Reference: 278375

17 June 2016

Julia Snape
Information requests

information.requests@ofcom.org.uk

Freedom of Information Act 2000 (the "Act")

Thank you for your request of 24 May for information about IMSI catchers. We have considered it under the Act.

Your request

Your request said:

"*Recently it has come to light that the Scottish Prison Service are operating an IMSI Catcher at HMP Shotts.*

https://www.documentcloud.org/documents/2842174-HQ-16022-a-Tibbitt.html

According to the SPS, there is a Memorandum of Understanding agreement between the SPS, Ofcom and mobile phone operators that governs the operation of the device. In light of this information, I'd be grateful if you could supply me with the following:

1. A copy of the MOU agreement described in the SPS document linked to above.
2. Details of any correspondence, reports or memos between Ofcom and the SPS that relate to the operation of the IMSI catchers installed at HMP Shots and HMP Glenochil.
3. Copies of any similar MOU agreements that exist between Ofcom, other public agencies and mobile phone operators that relate to the operation IMSI catchers at other sites in the UK."

Ofcom's response

We hold information falling within each part of your request and provide you with:

1. a redacted copy of the MoU between Ofcom, the Scottish Prison Service ("SPS") and mobile network operators ("MNOs");

2. redacted copies of some correspondence between Ofcom and the SPS relating to the operation of the IMSI catcher at HMP Shots; and

3. a redacted copy of the MoU between Ofcom, the Ministry of Justice ("MoJ") and MNOs.

Some information we hold falling within the second part of your request is withheld. That information and the information redacted from the disclosed correspondence is withheld on the basis of the exemptions in sections 31(1)(f) and 40(2) of the Act.

We do not hold information falling within your request relating to HMP Glenochil.

The exemptions

Section 31(1)(f) of the Act says:

"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—…

….(f) the maintenance of security and good order in prisons or in other institutions where persons are lawfully detained…"

This is a qualified exemption, subject to a public interest test. Broadly, this means that the information should only be withheld under the exemption where the public interest in doing so outweighs that in favour of disclosure.

Section 40(2), meanwhile, provides that personal data which relates to persons other than the requester is exempt where, amongst other things, its disclosure would contravene any of the data protection principles in the Data Protection Act 1998 (the "1998 Act"). Those principles include that personal data must be processed fairly and lawfully. This is an absolute exemption. It is not subject to such a public interest test.

Information withheld

These parts of the MoUs have been withheld under the exemptions stated:

- paragraphs 13, 17, 18 and the 7th bullet of paragraph 26 - withheld under section 31(1)(f);

- the names and signatures of signatories from Ofcom and the MNOs - under section 40(2);

- Annex A, which relate to technical information about the equipment concerned - under section 31(1)(f); and

- Annex B, which includes the single points of contact for each of the signatory organisations - under section 40(2).

Parts of the correspondence with the SPS have also been withheld under section 31(1)(f) and the names of the individuals who wrote or received it are withheld under section 40(2).

Applying the exemptions – s.31(1)(f)

The information redacted from the MoUs is technical information relating to the way the relevant mobile signal blocking technology operates. Information withheld in the relevant correspondence is also information about the operation of the ISMI catcher at HMP Shotts. In both cases, the information is withheld on the basis that releasing it would prejudice the maintenance of security and good order in prisons, under section 31(1)(f), since it would make public information that could be used to avoid the effects of the relevant technology and facilitate the unlawful use of mobile phones in prisons.

The public interest test we have undertaken on the application of Section 31(1)(f) is attached at Annex A.

Applying the exemptions – s.40(2)

The copies of the MoUs that Ofcom holds contain personal data, including the names and signatures, relating to signatories from Ofcom, the SPS, the MoJ and the MNOs. They also include the names and contact details of individuals from those organisations who are designated to act as their points of contact for matters relating to the MoU. All of that data, apart from the name and signature of the Chief Executive of the SPS, has been redacted under the exemption in s.40(2) of the Act.

The redacted information is personal data under the 1998 Act. That Act defines "personal data" as including data which relate to a living individual who can be identified from it. Relevant case law has clarified the definition further, setting out that personal data is information that affects the privacy of the subject, whether in their personal, business or professional capacity.[1] The relevant names and contact details here fall within that definition.

Ofcom may only process that data (which includes disclosing it) where doing so is in accordance with the data protection principles in the 1998 Act. Where doing so would contravene those principles, Ofcom may not process the data and it is exempt from disclosure under s.40(2) of the Act.

As noted above, one of the data protection principles is that personal data must be processed fairly and lawfully. In this case, my view, after careful consideration taking account of guidance published by the Information Commissioner,[2] is that disclosing the withheld personal data would contravene that principle.

In particular, my view is that those individuals to whom the personal data relates would not expect that that information might be disclosed to others in the context of an MoU. Further, I also consider that disclosure would cause unnecessary or unjustified distress or damage to those individuals.

Of the Ofcom officers whose personal data is redacted, one is a member of Ofcom's Senior Management Group ("SMG") and the others are less senior. In some contexts, the SMG member might expect their name to be disclosed as a publicly accountable ambassador for

---

[1] See *Durant v FSA* [2003] EWCA Civ 1746, para 28.
[2] See, in particular, https://ico.org.uk/media/for-organisations/documents/1187/section_40_requests_for_personal_data_about_employees.pdf

Ofcom. However, I do not consider that is so here, nor for the other Ofcom officers.

Rather, disclosure of the redacted information would suggest those individuals hold information about the use of mobile phone signal blocking technology in prisons. That is something outside the scope of their ordinary duties as Ofcom officers, and disclosure would expose them to a risk of being targeted by wrongdoing individuals to whom such information may be useful for unlawful purposes relating to the use of mobile phones in prisons. I do not consider any Ofcom officers would expect their personal data to be disclosed where such a risk arises, and they are liable to be caused unnecessary or unjustified distress or damage were such disclosure made.

My further view is that a similar position applies to the personal data of the MNOs' signatories. Their roles are to represent their employers in matters relating to their businesses of operating mobile phone networks, not to be held responsible for security measures in prisons.

In both cases, this contrasts with the position of the SPS's CEO. In my view, he would be expected to hold information about security measures in prisons. Similarly, he would expect to be held accountable for such measures and he would not, I think, be exposed to risk or distress by disclosure of his name and signature in this context.

I hope you find the information provided useful.

Kind regards

Julia Snape

If you are unhappy with the response or level of service you have received in relation to your request from Ofcom, you may ask for an internal review. If you ask us for an internal review of our decision, it will be treated as a formal complaint and will be subject to an independent review within Ofcom. We will acknowledge the complaint and inform you of the date by which you might expect to be told the outcome.
The following outcomes are possible:
• the original decision is upheld; or
• the original decision is reversed or modified.

Timing
If you wish to exercise your right to an internal review **you should contact us within two months of the date of this letter**. There is no statutory deadline for undertaking internal reviews and it will depend upon the complexity of the case. However, we aim to conclude all such reviews within 20 working days, and up to 40 working days in exceptional cases. We will keep you informed of the progress of any such review. If you wish to request an internal review, you should contact:

Steve Gettings
The Secretary to the Corporation
Ofcom
Riverside House
2a Southwark Bridge Road
London SE1 9HA

If you are not content with the outcome of the internal review, you have the right to apply directly to the Information Commissioner for a decision. The Information Commissioner can be contacted at:
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Section 31(1)(f): Law Enforcement

Section 31 exempts information if disclosure would or would be likely to prejudice, among other things:

- *the maintenance of security and good order in prisons or in other institutions where persons are lawfully detained.*

Section 31 is subject to a public interest balance.

Factors for disclosure	**Factors for withholding**
• The public have an interest in knowing that prisons operate a robust security regime and are alert to smuggling and possession of contraband items and the technologies used to combat these threats. • They similarly have an interest in seeing that relevant safeguards and protections are in place with regard to the effects of the relevant technology on mobile phone signals inside and outside prisons.	• The presence of illicit mobile phones in prisons presents a serious risk to their security and the safety of the public. They can be used for a variety of criminal purposes and are associated with drug trafficking, violence and bullying in prisons. • Releasing operational details about the use and deployment of those technologies would be likely to aid the subversion of the effective use of the equipment. It would, for example, indicate the extent to which relevant technologies may be used. • Likewise, releasing sensitive correspondence that may include information about the technology deployed, the way it works and the steps the prison services, Ofcom and the MNOs may take in relation to its operation, may alert prisoners and others to the workings of the security arrangements in place. That would help in circumventing those arrangements. • Each of these consequences, or likely consequences, is against the public interest, in light of the illegality of mobile phone use in prisons and the ways mobile phones are liable to be used there. • There is also an important public interest in the relevant public authorities and MNOs being able to co-operate effectively in putting in place security measures and safeguards for the public. This may be undermined if information which is liable to have harmful effects on security and good

	order is disclosed.
Reasons why public interest favours withholding information	
• There are some good reasons for releasing information of the relevant kinds to the public. We have carefully considered those and made some disclosures in response to this request. However, it is strongly against the public interest to disclose the information withheld under section 31(1)(f) where to do so would aid the unlawful use of mobile phones in prisons and have (or likely have) the kinds of consequences outlined in the right hand column above.	