Reference: 01555327

Temiloluwa Dawodu
Information Rights Advisor
information.requests@ofcom.org.uk

10 February 2023

## Freedom of Information: Right to know request

Thank you for your request for information in relation to the location of active mobile phone sites in the United Kingdom. We received this request on 16 January 2023. We have considered it under the Freedom of Information Act 2000 (the "FOI Act") and the Environmental Information Regulations 2004 (the "EIR").

## Your request and our response

*I understand that MNOs report information of active transceiver sites across the UK to Ofcom as part of their obligations. I believe this information falls under the realm of the Freedom of Information Act.*

*I would like to request information about:*

1. *the locations of mobile phone transceiver sites within the UK under the Freedom of Information Act*

*I do understand, based on previous EIR requests about 5G in particular, that, "Ofcom does not hold information about MNO's plans for where and when they may deploy 5G." I would like to note that this is carefully worded to specify that you do not have information about MNO's future deployment plans. For clarification, I am not interested in future plans, but current deployments.*

Whilst we do hold information within the scope of your request, this information is exempt under section 39 of the FOI Act. The effect of section 39 is that it exempts information relating to the environment from disclosure under the FOI Act. Requests for such information should be processed in accordance with the EIR. Ofcom considers your request to relate to environmental information within the scope of the EIR and has therefore considered your request under the EIR.

The EIR provides that a public authority may refuse to disclose environmental information requested to the extent, amongst other things, that its disclosure would adversely affect international relations, defence, national security or public safety (regulation 12(5)(a) of the EIR), and in all the circumstances of the case, the public interest in maintaining the exception outweighs the public interest in disclosing the information.

Ofcom has considered your request in light of the relevant statutory scheme. We have also considered advice from HM Government as to the potential implications of disclosure of the location of mobile sites on national security matters. HM Government has raised significant concerns with Ofcom about the release of such information on national security grounds and has advised that disclosure of the information would adversely affect national security.

Taking this into account, Ofcom considers that regulation 12(5)(a) of the EIR is engaged; specifically, that disclosure of the information would adversely affect national security.

In applying this exception, Ofcom has balanced the public interest in withholding the information against the public interest in disclosing it and decided that in all the circumstances of the case the public interest in maintaining the exception outweighs the public interest in disclosure. In assessing this, under regulation 12(2), we have also applied a presumption in favour of disclosure. Annex A sets out the exception in full, as well as the factors we considered when deciding where the public interest lay.

*2) the "operator data" used to calculate figures for the Connected Nations 2022 report:*

*a) which operators do you receive data from*

*b) what data do you receive (e.g., projected/real RSRP metrics, site locations, coverage by frequency, etc.)*

*b i) if the data you receive is different for each operator, please specify this and clarify what data is provided by each operator.*

*Ofcom appear to have at least some information about mobile network sites and coverage as it is used in the annual Connected Nations reports. I understand that Ofcom worked with Opensignal to obtain data for the Connected Nations reports, but this does not appear to match the "operator data" source detailed in the reports.*

Please see paragraphs A1.37 – A1.49 of our Connected Nations Methodology Annex.

Paragraph A1.37 states: “Our data on the coverage of mobile networks was collected from the four mobile network operators, EE, Virgin Media O2, Three and Vodafone (see mobile network operators in our section on Obtaining information from providers) as 100m x 100m pixels referenced against the Ordnance Survey Great Britain (OSGB) grid system.”

This information is predicted coverage (see A1.47): “The mobile coverage figures provided in this report rely on the accuracy of coverage prediction data supplied by the mobile operators. We note that operators continue to update and improve their prediction models, which is welcome.”

This information is collected every month in a consistent format from all operators and is used to update the data underlying our checker (Mobile and Broadband checker - Ofcom) as well as informing the outputs associated with the Connected Nations publications (e.g. Interactive charts and Open Data files).

As indicated in A1.47 we also carry out drive testing and other due diligence activities that supports the findings of our Connected Nations reports. For details of additional information published in the

Connected Nations report that we obtain from mobile network operators, such as reported reliability incidents, please see the respective sections in the report.

Finally, please note that Opensignal have provided us with access to a crowdsourced dataset. This allows us to assess the latest view of mobile network performance from the consumer's perspective. Within our Connected Nations report we have only used Opensignal data in the section titled "Developing insights into the quality of mobile network performance" (pages 39 to 41). Further explanation of the approach used with this crowdsourced data can be found in the associated Methodology Annex.

*3) What national security risks are there in regards to disclosing mobile network transceivers to the general public?*

*I would like to note that in the past Ofcom have denied requests similar to mine under the guise of "national security" reasons due to internet service being part of Critical National Infrastructure (CNI). If this is the case, would the publication of other similar datasets not also fall under this reasoning?*

*For example, your website details a list of (a) all TV transmitters in the UK (Television transmitter location maps - Ofcom), (b) radio transmitters in the UK (Coverage - Ofcom), and (c) information about and locations of point-to-point links (Spectrum information portal - Ofcom).*

*3 b) How do the above datasets present a lower risk to national security than mobile network transceiver locations?*

Government has not raised national security risks with Ofcom in relation to what we publish in relation to these other datasets. Different risks may apply depending on the type of dataset and the form in which it is published (including the specificity of any location-based data). The national security risks identified by Government in relation to mobile sites are set out in Annex A below.

I hope this information is helpful. If you have any queries, then please contact information.requests@ofcom.org.uk. Please remember to quote the reference number above in any future communications.

Yours sincerely,

Temiloluwa Dawodu

If you are unhappy with the response you have received in relation to your request for information and/or consider that your request was refused without a reason valid under the law, you may ask for an internal review. If you ask us for an internal review of our decision, it will be subject to an independent review within Ofcom.

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 responding to 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 information.requests@ofcom.org.uk.

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

**Annex A**

**Regulation 12(5)(a) of the Environmental Information Regulations 2004**

**The exception**
*Regulation 12(5)(a) of the Environmental Information Regulations 2004 – a public authority may refuse to disclose information to the extent that its disclosure would adversely affect international relations, defence, national security or public safety.*
The regulation is engaged because disclosure of this information would adversely affect national security.
**The public interest test**
Regulation 12(5)(a) is subject to the public interest test.
Key points:
Ofcom can refuse to disclose information under this exception only if in all the circumstances of the case the public interest in maintaining the exception outweighs the public interest in disclosing the information. In assessing this, under regulation 12(2), Ofcom must also apply a presumption in favour of disclosure.
In carrying out the public interest test, Ofcom should consider the arguments in favour of disclosing the information and those in favour of maintaining the exception, attaching the relative weight to each argument (for and against disclosure) to decide where the balance of public interest lies.
We have set out the matters Ofcom have considered in reaching its decision with respect to the public interest below.

| Factors for disclosure | Factors for withholding |
|---|---|
| • **Transparency:** There is always a general public interest in transparency. The EIR implements EU Directive 2003/4/EC on public access to environmental information. Recital 1 of the preamble to the Directive states this public interest:<br><br>*"Increased public access to environmental information and the dissemination of such information contribute to a greater awareness of environmental matters, a free exchange of views, more effective participation by the public in environmental decision-making and, eventually, to a better environment."* | HM Government has advised Ofcom that:<br>• Disclosure of this information raises significant concerns on national security grounds and would adversely affect national security.<br><br>• Specifically, disclosure would create an increased threat to the UK's Critical National Infrastructure (CNI). CNI is those critical elements of infrastructure (including assets, facilities, systems, networks or processes), the loss or compromise of which could result in major detrimental impact on the confidentiality, integrity, and availability of networks, or delivery of essential |

| | |
|---|---|
| • **Accountability:** Mobile sites produce electromagnetic fields (EMF) or radio waves. At high enough levels, EMF can impact public health. As a result, the UK Health Security Agency (previously known as Public Health England (PHE)), an expert health body, advises that spectrum users should ensure that EMF levels comply with the internationally agreed levels in the ICNIRP Guidelines. Some individuals may have concerns about the potential health effects of EMF and want to know the location of any mobile site in their local area and whether the EMF levels from such mobile sites comply with the levels in the ICNIRP Guidelines.<br><br>• **Information already in the public domain:** Some local planning authorities have published information on the location of mobile sites (including on proposed sites). Information on mobile site locations is also available on some open source websites and mobile network operators' (MNOs) websites may indicate the general location of some masts (as well as future roll-out plans).<br><br>• The location of mobile sites and other technical data is published in some other countries including in Ireland and France.[1] | services (including those of the emergency services).<br><br>• Government has strong concerns about publishing the requested information and has advised that publishing mobile site information constitutes a security risk.<br><br>• Government's concerns centre on four areas:<br><br>1. **Espionage / sabotage:** Publishing the requested information could enable an attacker to remotely survey which mobile sites would be of interest from an espionage, sabotage or disruption perspective.<br><br>2. **Jamming:** Publishing the requested information could enable the jamming of radio signals.<br><br>3. **Physical security:** Information relating to hub sites (mobile sites that act as their own radio coverage site and also serve to 'daisy chain' other sites), switch sites, and data centres would be of particular concern from a national security perspective. The physical security of hub sites will become even more important as features such as Mobile Edge Computing become widely available.<br><br>4. **Developments in emergency services communications:** In the future, knowledge of commercial networks could help enable an attacker to target the UK's emergency service communications network to a degree that knowledge would not have enabled in the past. This is due to the Emergency Services Network programme switching emergency service communication from the private Airwave network to a commercial network. |

[1] http://siteviewer.comreg.ie/#explore (Ireland); https://www.cartoradio.fr/index.html#/cartographie/stations (France)

| | |
|---|---|
| | • Government acknowledges that detailed technical information is not requested, making such an attack more difficult. However, site location provides the starting point for an attack to gain and build additional and more detailed information that may then make any subsequent attack more likely to succeed.<br><br>• Current open source options are of much more limited use to a potential attacker than the data being requested - the data set being requested has the potential to be more damaging due to both its granularity and authoritative status.<br><br>Taking into account the factors in favour of disclosure, we have also taken into account the following:<br>• Some of the publicly available data (such as local planning data) has not been updated for several years and is likely to be inaccurate and incomplete. Further, MNOs' websites only provide general location information and do not disclose specific site locations.<br><br>• On accountability, we do not set EMF safety levels but we do carry out proactive testing of EMF levels near to mobile sites to check they comply with the internationally agreed levels in the ICNIRP Guidelines. Our website provides information on recent testing and measurements of EMF levels that we have taken near mobile sites. Our published measurements have consistently shown that EMF levels are well within the internationally agreed levels in the ICNIRP Guidelines. We also provide a service where individuals can request Ofcom to carry out EMF measurements near mobile sites.<br><br>• There have been a significant number of attacks on mobile sites in recent years and publishing information on the location of sites risks further sites being attacked. Such attacks always have an adverse impact such as customers losing mobile signal and mobile operators incurring |

| | |
|---|---|
| | additional costs but they can have severe consequences, for example, where a mobile site that supports critical communications for the emergency services is attacked; the impact can be particularly serious in the current climate if there is disruption to a hospital's communications systems. Such attacks can also cause physical harm to employees of mobile operators, emergency services personnel and the general public. |

**Reasons why public interest favours withholding information**

- The greater likelihood of the adverse effect, the greater the public interest in maintaining the exception. This is affected by how extensive the adverse effect is – in this case the adverse effect on national security has the potential to affect the security of the United Kingdom and its people, and the opportunity for the adverse effect to arise is ongoing.

- The impact of the adverse effect on national security also has the potential to harm the United Kingdom and its people and is therefore severe.

- The open source information that provides similar data may present inaccurate, partial or out-of-date data, which makes them of much more limited use to a potential attacker. Using these open source information websites would not yield the same level of accuracy as would be contained in the information requested.

- Much of the other publicly available data does not disclose specific site locations or has not been updated for several years and is similarly likely to be inaccurate and incomplete.

- We have carefully considered whether the arguments around transparency and accountability may outweigh the arguments in favour of withholding the information. In doing so, we have taken into account the national security risks identified above as well as (i) the fact all of our EMF measurements to date have shown that EMF levels are well within the internationally agreed levels in the ICNIRP Guidelines; and (ii) the high risk of attacks on mobile sites which can have significant adverse consequences.

- On balance, the arguments against disclosure – including the likelihood and severity of the adverse effect on national security, and the increased threat to national security in respect of the requested information when compared to the information already in the public domain - carry greater weight than the arguments in favour of disclosure. Therefore, the public interest in maintaining the exception outweighs the public interest in disclosure.

**Regulation 12(5)(a) exception**

I have delegated authority from the Ofcom Board to make decisions in relation to Ofcom's obligations under the Environmental Information Regulations 2004 (EIR).

Taking into account the advice from Government on the potential implications of disclosure, in my reasonable opinion, disclosure of the information requested would adversely affect national security. Regulation 12(5)(a) of the EIR therefore applies.

In applying this exception, I have balanced the public interest in withholding the information against the public interest in disclosing the information. I have set out above the factors I considered when deciding where the public interest lies.

I have decided that in all the circumstances of the case, the public interest in maintaining the exception outweighs the public interest in disclosing the information. In assessing this, I have applied a presumption in favour of disclosure.

Disclosure of the information requested is therefore refused under regulation 12(5)(a) of the EIR.

If you have any queries about this letter, please contact information.requests@ofcom.org.uk.

Signed:

Helen Hearn

Director, Spectrum

Date: 10 February 2023