelligence Services Act 1994 cover a technique is meaningless. For example, both pieces of legislation authorise the power to interfere with property, which may include entry onto property. A logical extension of this argument would engage section 23(5) for any technique covered by both statutes. Similarly, reliance on the argument that there is a close relationship between the police forces and security bodies is dangerously vague. Indeed, a logical extension of that argument would engage section 23(5) for any technique deployed by the police forces. The Staffordshire PCC have made no attempt to indicate the circumstances in which police forces use IMSI Catchers, which could include ordinary law enforcement activities such as tracking a suspect for a variety of offences, and how those circumstances in any way relate to the section 23 bodies.

C. Section 24(2) FOIA

35. 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.

36. The Commissioner has recently held in a decision on IMSI Catchers that consideration of the section 24(2) exemption is a "*two-stage process*": first, the exemption must be engaged "*due to the requirement of national security*" and second, the exemption is "*qualified by the public interest, which means that the confirmation or denial must be provided if the public interest in the maintenance of the exemption does not outweigh the public interest in disclosure*."[15]

37. The Commissioner has also previously held that *"this exemption should be interpreted so that it is only necessary for a public authority to show that either a confirmation or a denial of whether requested information is held would be likely to harm national security. The Commissioner interprets the phrase 'required' in the context of this exemption as 'reasonably necessary'. In effect this means that there has to be a risk of harm to national security for the exemption to be relied upon, but there is no need for a public authority to prove that there is a specific, direct or imminent threat'. "*[16]

38. In the recent decision on IMSI catchers, the Commissioner found that there was some valid public interest in confirmation or denial as it would "*increase public knowledge*

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

regarding the extent, or otherwise, of the use of IMSI catchers, by Nottinghamshire Police, which may give an indication regarding their use by the police service as a whole." However, the Commissioner determined that this interest was outweighed by that in safeguarding national security.[17]

i. Safeguarding National Security

39. In the recent decision on IMSI Catchers, the Commissioner discussed the first prong of the section 24(2) FOIA exemption and relied heavily on the justification that because the Commissioner had already found section 23(5) to be engaged, section 24(2) would also be engaged, since "*a disclosure that touches on the work of the security bodies would consequentially undermine national security*."[18]

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

41. The Staffordshire PCC also base arguments around national security on skeletal assertions that national security would be impacted by (1) at a general level, confirming or denying the use of "specialist techniques" and (2) at a specific level, indicating that a technique is used one area but not in another area. Both arguments are baseless. As to the first argument, the Staffordshire PCC does not define a "specialist technique" and why IMSI Catchers constitute a specialist technique. Furthermore, it does not follow that merely confirming or denying that a police force uses IMSI Catchers reveals operationally sensitive information that would negatively impact national security. In fact, the government has willingly admitted and subjected to either public regulation or FOIA requests the use of a variety of what might also be considered "specialist techniques" – from hacking[19] to the use of equipment to physically extract mobile phone data.[20] There is therefore no reason that information governing the use of IMSI Catchers by police forces

[17] ICO, Decision Notice, Ref. FS50665716, 13 June 2017, paras. 29-30; *see also* ICO Decision Notice, Ref. FS50660527, 8 June 2017, paras. 30-31.
[18] ICO, Decision Notice, Ref. FS50665716, 13 June 2017, para. 27; *see also* ICO Decision Notice, Ref. FS50660527, 8 June 2017, para. 29.
[19] *See* Part 5, Investigatory Powers Act; *see also* Equipment Interference: Draft Code of Practice.
[20] *See, e.g.*, Disclosure by the Metropolitan Police Service, 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.

should be afforded special protection. As to the second argument, it does not follow that determining which police forces use this equipment could permit individuals to map or be aware of how operationally sensitive information is obtained, thereby negatively impacting national security. Different police forces will obtain information in many different ways.

ii. Public Interest Test

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

43. 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 Staffordshire PCC has failed to consider that there is public interest in citizens being informed about methods of surveillance that could have a profound impact on their fundamental rights, including the rights to privacy, freedom of expression and freedom of assembly and association. In particular, there is significant public interest in the topic of IMSI Catchers and the regulation of related communication surveillance technologies. Indeed, because IMSI Catchers can indiscriminately collect data (by tricking all mobile phones within a given range to identify themselves and reveal their location), their use can interfere with the rights of many persons, including those who are not the intended targets of surveillance.

44. 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.

45. With respect to the public interest, the Court stated that "*the public interest relates to matters which affect the public to such an extent that it may legitimately take an interest in them, which attract its attention or which concern it to a significant degree, especially in that they affect the well-being of citizens of the life of the community*".[21] As discussed above, IMSI Catchers engage the public interest because their use implicates the fundamental rights of many citizens, Privacy International seeks this information in its role as a public watchdog, and it intends to use the information requested to educate the public about the use of IMSI Catchers and their human rights implications.

46. The *Magyar Helsinki Bizottság* decision's reasoning on public interest effectively affirmed a prior decision in *Youth Initiative for Human Rights v Serbia*, which concerned an NGO that was monitoring the implementation of transitional laws in Serbia with a view to ensuring respect for human rights.[22] The applicant NGO requested the intelligence agency of Serbia to provide it with factual information concerning the use of electronic surveillance measures by that agency. The Court held that the NGO was involved in the legitimate gathering of information of public interest with the intention of imparting that information to the public and thereby contributing to the public debate.

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

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

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

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

[21] *Magyar Helsinki Bizottság v Hungary*, European Court of Human Rights, App. No. 18030/11, 8 Nov. 2016, para. 162.
[22] *Youth Initiative for Human Rights v Serbia*, European Court of Human Rights, App. No. 48135/06, 25 June 2013.

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

D. Section 31(3) FOIA

48. 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.

49. 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… 'would be likely' to result in prejudice or confirming or denying whether information is held 'would' result in prejudice. In relation to the lower threshold the Commissioner considers that the chance of prejudice occurring must be more than a hypothetical possibility; rather there must be a real and significant risk. With regard to the higher threshold, in the Commissioner's view this places a stronger evidential burden on the public authority to discharge.*"[23]

i. Prejudice to Law Enforcement Matters

50. Again, as discussed above, in relation to the section 23(5) and 24(2) FOIA exemptions, the request relates in part to legislation, policy guidance and information governing the use of IMSI Catchers by police forces. These records, which relate to the legal basis for a public authority's powers and activities and the rules governing those powers and

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

activities, cannot be subject to NCND under any exemption.

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

ii. Public Interest Test

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

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

54. 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.

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

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

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

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

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

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

F. Conclusion

56. For the reasons set out above, the Commissioner is respectfully invited to allow this appeal and to issue a decision notice directing the Staffordshire PCC 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.

14 February 2018

Ailidh Callander
Scarlet Kim

Privacy International

EXHIBIT A

PRIVACY INTERNATIONAL

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

Matthew Ellis
Police and Crime Commissioner for Staffordshire
Staffordshire Police HQ (Block 9)
Weston Road, Stafford
ST18 0YY

1 November 2016

Dear Mr. Ellis,

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

Alliance Governance Group Meeting Minutes

I refer, in particular, to the recent article written by the journalist collective The Bristol Cable "Revealed: Bristol's police and mass mobile phone surveillance".[1] The article makes reference to the minutes of an Alliance Governance Group meeting in May 2016 between Warwickshire and West Mercia Police in which the topic of "Covert Communications Data Capture" (CCDC) equipment was discussed.[2]

Specifically, the minute's record: "Within the West Midlands region both West Midlands and **Staffordshire Police** have recently **purchased and operated 4G compatible CCDC equipment**. Both have purchased the same equipment from the company referred to as option 3"

I am unable to find relevant information regarding these purchases on the Staffordshire Police and Crime Commissioner website.

Guardian Article

I also refer to the 10 October 2016, the Guardian published the article "Controversial snooping technology 'used by at least seven police forces'" in which you were quoted as saying[3]:

"Some tactics police use to keep people safe and bring criminals to justice can be intrusive and it is crucial that there are **robust safeguards, framed by legislation, around the work, and there are**."

[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

Record Requests

Privacy International requests the following records:

1. Records relating to the purchase of CCDC equipment, referred to in the Alliance Government Group minutes referenced above, including purchase orders, invoices, contracts, loan agreements, solicitation letters, correspondence with companies and other similar records.

2. Records relating to the "robust safeguards" and "legislation" to govern the use of CCDC equipment by Staffordshire Police that you referred to in the Guardian article referenced above.

3. Any other records, including legislation, codes of practice, policy statements, guides, manuals, memoranda, presentations, training materials or other records governing the use of CCDC equipment by Staffordshire Police, including restrictions on when, where, how, and against whom it may be used, limitations on retention and use of collected data, guidance on when a warrant or other legal process must be obtained, and rules governing when the existence and use of CCDC equipment may be revealed to the public, criminal defendants, or judges.

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

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

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

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

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

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

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

Sincerely,

Matthew Rice
Advocacy Officer

cc: Scarlet Kim
Legal Officer

EXHIBIT B

BEFORE THE INFORMATION COMMISSIONER

BETWEEN

PRIVACY INTERNATIONAL

Applicant

- and -

STAFFORDSHIRE POLICE AND CRIME COMMISSIONER

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 Staffordshire Police and Crime Commissioner ("PCC"), Home Office, National Police Chiefs Council, National Crime Agency, Metropolitan Police, South Yorkshire Police, Avon and Somerset PCC, Kent 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 govenring the use of such equipment. This equipment can be referred to using a range of terms, including "Covert Communications Data Capture" ("CCDC") equipment, "IMSI Catchers", "IMSI Grabbers", "Cell site simulators" and "Stingrays". In this document the equipment is hereafter referred to as "IMSI Catchers".

3. Staffordshire PCC has failed to respond to the initial request for information. That request is annexed to these grounds as Exhibit A.

4. This decision was wrong and/or unlawful, in that:

    a. Staffordshire PCC has failed in its duty under section 1 of the Freedom of Information Act ("FOIA") 2000 to provide the requested information, deny the request or confirm or deny that it holds information.

    b. Staffordshire PCC has breached section 10 FOIA by failing to respond within the required time for compliance.

II. The Facts

A. Privacy International

5. 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, and fight 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 the United Kingdom*, European Court of Human Rights, App. no. 60646/14).

6. 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 phone 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

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

8. 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

[1] IMSI Catchers typically also collect the "International Mobile Station Equipment Identifier" ("IMEI") of mobile phones. The IMEI is unique to each mobile phone whereas the IMSI is unique to each SIM card.

to the extent necessary to determine that individual's mobile IMSI/IMEI or whereabouts.[2] 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.[3]

9. On 10 October 2016, an article appeared in the Bristol Cable entitled: "Revealed: Bristol's police and mass mobile phone surveillance."[4] 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.

10. Specifically, the minutes record: "*Within the West Midlands region both West Midlands and Staffordshire Police have recently purchased and operated 4G compatible CCDC equipment. Both have purchased the same equipment from the company referred to as option 3*".[5]

11. On the same day, the Guardian published the article "Controversial snooping technology 'used by at least seven police forces'".[6] Staffordshire PCC was quoted in the article as saying "*Some tactics police use to keep people safe and bring criminals to justice can be intrusive and it is crucial that there are robust safeguards, framed by legislation, around the work, and there are*."

III. Request for Information

12. On 1 November 2016, Privacy International requested the following information from Staffordshire PCC:

> "*1. Records relating to the purchase of CCDC equipment, referred to in the Alliance Government Group minutes . . . including purchase orders, invoices, contracts, loan agreements, solicitation letters, correspondence with companies and other similar records.*
>
> *2. Records relating to the "robust safeguards" and "legislation" to govern the use of CCDC equipment by Staffordshire Police that you referred to in the Guardian article referenced above.*

---

[2] Section 100i of the *Criminal Procedure Code* (*Strafprozessordnung*, StPO) (Germany), available at https://www.gesetze-im-internet.de/englisch_stpo/englisch_stpo.html.
[3] 2015 U.S. Department of Justice Policy, available at https://www.justice.gov/opa/file/767321/download.
[4] Alon Aviram, "Revealed: Bristol's police and mass mobile phone surveillance," The Bristol Cable, 10 October 2016, https://thebristolcable.org/2016/10/imsi/.
[5] Alliance Governance Group Minutes, available at https://thebristolcable.org/wp-content/uploads/2016/10/09-imsi-4.pdf.
[6] 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.

3. Any other records, including legislation, codes of practice, policy statements, guides, manuals, memoranda, presentations, training materials or other records governing the possession and use of CCDC equipment by Staffordshire Police, including restrictions on when, where, how, and against whom it may be used, limitations on retention and use of collected data, guidance on when a warrant or other legal process must be obtained, and rules governing when the existence and use of CCDC equipment may be revealed to the public, criminal defendants, or judges."

13. The request made it clear that Privacy International sought the records regardless of how "CCDC equipment" was identified.

14. On 1 December 2016, Staffordshire PCC sent an email apologising for the delay and indicating that a response would be forthcoming shortly. On 22 December 2016, following an email from Privacy International, Staffordshire PCC sent another email again indicating that a response would be forthcoming shortly. On 18 January 2017, following an email from Privacy International, Staffordshire PCC sent another email again indicating that a response would be forthcoming shortly. These emails are annexed to these grounds as Exhibit B. Since then, Privacy International has received no response to the request despite numerous attempts to obtain a response. Privacy International sent further emails to Staffordshire PCC on 19 May 2017, 8 June 2017, 19 July 2017, 21 August 2017 and 7 September 2017. These emails are annexed to these grounds as Exhibit C. No further response was received.

IV. Decision Under Challenge

15. Staffordshire PCC has failed to provide Privacy International with a response to the request despite numerous efforts on its part. The failure to respond substantively to the request since 1 November 2016 contravenes sections 1 and 10 FOIA. Section 10 FOIA provides that a public authority has a duty to "*comply with section 1(1) promptly and in any event not later than the twentieth working day following the date of receipt*." Section 1(1) provides that a person making a request pursuant to FOIA is entitled "*to be informed in writing by the public authority whether it holds information of the description specified in the request, and . . . to have that information communicated*."

16. Staffordshire PCC has failed in these duties and has failed to respond to the request promptly. Privacy International has not been provided with any explanation as to the delay.

V. Conclusion

17. For the reasons set out above, Privacy International is applying to the Information Commissioner for a decision in accordance with section 50 FOIA. The Commissioner is

respectfully invited to allow this appeal and to issue a decision notice, finding a breach of sections 1 and 10 FOIA and requiring Staffordshire PCC to take steps to comply with its obligations under FOIA.

15 December 2017

Ailidh Callander
Scarlet Kim

Privacy International

EXHIBIT C

Reference: FS50716661

Freedom of Information Act 2000 (FOIA)

Decision notice

Date: 8 January 2018

Public Authority: Police and Crime Commissioner for Staffordshire
Address: Staffordshire Police Headquarters
Weston Road
Stafford
ST18 0YY

Complainant: Scarlet Kim obo Privacy International
Address: scarlet@privacyinternational.org

Decision (including any steps ordered)

1. The complainant has requested information about the purchase and use of mobile phone surveillance equipment from the Police and Crime Commissioner for Staffordshire ("the PCC"); to date she has not received a substantive response. The Commissioner's decision is that the PCC has breached sections 1(1) and 10(1) of the FOIA in that it failed to provide a valid response to the request within 20 working days of receipt. She requires it to comply with the request or to issue a valid refusal notice as set out in section 17 of the FOIA.

2. The PCC must take these steps within 35 calendar days of the date of this decision notice. Failure to comply may result in the Commissioner making written certification of this fact to the High Court pursuant to section 54 of the FOIA and may be dealt with as a contempt of court.

Request and response

3. On 1 November 2016 the complainant wrote to the PCC and requested information about the purchase and use of mobile phone surveillance equipment by the Staffordshire Police. The complainant referred directly to minutes of the Alliance Government Group, as reported by journalist

collective "The Bristol Cable", and an article in the Guardian newspaper; she provided links to the relevant articles. The request was worded as follows:

> *" I am writing on behalf of Privacy International to seek records ...relating to the purchase and use of mobile phone surveillance equipment by the Staffordshire Police ....*
>
> *1. Records relating to the purchase of CCDC equipment, referred to in the Alliance Government Group minutes referenced above, including purchase orders, invoices, contracts, loan agreements, solicitation letters, correspondence with companies and other similar records.*
>
> *2. Records relating to the "robust safeguards" and "legislation" to govern the use of CCDC equipment by Staffordshire Police that you referred to in the Guardian article referenced above.*
>
> *3. Any other records, including legislation, codes of practice, policy statements, guides, manuals, memoranda, presentations, training materials or other records governing the use of CCDC equipment by Staffordshire Police, including restrictions on when, where, how, and against whom it may be used, limitations on retention and use of collected data, guidance on when a warrant or other legal process must be obtained, and rules governing when the existence and use of CCDC equipment may be revealed to the public, criminal defendants, or judges.*
>
> *Privacy International seeks records regardless of how CCDC equipment is identified. In this respect, Privacy International notes that CCDC equipment can be referred to using a range of other terms, including "IMSI Catchers", "IMSI Grabbers", "Cell site simulators" and "Stingrays".*
>
> *Please include copies of material that you hold either in the form of paper or electronic records, including emails. If possible, please provide all requested records in electronic format.*
>
> *Upon locating the requested records, please contact us and advise us of any costs of providing copies, so that we may decide whether it is necessary to narrow our request.*
>
> *We would appreciate a response as soon as possible and look forward to hearing from you shortly".*

4. Receipt of the request was acknowledged on the same day.

5. On 1 December 2016 the complainant chased a response. The PCC advised on the same day that it was hoping to get: " *something out to you by next week*". A response was chased again on 16 and 22 December 2016 and, on 22 December 2016, the PCC advised: "*Apologies yes I should have your response by today/tomorrow at the latest and sorry for the delay*".

6. A response was chased on several further occasions including 19 May 2017, 8 June 2017, 19 July 2017, 21 August 2017 and 7 September 2017.

Scope of the case

7. The complainant contacted the Commissioner on 15 December 2017 to complain about the lack of response to her information request.

8. The Commissioner contacted the PCC on 21 December 2017 asking the PCC to respond to the request within five working days. The PCC apologised for the delay and advised that it thought the request had been dealt with. It assured the Commissioner that a response would be sent to the complainant, and a copy provided for her information, within the five days.

9. No substantive response to the request had been provided by the date of this notice.

Reasons for decision

Section 1 – general right of access
Section 10 - time for compliance

10. Section 1(1) of the FOIA states that an individual who asks for information is entitled to be informed whether the information is held and, if the information is held, to have that information communicated to them.

11. Section 10(1) of the FOIA states that on receipt of a request for information a public authority should respond to the applicant within 20 working days.

12. From the information provided to the Commissioner in this case it is evident that the PCC did not deal with the request for information in accordance with the FOIA. In this case the PCC has breached sections 1(1) and 10(1) by failing to respond to the request within 20 working days. The PCC is now required to respond to the request of 1 November 2016 in accordance with the FOIA.

Other matters

13. As well as finding above that the PCC is in breach of the FOIA, the Commissioner has also made a record of the delay in this case. This may form evidence in future enforcement action against the PCC should evidence from other cases suggest that there are systemic issues which are causing delays.

Right of appeal

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

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

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

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

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

Signed .....

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

EXHIBIT D

Office of the Police and Crime Commissioner
STAFFORDSHIRE

01785 232270
www.staffordshire-pcc-gov.uk
Twitter: @StaffsPCC

FAO Mr Matthew Rice
Privacy International
62 Briton Street
London
EC1M 5UY

Date: 9 February 2018

Ref: FOI/2016/Privacy International

Dear Matthew/Scarlet

I write on behalf of the Police and Crime Commissioner (PCC) in responding to your Freedom of Information (FOI) request. I apologise for the delay in our replying, but please find below our response.

- Records relating to the purchase of CCDC equipment, referred to in the Alliance Government Group minutes referenced above, including purchase orders, invoices, contracts, loan agreements, solicitation letters, correspondence with companies and other similar records.

- Records relating to the "robust safeguards" and "legislation" to govern the use of CCDC equipment by Staffordshire Police that you referred to in the Guardian article referenced above.

- Any other records, including legislation, codes of practice, policy statements, guides, manuals, memoranda, presentations, training materials or other records governing the use of CCDC equipment by Staffordshire Police, including restrictions on when, where, how, and against whom it may be used, limitations on retention and use of collected data, guidance on when a warrant or other legal process must be obtained, and rules governing when the existence and use of CCDC equipment may be revealed to the public, criminal defendants, or judges.

The information that you have requested has been handled under the Freedom of Information ACT 2000 (FOIA) and I can neither confirm nor deny whether we hold the information that you have requested.

We are not obliged to confirm or deny whether we hold the information you have requested as by confirming or denying that Office of the Police and Crime Commissioner (OPCC) 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.

Section 23(5), 24(2), and 31(3) of the Act provides that there is no duty to confirm or deny whether we hold the information that has been requested. The response provided should not be taken as an indication that the information you requested is or is not held by the department.

The terms of the Section 23 exemption in the Freedom of Information Act mean that we do not have to consider whether or not it would be in the public interest for us to reveal whether or not the information is held.

In regards to the terms of the Section 24 and 31 exemptions these are prejudice based qualified exemptions and there is a requirement to articulate the harm that would be caused in confirming or denying that the information is held as well as carrying out a public interest test.

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 OPCC, 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 OPCC, 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, 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.

Public Interest Test

We have applied the public interest test to confirming or denying whether information is held in respect of sections 24 and 31 in regards to your request and are satisfied that the response we have provided meets this test.

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 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.

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.

Office of the Police and Crime Commissioner
STAFFORDSHIRE

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.

You can find out more about the Freedom of Information Act by reading the full text of the Act (available at www.legislation.gov.uk/ukpga/2000/36/contents).

If you are dissatisfied with the handling of your request, you have the right to ask for an internal review. Internal review requests should be submitted within two months of the date of receipt of this email and should be addressed to:

Glynn Dixon
Office of the Police and Crime Commissioner
Block 9
Weston Road
Stafford
ST18 0YY

Please remember to quote the reference number in any future communications.

Should you require any further information please contact Central Disclosure Unit on 01785 232270

Yours sincerely

Veronica Powell
Office Manager for and on behalf of the
Office of the Police and Crime Commissioner for Staffordshire

EXHIBIT E

From: **Carolyn S. Howes** Carolyn.Howes@ico.org.uk
Subject: Staffordshire PCC
Date: 12 February 2018 at 10:22
To: Scarlet scarlet@privacyinternational.org

CH

Hi Scarlet

I note that Staffs PCC has now complied with our decision notice and issued a response, which they have copied to me. As you have already waited so long for this, I am happy to accept any complaint you wish to submit without a further internal review – which I very much doubt would lead to any changes at this stage in any event.

Therefore, if you wish to submit a complaint against them please do so. I have not advised them that I will accept one at this point, but I will do when I commence any investigation.

Regards
Carolyn

ico.
Information Commissioner's Office

Carolyn Howes
Senior Case Officer

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
T. 01625 545712 F. 01625 524510 ico.org.uk
twitter.com/iconews
Please consider the environment before printing this email

EXHIBIT F

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

I. Introduction

In the United States, a range of requests pursuant to federal and state freedom of information laws relating to law enforcement acquisition, use and regulation of IMSI Catchers have resulted in the disclosure of relevant records, including purchase records, product descriptions, non-disclosure agreements and policy guidance. These records were disclosed notwithstanding exemptions under the relevant laws protecting certain categories of information, including information classified to protect national security and information related to law enforcement techniques and procedures. Privacy International provides an overview of US freedom of information laws, a summary of these requests, and a summary of the records produced, which are publicly available. It believes that this comparative perspective may prove useful to the Information Commissioner in considering the refusals of the public bodies to confirm or deny the existence of records relating to the acquisition, use and regulation of IMSI Catchers in the UK.

II. A Summary of US Freedom of Information Laws

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

---

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

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

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

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

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

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

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

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

---

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

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

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

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

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

---

[9] Reporters Committee for Freedom of the Press, *Federal FOIA Appeals Guide*, Exemption 1, Pt. II.F, https://www.rcfp.org/federal-foia-appeals-guide/exemption-1/ii-appealing-agency%E2%80%99s-withholding-records-substantive-grou-10.

[10] *Id*. at Exemption 7, Pt. I.C.iii. https://www.rcfp.org/federal-foia-appeals-guide/exemption-7/ii-harm-disclosure/c-7c/iii-glomar-response.

[11] 5 U.S.C. § 552 (a)(3)(A).

[12] An agency's failure to comply with the time limits to respond to an initial request or an administrative appeal may be treated as "constructive exhaustion", entitling the requester to seek judicial review. *See* 5 U.S.C. § 552(a)(6)(C).

[13] A comprehensive guide to each state's open laws framework is available at Reporters Committee for a Free Press, *Open Government Guide*, https://www.rcfp.org/open-government-guide.

[14] Reporters Committee for Freedom of the Press, *New York – Open Government Guide*, Pt. II.A.1.c, https://www.rcfp.org/new-york-open-government-guide/ii-exemptions-and-other-legal-limitations/exemptions-open-records-s-3 (citing relevant New York case law in support of this statement).

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

III. FOIA Requests to Federal Agencies for IMSI Catcher Records

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

A. Electronic Privacy Information Center – FBI

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

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

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

---

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

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

C. American Civil Liberties Union – Various Federal Agencies

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

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

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

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

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

---

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

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

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

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

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

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

A. Florida

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

Florida Department of Law Enforcement ("FDLE")

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

Tallahassee Police Department ("TPD")

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

Miami-Dade Police Department

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

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

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

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

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

B. New York

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

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

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

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

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

The records disclosed by the RPD include:

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

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

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

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

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

C. Michigan

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

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

D. CityLab

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

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