BEFORE THE INFORMATION COMMISSIONER

BETWEEN

PRIVACY INTERNATIONAL

Applicant

- and -

WARWICKSHIRE 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 Warwickshire 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, Staffordshire 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 Warwickshire PCC is annexed to these grounds as Exhibit A.

3. On 20 December 2016, the Warwickshire PCC responded to the request. The Warwickshire PCC indicated that, in response to 3 of the 4 categories of records requested, it held "*a small amount of information namely a business case regarding the replacement of existing CCDC equipment"* in response to the request but that this information was exempt from disclosure under sections 24(1) and 31(a) and (b) of the Freedom of Information Act ("FOIA") 2000. The Warwickshire PCC further indicated that, in response to 1 of the 4 categories of records requested, it could neither confirm nor deny ("NCND") whether it held the information requested pursuant to section 23(5) FOIA. This response is annexed to these grounds as Exhibit B.

4. On 22 May 2017, Privacy International made a request for internal review of the Warwickshire PCC's decision. This request is annexed to these grounds as Exhibit C.

5. On 13 July 2017, the Warwickshire PCC upheld its initial decision with the exception of one aspect of its decision to NCND one of the categories of records. It held that part of that category was exempt pursuant to section 21 FOIA. This decision is annexed to these grounds as Exhibit D.

6. The Warwickshire PCC's 13 July 2017 decision was wrong and/or unlawful in that it erred in concluding that:

    a. Sections 24(1) and 31(1)(a)-(b) FOIA were engaged by the request;

    b. In all the circumstances of the case, the public interest in not disclosing the information requested outweighs the public interest in disclosing the information requested pursuant to sections 24(1) and 31(1)(a)-(b) FOIA;

    c. It sufficiently demonstrated the application of section 21 FOIA to the request;

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

    e. Section 23(5) was engaged by the request.

II. The Facts

A. Privacy International

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

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

B. IMSI Catchers

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

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

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

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

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

14. Finally, the use of IMSI Catchers has a number of implications for the ability of individuals to maintain their anonymity, including when attending a gathering. There are

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

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

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

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

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

17. On 10 October 2016, an article appeared in *The Bristol Cable* entitled: "Revealed: Bristol's police and mass mobile phone surveillance."[7] The article makes reference (and links) 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.[8] Specifically, those minutes state: "*Both [Warwickshire and West Mercia] PCCs agreed to Replacing the existing equipment with a new supplier*."

---

[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/.

[8] https://thebristolcable.org/wp-content/uploads/2016/10/09-imsi-4.pdf

18. 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*."

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

III. Procedural History

A. Request for Information

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

> 1. *Records relating to the purchase of "existing" 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 purchase of replacement CCDC equipment, referred to in the Alliance Government Group minutes…, including purchase orders, invoices, contracts, loan agreements, solicitation letters, correspondence with companies and other similar records.*
>
> 3. *Records relating to the decision "to Replace[ ] the existing [CCDC] equipment with a new supplier", referred to in the Alliance Governance Group minutes…, including any records referred to or consulted in reaching that decision.*
>
> 4. *Legislation, codes of practice, policy statements, guides, manuals, memoranda, presentations, training materials or other records governing the use of CCDC equipment by Warwickshire Police, including restrictions on when, where, how and against whom it may be used, limitations on retention and use of collected data, guidance on when a warrant or other legal process must be obtained, and rules governing when the existence and use of CCDC equipment may be revealed to the public, criminal defendants, or judges.*

[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

21. On 20 December 2016, the Warwickshire PCC refused the request.

22. With respect to questions 1-3, the Warwickshire PCC indicated that it held "*a small amount of information namely a business case regarding the replacement of existing CCDC equipment*" but that "*this is exempt from disclosure under section 24(1) (national security) and section 31(a) and (b) (law enforcement)*" FOIA. The reasons given for the refusal to disclose the information were as follows:

    a. Section 24(1) provides that information is exempt from disclosure if the exemption is required for the purposes of safeguarding national security. The document is a confidential strategic paper, produced to evaluate the functionality and options in respect of existing and replacement CCDC equipment, and if disclosed would undermine national security.

        i. There is a public interest in how public funds are spent, and a natural concern to ensure that any measures in place to safeguard national security are effective, and further that any covert activities are proportionate to the risks that a public authority may be seeking to address. While there is a level of public awareness in this area, the exact nature of the discussions regarding the equipment or any associated issues are not widely known.

        ii. There is an inherent public interest in safeguarding national security to ensure the safety of the UK. The disclosure of this information would undermine the strategic aims and deliberations in respect of the equipment by exposing them to criminals and terrorists who would seek to use the information to their advantage. Any information which undermines the operational integrity and effectiveness of the OPCC's activities (and that of other agencies) would adversely affect public safety and this would not be in the wider public interest. On balance, the public interest therefore favours maintaining this exemption.

    b. Section 31(1) provides that information is exempt if disclosure would, or would be likely to prejudice (a) the prevention or detection of crime or (b) the apprehension or prosecution of offenders.

        i. The disclosure of this document would prejudice the methods and strategies deployed or considered by the OPCC in relation to the prevention and detection of crime and the apprehension or prosecution of offenders. As mentioned, although there is now a level of public awareness in this area, the exact nature of the discussions regarding the equipment or any associated issues is not openly discussed. While the

disclosure of this document would serve to increase public awareness, it would do so particularly amongst those individuals involved in serious and organised crime or terrorism, and who would be best placed to exploit the information to their advantage.

ii. In addition to the public interest factors mentioned in respect of section 24(1), there is a public interest in disclosing information that holds public bodies to account, and increases transparency about how they perform their functions. However, there is an inherent public interest in both protecting society from the impact of crime and preserving the integrity of the OPPC's law enforcement activities in this area. The disclosure of this information would serve to provide a greater understanding to criminals and terrorists, as to the OPCC's strategic aims and deliberations regarding the use of such equipment, including any associated issues, the detail of which is not openly discussed in order to maintain operational effectiveness. Furthermore, the OPCC requires a safe space in which to explore and evaluate its operational activities, in the absence of external scrutiny. The disclosure of this information would hinder the effective conduct of the OPCC's functions (and that of other agencies) with regard to the prevention or detection of crime and the apprehension or prosecution of offenders for fear that such information may enter the public domain. On balance, the public interest therefore favours maintaining this exemption.

23. With respect to question 4, the Warwickshire PCC submitted that section 23(5) FOIA was "*engaged…and as such the OPCC can neither confirm nor deny whether information falling under this aspect [of] your request is held, as to do so would undermine the operational effectiveness of national security and law enforcement*."

C. Request for Internal Review

24. On 22 May 2017, Privacy International challenged the refusal.

25. First, Privacy International submitted that when considering the application of any of the FOIA exemptions, it is necessary to have regard to the language and purpose of FOIA, which require exemptions to be narrowly construed:

a. The word "*required"* in section 1(1)(a) FOIA "*means reasonably necessary. It is not sufficient for the information sought simply to relate to national security; there must be a clear basis for arguing that disclosure would have an adverse effect on national security before the exemption is engaged*";[10]

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

b. It is therefore clear that a decision to NCND requires a clear justification and merits close scrutiny. This is because it flies in the face of the "*default setting*" in FOIA, which is in favour of disclosure.[11] It also flies in the face of the Article 10 right to receive information, as recently confirmed by the European Court of Human Rights;[12]

26. With respect to the refusal to disclose relevant records responsive to questions 1-3, Privacy International submitted that 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 failing to disclose the information held;

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

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

d. The refusal recognises that "*there is a public interest in how public funds are spent, and a natural concern to ensure that any measures in place to safeguard national security are effective, and further that any covert activities are proportionate to the risks that a public authority may be seeking [to] address*". Despite these factors, the request was refused on the basis of assertions.

27. With respect to the decision to NCND the existence of records responsive to question 4, Privacy International submitted:

a. The Warwickshire PCC response was predicated on a *non-sequitur*:

i. It simply does not follow that merely confirming or denying the existence of legislation, codes of practice, policy statements, etc. governing the use of IMSI Catchers would reveal operationally sensitive information about the scope of police activities and operations. This reasoning is not understood. It appears that the Warwickshire PCC has confused consideration of NCND with consideration of the provision of information itself;

28. Second, Privacy International submitted that the refusal failed to have regard to obviously

[11] *Galloway v Information Commissioner v The Central and North West London NHS Foundation Trust* (2009) 108 BMLR 50, at §70.
[12] *Magyar Helsinki Bizottság v Hungary*, European Court of Human Rights, App. No. 18030/11, 8 Nov. 2016.

material considerations, including, but not limited to:

a. The fact that the Warwickshire PCC's purchase of IMSI Catchers is already in the public domain, as set out in Privacy International's original request;

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

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

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

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

D. Decision in Response to Request for Internal Review

30. On 13 July 2017, the Warwickshire PCC responded by upholding the original decision.

31. With respect to the refusal to disclose the document responsive to questions 1-3 pursuant to section 24(1) FOIA, the Warwickshire PCC stated:

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

32. The Warwickshire PCC indicated that the responsive document would reveal "*the analysis of the current system in the Business Case in terms of what they operationally allow the police to do, and what different options for future systems would allow, and how they work functionally*" and that disclosure "*would give key knowledge to those who would seek to evade such systems and avoid coming to the attention of the police and other agencies who are entrusted with ensuring national security is protected*." The Warwickshire PCC concluded that "*there is indeed a clear basis for concluding that disclosure would have an adverse impact on national security*" and that the public interest in the protection from national security threats was stronger than the public interest case for releasing information.

33. Similarly, in reviewing the refusal to disclose the document responsive to questions 1-3 pursuant to section 31(1) FOIA, the Warwickshire PCC stated that "*the information contained within the Business Case, concerning the operation and functionality of the C[CD]C system as well as potential options for the future, do indeed lead to the conclusion that release of the information would, or would be likely to, prejudice the prevention or detection of crime and the apprehension or prosecution of offenders*." The Warwickshire PCC submitted that the release of the document would not "*lead to a mere theoretical prejudice*" and that "*[t]he information contained, in the hands of those who wish to evade law enforcement bodies, would make it easier to avoid attempts to undertake covert surveillance*." While the Warwickshire PCC acknowledged that it could not be "*absolutely certain that crime prevention and detection, and the apprehension and prosecution of offenders, would be adversely impacted by releasing details of the Business Case*", it considered it to be "*highly likely*". The Warwickshire PCC concluded that "*public interest in having knowledge of and understanding covert communications systems utilised by the police is outweighed by the public interest in prevention and detection of crime, as well as the apprehension and prosecution of offenders*."

34. With respect to the decision to NCND the existence of records responsive to question 4 pursuant to section 23(5) FOIA, the Warwickshire PCC began by noting that "*the section 23(5) exemption is clearly not appropriate with regard to*" legislation, which is "*produced and published by Parliament and Government in an open form*." However, the Warwickshire PCC further indicated that "*[r]elevant legislation, and anything else that is published in a public form, would fall under the section 21 exemption as being 'information accessible to the application by other means'*". But with respect "*to anything that does not fall within the section 21 exemption*," the Warwickshire PCC concluded that "*it is appropriate to use the provisions of section 23(5) to neither confirm nor deny the existence of any such documentation*." The Warwickshire PCC reasoned that "*this is clearly a request about matters related to national security, and the whole of section 23 is an absolute exemption*" and that "*[w]ith regard to there being a realistic possibility that a security body would be involved in the issue, given the nature of the CCDC equipment and the purposes for which it may be used, this is proven on the balance of probabilities*."

IV. The Appeal

A. The Purpose of FOIA

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

36. There is a high degree of consensus under international law that access to information is part of the right to freedom of expression. In particular, the Commissioner should have

regard to the Grand Chamber decision in *Magyar Helsinki Bizottság v Hungary*.[13] 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.[14]

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

> *"167. The manner in which public watchdogs carry out their activities may have a significant impact on the proper functioning of a democratic society. It is in the interests of democratic society to enable the press to exercise its vital role of 'public watchdog' in imparting information on matters of public concern (see Bladet Tromsø and Stensaas, cited above, § 59), just as it is to enable NGOs scrutinising the State to do the same thing. Given that accurate information is a tool of their trade, it will often be necessary for persons and organisations exercising watchdog functions to gain access to information in order to perform their role of reporting on matters of public interest. Obstacles created in order to hinder access to information may result in those working in the media or related fields no longer being able to assume their 'watchdog' role effectively, and their ability to provide accurate and reliable information may be adversely affected (see Társaság, cited above, § 38).*
>
> *168. Thus, the Court considers that an important consideration is whether the person seeking access to the information in question does so with a view to informing the public in the capacity of a public 'watchdog'."*

38. As a human rights organisation, Privacy International plays the role of a watchdog, similar to that played by the press.[15] 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.*"[16] Privacy International seeks to advance the right to privacy around the world, including in the UK. It carries out this

[13] *Magyar Helsinki Bizottság v Hungary*, European Court of Human Rights, App. No. 18030/11, 8 Nov. 2016.
[14] 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.
[15] *See Társaság a Szabadságjogokért v Hungary*, App. No. 37374/05, 14 April 2009.
[16] The United Kingdom's Observations on the Merits, *10 Human Rights Organisations v United Kingdom*, App. No. 24960/15, 14 April 2016, §6.1.

work, in part, by conducting research on a variety of issues related to privacy and surveillance and publishing that research in multiple formats, including research reports, policy papers and blog posts. It seeks information about IMSI Catchers in order to educate the public about the government's use of this surveillance technology and its human rights implications, including for the right to privacy.

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

B. Questions 1-3 – Sections 24(1) and 31(1)(a)-(b) FOIA

i. Section 24(1) FOIA

40. Pursuant to section 24(1) FOIA, information is exempt if exemption from section 1(1)(a) is required for the purpose of safeguarding national security.

41. The Commissioner has explained that consideration of the section 24(1) exemption "*involves two stages; first, the exemption must be engaged due to the requirements of national security. Secondly, this exemption is qualified by the public interest, which means that the information must be disclosed if the public interest in the maintenance of the exemption does not outweigh the public interest in disclosure*."[17]

42. The Warwickshire PCC has provided insufficient reasons for justifying why the section 24(2) exemption is engaged by the request. It does not inherently follow that disclosing the capabilities and uses of a particular technique or tool reveals information that would negatively impact national security. Furthermore, the Warwickshire PCC has presented no evidence of risk to support its position.

43. In carrying out the public interest test, the original decision identified as factors against disclosing the responsive document that "*disclosure…would undermine the strategic aims and deliberations in respect of the equipment by exposing them to opportunist criminals and terrorists who would seek to use the information to their advantage*" and "*[a]ny information which undermines the operational integrity and effectiveness of the OPCC's activities (and that of other agencies) would adversely affect public safety and this would*

[17] ICO, Decision Notice, Ref. FS50673315, 1 February 2018, para. 21, available at https://ico.org.uk/media/action-weve-taken/decision-notices/2018/2173166/fs50673315.pdf.

not be in the wider public interest." The review of the original decision reiterated these factors, noting that "*giving the public access to a document analysing both current and potential future CCPC capabilities and operational uses would raise a significant risk that it would both be seen by those who pose a threat to national security and would then be utilised to the detriment of the safety and security of British citizens*."

44. The original decision identified as factors in favour of disclosing the information that "*there is a public interest in how public funds are spent, and a natural concern to ensure that any measures in place to safeguard national security are effective, and further that any covert activities are proportionate to the risks that a public authority may be seeking to address*." It further noted that "*[w]hile there is a level of public awareness in this area, the exact nature of the discussions regarding the equipment or any associated issues, are not widely known*." The review of the original decision further noted that "*[t]he public interest case concerning the existence, deployment and functionality of CC[D]C equipment is indeed strong*".

45. The Warwickshire 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.

46. 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.

47. 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*".[18] As discussed

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

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

48. 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.[19] 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.

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

    a. Insufficient reasons have been provided as to why there is a public interest in failing to disclose the information held;

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

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

    d. Privacy International 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 Warwickshire Police have specifically been named in this regard.

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

ii. Section 31(1)(a)-(b) FOIA

50. Pursuant to section 31(1)(a)-(b) FOIA, information is exempt if disclosure would, or would be likely to, prejudice the prevention or detection of crime or the apprehension or prosecution of offenders.

51. The Commissioner has identified section 31 FOIA to be a "*prejudice-based exemption*" that is also "*qualified*" and "*therefore subject to the public interest test*." Accordingly, "*not only does the information have to prejudice one of the purposes listed but, before the information can be withheld, the public interest in maintaining the exemption must outweigh the public interest in its disclosure*."[20]

52. The Warwickshire PCC has provided insufficient reasons for justifying why the section 31(1) exemption is engaged by the request. Again, it does not inherently follow that disclosing the capabilities and uses of a particular technique or tool reveals information that would negatively impact law enforcement. Furthermore, the Warwickshire PCC has presented no evidence to demonstrate how any claimed prejudice is real, actual or of substance, or the likelihood that any claimed prejudice will be met.

53. In carrying out the public interest test, the original decision identified as the factors against disclosing the responsive document that "*disclosure…would prejudice the methods and strategies deployed or considered the OPCC in relation to the prevention and detection of crime and the apprehension or prosecution of offenders*", including by raising awareness "*particularly amongst those individuals involved in serious and organised crime or terrorism, and who would be best placed to exploit the information to their advantage*." The review of the original decision reiterated these factors, noting that the information "*in the hands of those who wish to evade law enforcement bodies, would make it easier to avoid attempts to undertake covert surveillance*" and that there is "*therefore a high chance of such information being likely to prejudice prevention and detection of crime, as well as the apprehension and prosecution of offenders*."

54. The original decision identified as the factors in favour of disclosing the responsive document that disclosure "*would serve to increase public awareness*" (while noting that it would do so "*particularly amongst those individuals involved in serious and organised crime or terrorism*") and that "*there is a public interest in disclosing information that holds public bodies to account, and increases transparency about how they perform their functions*."

55. As discussed above, the Warwickshire 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

[20] ICO, Decision Notice, Ref. FS50669281, 21 Nov. 2017, para. 16, available at https://ico.org.uk/media/action-weve-taken/decision-notices/2018/2173022/fs50669281.pdf.

expression and freedom of assembly and association.

56. Moreover, 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.

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

    a. Insufficient reasons have been provided as to why there is a public interest in failing to disclose the information held;

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

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

    d. Privacy International 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 Warwickshire Police have specifically been named in this regard.

C. Questions 4 – Sections 21 and 23(5) FOIA

a. Section 21 FOIA

58. By virtue of section 21 FOIA, there is an exemption to the disclosure of information under FOIA if that information is reasonably accessible to the applicant by other means.

59. The Information Commissioner's Office guidance on section 21 FOIA provides, as a general principle that:

> "*Although the information that is requested may be available elsewhere, a public authority will need to consider whether it is actually reasonable to the applicant*

before it can apply section 21. For example, the authority may still need to direct the applicant to where in the public domain the information can be found. Similarly, if the information is available to the applicant via another access regime, the authority should ensure that the applicant is familiar with the details of the regime and how it operates. In such ways, public authorities can demonstrate that section 21 is applicable and that the applicant has no right of access to the information via FOIA."[21]

60. Privacy International submits that pursuant to this guidance, the Warwickshire PCC has failed to sufficiently demonstrate the applicability of section 21 FOIA to legislation governing the use of IMSI Catchers. The Warwickshire PCC's response is limited to noting that "*[r]elevant legislation, and anything else that is published in a public form, would fall under the section 21 exemption*". First, the Warwickshire PCC fails to indicate what exactly constitutes "relevant legislation" or other relevant information "that is published in a public form". This information is necessary to direct Privacy International given that to Privacy International's knowledge IMSI Catchers are nowhere explicitly regulated by law. Second, the Warwickshire PCC fails to indicate where such "relevant legislation" or other information "that is published in a public form" can be found in the public domain.

b. Section 23(5) FOIA

61. By virtue of section 23(5) FOIA the duty to confirm or deny does not arise if, or to the extent that, compliance with section 1(1)(a) would involve the disclosure of any information, which was directly or indirectly supplied to the public authority by, or which relates to, any of the bodies specified in section 23(3).

62. 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*

[21] Information Commissioner's Office, Information reasonably accessible to the applicant by other means (section 21), para. 11.

information requested is within what could be described as the ambit of security bodies' operations, section 23(5) is likely to apply" and that *"[f]actors indicating whether a request is of this nature will include the functions of the public authority receiving the request, the subject area to which the request relates and the actual wording of the request.*" Finally, the Commissioner noted that "*there is clearly a close relationship between the police service and the security bodies*" and therefore, "*on the balance of probabilities, any information about its potential use of IMSI technology, if held, could be related to one of more bodies identified in section 23(3) of the FOIA*."[22]

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

    a. Privacy International's request relates to *policy guidance and other information* governing the use of IMSI Catchers held by the Warwickshire 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 Warwickshire 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 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 Warwickshire 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.

[22] 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.

F. Conclusion

64. For the reasons set out above, the ICO is respectfully invited to allow this appeal and to issue a decision notice directing the Warwickshire PCC to comply with its obligations under section 1(1) FOIA and (1) communicate information of the description specified in questions 1-3 of the request (2) inform Privacy International whether it holds information of the description specified in question 4 of the request and communicate that information.

16 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

Philip Seccombe
Police and Crime Commissioner for Warwickshire
3 Northgate Street
Warwick CV34 4SP

1 November 2016

Dear Mr. Seccombe,

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 Warwickshire police forces.

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

Specifically, the minutes record that three options relating to "CCDC replacement" were discussed:

> "Option 1 – Upgrading the existing equipment with the current supplier.
> Option 2 – Replacing the existing equipment with the current supplier's new product.
> Option 3 – Replacing the existing equipment with a new supplier."

The minutes go on to observe that: "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 in option 3." The Minutes indicate that the following decision was made: "**Both PCCs [West Mercia and Warwickshire Police and Crime Commissioners] agreed to Replacing the existing equipment with a new supplier."**

Privacy International requests the following records:

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

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

[1] https://thebristolcable.org/2016/10/imsi/
[2] https://thebristolcable.org/wp-content/uploads/2016/10/09-imsi-4.pdf

3. Records relating to the decision "to Replace[ ] the existing [CCDC] equipment with a new supplier", referred to in the Alliance Governance Group minutes above, including any records referred to or consulted in reaching that decision.

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

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 EC15 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

Police and Crime Commissioner Warwickshire

Warwickshire Office of the PCC
3 Northgate Street
Warwick
CV34 4SP

PHILIP SECCOMBE TD
Police and Crime Commissioner

Tel: 01926 412322
E-mail: OPCC@warwickshire.gov.uk

20 December 2016

Sent via email
matthew@privacyinternational.org

Mr M Rice
Advocacy Officer
Privacy International
62 Britton Street
LONDON
EC15 5UY

Dear Mr Rice

FREEDOM OF INFORMATION ACT 2000 – INFORMATION REQUEST

Your request for information has now been considered.

Unfortunately the Office of the Police and Crime Commissioner (OPCC) is unable to comply with it. The information you requested relates to Covert Communications Data Capture (CCDC) equipment and comprises of four questions, which are summarised for ease, as follows:

1. Records relating to the purchase of existing CCDC equipment;
2. Records relating to the purchase of replacement CCDC equipment;
3. Records relating to the decision to replace existing equipment with a new supplier; and
4. Legislation, codes of practice, policy statements etc governing the use of CCDC equipment.

As indicated in our letter dated 29 November 2016, the information you have requested is subject to qualified exemptions, which means that the OPCC must consider whether it is in the public interest to release the information. We have now considered the public interest and concluded that we are unable to release the information to you and have explained our reasoning below.

In relation to questions 1-3 we hold a small amount of information namely a business case regarding the replacement of existing CCDC equipment. However, this is exempt from disclosure under section 24(1) (national security) and section 31(a) and (b) (law enforcement) of the Act.

Please note that in our previous letter we referred to section 30(1) (a) and (b) which was a typo on our part and the correct statutory citation appears above.

/continued . . .

Section 24(1) provides that information is exempt from disclosure if the exemption is required for the purposes of safeguarding national security. The document in question is a confidential strategic paper, it was produced to evaluate the functionality and options in respect of existing and replacement CCDC equipment, and if disclosed would undermine national security.

We recognise that there is a public interest in how public funds are spent, and a natural concern to ensure that any measures in place to safeguard national security are effective, and further that any covert activities are proportionate to the risks that a public authority may be seeking to address. While there is a level of public awareness in this area, the exact nature of the discussions regarding the equipment or any associated issues, are not widely known. There is an inherent public interest in safeguarding national security to ensure the safety of the UK. The disclosure of this information would undermine the strategic aims and deliberations in respect of the equipment by exposing them to opportunist criminals and terrorists who would seek to use the information to their advantage. Any information which undermines the operational integrity and effectiveness of the OPCC's activities (and that of other agencies) would adversely affect public safety and this would not be in the wider public interest. Therefore, after due consideration, and on balance, we consider that the public interest favours maintaining this exemption.

Section 31(1) provides that information is exempt if disclosure would, or would be likely to, prejudice (a) the prevention or detection of crime or (b) the apprehension or prosecution of offenders. The disclosure of this document would prejudice the methods and strategies deployed or considered by the OPCC in relation to the prevention and detection of crime and the apprehension or prosecution of offenders. As mentioned, although there is now a level of public awareness in this area, the exact nature of the discussion regarding the equipment and any associated issues is not openly discussed. While the disclosure of this document would serve to increase public awareness, it would do so particularly amongst those individuals involved in serious and organised crime or terrorism, and who would be best placed to exploit the information to their advantage.

In addition to the public interest factors mentioned in respect of section 24(1), we recognise there is a public interest in disclosing information that holds public bodies to account, and increases transparency about how they perform their functions. However, there is an inherent public interest in both protecting society from the impact of crime and preserving the integrity of the OPCC's law enforcement activities in this area. The disclosure of this information would serve to provide a greater understanding to opportunist criminals and terrorists, as to the OPCC's strategic aims and deliberations regarding the use of such equipment, including any associated issues, the detail of which is not openly discussed in order to maintain operational effectiveness. Furthermore, the OPCC requires a safe space in which to explore and evaluate its operational activities, in the absence of external scrutiny. The disclosure of this information would hinder the effective conduct of the OPPC's functions (and that of other agencies) with regard to the prevention or detection of crime and the apprehension or prosecution of offenders for fear that such information may enter the public domain. Therefore, after due consideration, and on balance, we consider that the public interest favours maintaining this exemption.

Finally, section 23(5) (security bodies) provides that the duty to confirm or deny whether information is held does not arise if this would disclose information relating to a security body. We consider that this exemption is engaged in respect of question 4 and as such the OPCC can neither confirm nor deny whether information falling under this aspect your request is held, as to do so would undermine the operational effectiveness of national security and law enforcement. This is an absolute exemption which means there is no requirement to consider the public interest

/continued . . .

You have the right to request that the OPCC carry out an internal review if you are not satisfied with the way your request was dealt with or wish to appeal the decision. A request for an internal review should be made in writing and addressed to me at the address above. All requests for an internal review will be dealt with under the OPCC's internal review procedure.

In accordance with section 17 of the Freedom of Information Act 2000 please treat this letter as a Public Interest Refusal Notice.

If you are not satisfied with the outcome of the internal review you may appeal to the Information Commissioner's Office, at the following address:

FOI Compliance Team (complaints)
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Yours sincerely

Philip Seccombe TD
Police and Crime Commissioner

EXHIBIT C

PRIVACY INTERNATIONAL

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

22 May 2017

SENT VIA EMAIL

Philip Seccombe
Warwickshire Police and Crime Commissioner
3 Northgate Street
Warwick CV34 4SP

Re: Freedom of Information Request (Ref. No. PCC16 FOI 11/01)

A. Introduction

1. This is an appeal following a refusal to disclose information made by the Warwickshire Office of the Police and Crime Commissioner ("OPCC") on 20 December 2016. Privacy International respectfully requests an internal review of the decision.

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

B. The Background

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

4. The request referred to a recent article by a journalist collective making 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. The request further specified that the minutes indicate that Warwickshire PCC agreed to replace existing CCDC equipment with a new supplier.

5. The request stated that mobile phone surveillance equipment can be referred to using a range of other terms, including "Covert Communications Data Capture ("CCDC") equipment", "IMSI Catchers", "IMSI Grabbers", "Cell site simulators" and "Stingrays". For the purposes of this appeal, Privacy International refers to such equipment as "IMSI catchers".

6. Privacy International requested the following records:

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

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

3. Records relating to the decision "to Replace[ ] the existing [CCDC] equipment with a new supplier", referred to in the Alliance Governance Group minutes . . . including any records referred to or consulted in reaching that decision.

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

C. The Refusal

7. On 29 November 2016, the Warwickshire PCC refused the request. The refusal summarised our request as follows:

7.1 Records relating to the purchase of existing CCDC equipment;

7.2 Records relating to the purchase of replacement CCDC equipment;

7.3 Records relating to the decision to replace existing equipment with a new supplier; and

7.4 Legislation, codes of practice, policy statements etc governing the use of CCDC equipment.

8. The refusal relied on ss.23(5), 24(1), and 31(a) and (b) Freedom of Information Act 2000.

9. In relation to the first three items summarised above, the refusal provides that the OPCC holds a small amount of information, namely a business case regarding the replacement of existing CCDC equipment. However, the refusal concludes that this information is exempt under sections 24(1) and 31(1)(a) and (b) and provides the following:

    9.1 Section 24(1) provides that information is exempt from disclosure if the exemption is required for the purposes of safeguarding national security. The document is a confidential strategic paper, produced to evaluate the functionality and options in respect of existing and replacement CCDC equipment, and if disclosed would undermine national security.

    9.2 That disclosure of this information would undermine the use of the equipment by exposing the strategic aims and deliberations in respect of it to criminals and terrorists who would seek to use the information to their advantage. On balance, it was considered that the public interest favours maintaining this exemption.

    9.3 Pursuant to section 31(1)(a) and (b), disclosure of the document would prejudice the methods and strategies deployed or considered by OPCC in relation to the prevention and detection of crime and the apprehension and prosecution of offenders. The refusal states "*[w]hile the disclosure of this document would serve to increase public awareness, it would do so particularly amongst those individuals involved in serious and organised crime or terrorism, and who would be best placed to exploit the information to their advantage*."

    9.4 Disclosure of the information would hinder the effective conduct of the OPCC's and other agencies' functions. On balance, it was considered that the public interest favours maintaining this exemption.

10. With regards to the fourth item, the Refusal relies on section 23(5) and considers that the OPCC can neither confirm nor deny whether this information is held since to do so would:

    10.1 Undermine the operational effectiveness of national security and law enforcement.

D. The Appeal

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

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

    11.2 It is therefore clear that a decision to refuse disclosure requires a clear justification and merits close scrutiny. This is because it flies in the face of the "*default setting*" in the Freedom of Information Act 2000, which is in favour of disclosure.[2] It also flies in the face of the Article 10 right to receive information, as recently confirmed by the European Court of Human Rights;[3]

NCND: Legislation, codes of practice, policy statements etc governing the use of CCDC equipment

12. With respect to the fourth item, the reason provided by the OPCC, as set out above, fails to justify the application of NCND in this case. This is for the following four reasons.

13. Firstly, the OPCC response is predicated on a *non-sequitur*:

    13.1 It simply does not follow that merely confirming or denying the existence of legislation, codes of practice, policy statements, etc. governing the use of IMSI catchers would reveal operationally sensitive information about the scope of police activities and operations. This reasoning is not understood. It appears that the OPCC has confused consideration of "*neither confirm nor deny*" with consideration of the provision of information itself.

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

    14.1 The fact that the OPCC's purchase of IMSI catchers is already in the public domain, as set out in Privacy International's original request;

---

[1] *Philip Kalman v Information Commissioner and the Department of Transport* (EA/2009/111 8 July 2010).
[2] *Galloway v Information Commissioner v The Central and North West London NHS Foundation Trust* (2009) 108 BMLR 50, at §70.
[3] *Magyar Helsinki Bizottság v Hungary* (App. no. 18030/11).

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

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

15. Thirdly, when considered forensically, the exemption under Section 23(5) does not apply.

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

Public Interest: Records relating to the purchase of existing and replacement CCDC equipment and relating to the decision to replace existing equipment with a new supplier

16. The public interest balancing exercise falls squarely in favour of disclosure of the first to third categories of records:

16.1 No meaningful reasons have been provided as to why there is a public interest in failing to disclose the information held;

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

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

16.4 The refusal recognizes that "*there is a public interest in how public funds are spent, and a natural concern to ensure that any measures in place to safeguard national security are effective, and further that any covert activities are proportionate to the risks that a public authority may be seeking address.*" Despite these factors, the request was refused on the basis of assertions.

E. Conclusion

17. Privacy International respectfully requests the Warwickshire OPCC to re-consider the original request made for information as set out above.

Scarlet Kim

Legal Officer
Privacy International

EXHIBIT D

Philip Seccombe
Police and Crime Commissioner
for Warwickshire

13 July 2017

Warwickshire Office of the PCC
3 Northgate Street
Warwick
Warwickshire CV34 4SP

Neil Hewison
Chief Executive

Tel: 01926 412118
E-mail: neilhewison@warwickshire.gov.uk

Scarlet Kim
Legal Officer
Privacy International
62 Britton Street
LONDON
EC1M 5UY

Dear Madam

Appeal re FOI Request (Ref. No. PCC16 FOI 11/01) - Request for an Internal Review

I write with reference to your request for an internal review dated 22 May 2017 following the Office of the Police and Crime Commissioner (OPCC) response to your freedom of information request dated 1 November 2016. Please find attached a report that has been completed by Warwickshire Legal Services (WLS) setting out the findings of the internal review that they have conducted on the OPCC's behalf. The OPCC acknowledges that there has been a short delay in responding to Privacy International, however, we are aware that WLS has kept you informed and apologised for the delay. For the reasons set out in the report, the OPCC does not uphold your appeal, except in relation to one aspect of the fourth part of your request. If you are not satisfied with the outcome of the internal review you may appeal to the Information Commissioner's Office, at the following address:

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

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

Yours faithfully

Neil Hewison
Chief Executive

Enc

Internal Review Report – Freedom of Information Act 2000

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

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

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

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

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

How the request was dealt with

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

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

The response, sent out on 20th December 2016, made clear that in relation to the first three queries a Business Case document was held but nothing else, and that disclosure of the Business Case was exempt under section 24(1) and sections 31(a) & (b) of the Freedom of Information Act 2000 ("the Act"), on the grounds that (a) the document is a confidential strategic papers produced to evaluate the functionality and options in respect of existing and replacement CCDC equipment, and if disclosed would undermine national security; and (b) the disclosure of the document would prejudice the methods and strategies deployed or

considered by the OPCC in relation to the prevention and detection of crime and the apprehension or prosecution of offenders. The response also went in some detail on the public interest test but considered that, on balance, the public interest in maintain national security and the prevention and detection of crime outweighed, in relation to release of this document, the public interest in how public funds are spent, whether measures in place to safeguarding national security are effective, and in ensuring that transparency exists and public bodies are held to account.

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

Analysis of Response

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

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

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

Scope of this Internal Review

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

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

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

- Confirmation or denial of the existence of legislation, codes of practice, policy statements etc. would not reveal operationally sensitive information;
- There is a failure to have regard or give adequate weight to the fact that material is already in the public realm, that there is significant public interest in the area, and that legislative provisions and/or policy guidance cannot conceivably fall within any exemption; and
- There has to be a realistic possibility that a security body would be involved in the issue for the exemption to apply.

Review of First, Second and Third Parts

National Security

Section 24(1) of the Freedom of Information Act 2000 states that “Information which does not fall within section 23(1) is exempt information if exemption from section 1(1)(b) is required for the purpose of safeguarding national security”. As the request for the internal review makes clear, the words “required for the purpose of” are indeed critical when

considering whether this exemption applies. The Information Commissioner's guidance on use of the exemption states as follows:

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

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

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

Conclusions

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

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

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

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

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

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

(a) the prevention or detection of crime,

(b) the apprehension or prosecution of offenders"

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

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

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

"Deciding whether the prejudice would occur or is only likely to occur is important. The more certain the prejudice, the greater weight it will carry when considering the public interest. In this context the term "would prejudice" means that it has to be more probable than not that the prejudice would occur. "Would be likely to prejudice" is a lower test; there must be a real and significant risk, even if risk of prejudice occurring is less than 50 per cent".

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

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

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

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

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

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

Conclusions

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

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

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

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

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

Review of Fourth Part

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

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

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

(3) The bodies referred to in subsections (1) and (2) are—
(a) the Security Service,

(b) the Secret Intelligence Service,
(c) the Government Communications Headquarters,
(d) the special forces,
(e) the Tribunal established under section 65 of the Regulation of Investigatory Powers Act 2000,
(f) the Tribunal established under section 7 of the Interception of Communications Act 1985,
(g) the Tribunal established under section 5 of the Security Service Act 1989,
(h) the Tribunal established under section 9 of the Intelligence Services Act 1994,
(i) the Security Vetting Appeals Panel,
(j) the Security Commission,
(k) the National Criminal Intelligence Service,
(l) the Service Authority for the National Criminal Intelligence Service,
(m) the Serious Organised Crime Agency,
(n) the National Crime Agency, and
(o) the Intelligence and Security Committee of Parliament.

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

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

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

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

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

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

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

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

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

Conclusion

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

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

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

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

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

Guy Darvill
Warwickshire Legal Services

EXHIBIT E

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

I. Introduction

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

II. A Summary of US Freedom of Information Laws

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

---

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

III. FOIA Requests to Federal Agencies for IMSI Catcher Records

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

A. Electronic Privacy Information Center – FBI

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

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

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

---

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

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

C. American Civil Liberties Union – Various Federal Agencies

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

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

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

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

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

---

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

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

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

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

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

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

A. Florida

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

Florida Department of Law Enforcement ("FDLE")

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

Tallahassee Police Department ("TPD")

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

Miami-Dade Police Department

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

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

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

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

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

B. New York

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

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

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

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

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

The records disclosed by the RPD include:

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

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

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

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

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

C. Michigan

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

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

D. CityLab

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

6 February 2018 Privacy International

---

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