Reference: 01416001

Zach Westbrook
Information Rights Advisor
information.requests@ofcom.org.uk

1 March 2023

Freedom of Information request: Right to know request

Thank you for your request for information concerning 5G phone mast attacks. Your request was received on 4 January 2023 and we have considered it under the Freedom of Information Act 2000 (the "FOI Act") and the Environmental Information Regulations 2004 (the "EIR"). We wrote to you on 1 February 2023 to explain that it was necessary to extend the deadline in which we have to respond in order for us to consider whether the public interest is in favour of releasing the information requested or not. We have now concluded that consideration.

Your request

This is an FOI request for information held by OFCOM on attacks on mobile base stations since 1 August 2020 up until the present (attacks fuelled by anti-5G or similar campaigns).

In OFCOM publications, and following previous FOI requests, OFCOM has released the relevant data up until 31 July 2020 (and in the case of another dataset - identifying the regions of attacks - up until 11 Nov 2020). I was unable to find more recent data in later OFCOM reports or earlier FOI releases, hence I'm making an FOI request.

I don't know how you have databased this information, but if it helps I would like the following information:

- Number of attacks (in general, all attacks)

- Number of attacks "confirmed/strongly linked to anti-5G or similar campaigns" (if it assists, this is your own terminology when replying to an earlier request)

- Number of attacks as reported by individual MNOs (ie breakdown of attacks per MNO)

- Number of attacks broken down geographically, eg whether by town, city, county, local authority, country, region, or by, for example, telephone network area

- Attacks broken down by individual mast identifier

- Dates of attacks, or dates of reports on attacks

- Nature of attacks: eg arson, criminal damage, graffiti, attacks on MNO personnel

- Any technical info on consequences of attacks: eg mast inoperable for a certain number of hours/days, service hours lost

- Any cost info breakdown on the attacks, eg cost to operator per mast attack

- Attacks in relation to police action - eg crime report, cautions, arrests, court proceedings

- Whether info was broken down according to known or suspected motive, eg whether it was known to be 5G related or to do with 'similar campaigns'

- Any other useful information that can be included

- The name or identifier of the dataset referred to in this earlier FOI response, as well as a generic description of its purpose (https://www.ofcom.org.uk/__data/assets/pdf_file/0024/208815/annex-phone-mast-and-telecoms-infrastructure-incidents-data.pdf<https://eur01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.ofcom.org.uk%2F__data%2Fassets%2Fpdf_file%2F0024%2F208815%2Fannex-phone-mast-and-telecoms-infrastructure-incidents-data.pdf&data=05%7C01%7Cinformation.requests%40ofcom.org.uk%7Ca627161fde574e97241308daee843c19%7C0af648de310c40688ae4f9418bae24cc%7C0%7C1%7C638084548957743550%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=bNtzt6bW982iI%2FwesDF56Yqd6oqmZmd5P8e6XEztzfY%3D&reserved=0>) and the names of all the other header fields of this dataset (except for the date/county/description headings already identified)

If there are other subject fields that I have not included but which might, for example, be included on an Excel chart summarising this information, I would be grateful for that information. I'm guessing some of this info is held in database format so I would be happy just to have the database, with any required redactions.

If it is helpful, here are some quick links to earlier FOI requests and OFCOM publications:
https://www.ofcom.org.uk/__data/assets/pdf_file/0024/208815/annex-phone-mast-and-telecoms-infrastructure-incidents-data.pdf<https://eur01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.ofcom.org.uk%2F__data%2Fassets%2Fpdf_file%2F0024%2F208815%2Fannex-phone-mast-and-telecoms-infrastructure-incidents-data.pdf&data=05%7C01%7Cinformation.requests%40ofcom.org.uk%7Ca627161fde574e97241308daee843c19%7C0af648de310c40688ae4f9418bae24cc%7C0%7C1%7C638084548957743550%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=bNtzt6bW982iI%2FwesDF56Yqd6oqmZmd5P8e6XEztzfY%3D&reserved=0>

https://www.ofcom.org.uk/__data/assets/pdf_file/0006/220002/attacks-on-the-159-base-stations-associated-with-anti-5g-or-similar-campaigns.pdf<https://eur01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.ofcom.org.uk%2F__data%2Fassets%2Fpdf_file%2F0006%2F220002%2Fattacks-on-the-159-base-stations-associated-with-anti-5g-or-similar-campaigns.pdf&data=05%7C01%7Cinformation.requests%40ofcom.org.uk%7Ca627161fde574e97241308daee843c19%7C0af648de310c40688ae4f9418bae24cc%7C0%7C1%7C638084548957743550%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=YVpNOftsoys0QWtzyfByDmoopLLFn5UYF3hw1x7pm3c%3D&reserved=0>

Some information was also released in the 2020 edition of the Connected Nations report (though subsequent reports don't appear to have updated the situation).

Our response

By way of background, and as explained in our response to an FOI request dated 10 May 2021, Ofcom is not directly involved with the law enforcement agencies that investigate such attacks, nor with the infrastructure contractors who build networks and voluntarily supply some data to Ofcom which may fall within the scope of your request. While we have supplied certain information we hold that appears to fall within the request, we are not therefore in a position to confirm its accuracy or completeness and we cannot speculate on matters that are beyond Ofcom's remit (including costs to operators, arrest information, perceived motives, etc) as the UK communications regulator.

Please note that the 159 attacks referred to on page 34 of the Connected Nations 2020 Report (and referred to in our response to an FOI request dated 10 May 2021) cover the period 1 February 2020 to 31 July 2020 and are based on a different data set to the 149 attacks referred to in our response to an FOI request dated 3 December 2020 and covering the period 1 April 2020 to 11 November 2020.

We note that your request relates to attacks from 1 August 2020 i.e. you appear to be requesting an updated figure from our Connected Nations Report. However, the updated information we currently hold is based on the more detailed dataset previously provided up to 11 November 2020. To ensure we do not provide potentially misleading information from different datasets covering the same period, and taking into account the details of attacks you have requested, we consider it appropriate to provide you with updated information on mast attacks from 12 November 2020.

Mast attacks

As explained above, we are providing you with details of mast attacks from 12 November 2020 to 26 January 2023, including the following details:

- Date of attack
- Time of attack
- Area of attack
- County of attack
- Constabulary of attack

All of these attacks have been recorded as relating to arson and/or sabotage. We do not hold a breakdown of these attacks per MNO.

We do hold additional information within the scope of your request, namely:

- specific location information;
- whether a critical building is located nearby;
- police crime reference numbers; and
- more detailed descriptions of the attacks.

This additional information you have requested is being withheld as we consider that it is exempt from disclosure, in particular under:

- Sections 23(1) or 24(1) FOIA. Section 23 FOIA deals with information that has been supplied by, or relates to, a body specified in that section. Section 24(1) may apply where section 23(1) does not apply and deals with information required for the purpose of safeguarding national security.

- Section 31 FOIA. This part of the act deals with information that, if disclosed, would, or would be likely to, prejudice law enforcement. This covers both the prevention or detection of a crime and the exercise by Ofcom of functions for the purpose of ascertaining whether a person has failed to comply with legal obligations or regulatory action is otherwise justified.
- Section 43(2) FOIA. This exemption deals with information that, if disclosed, would, or would be likely to, prejudice the commercial interests of any person including the public authority holding it.

In applying these exemptions, we have had to balance the public interest in withholding the information against the public interest in disclosing the information. In this case, we consider that the public interest favours withholding the information. The attached Annexes A – C to this letter set out the exemptions.

Attacks on MNO personnel

In response to your request for information on attacks on MNO personnel, we are also separately providing you with information on confrontations which have been recorded in the dataset as being linked to 5G. We understand incidents have been recorded as being linked to 5G where an engineer categorised the motivation behind the attack as relating to 5G when s/he reported the incident. There may therefore be some incidents which were not recorded as being linked to 5G but which could be interpreted as being linked to 5G. We have not previously provided this dataset and are therefore providing it from 1 August 2020 to 26 January 2023 as requested.

I hope this information is helpful. If you have any further queries, then please send them to information.requests@ofcom.org.uk quoting the reference number above in any future communications.

Yours sincerely

Zach Westbrook

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. Further information about this, and the internal review process can be found on the Information Commissioner's Office here. Alternatively, the Information Commissioner can be contacted at:

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

Annex A

Section 23(1) of the Act:

"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).

(3) The bodies referred to in subsections (1) and (2) are— …

(n) the National Crime Agency.

Section 24(1) of the Act:

"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."

Factors for disclosure	Factors for withholding
• Enabling the public to gain a better understanding of the specific location of mast attacks.	• The dataset we hold relating to mast attacks was put together for the National Crime Agency and therefore relates to a body specified in Section 23(3) FOIA. • In the alternative, HM Government has advised us that disclosing the specific location of mobile sites raises significant concerns on national security grounds and would adversely affect national security. • 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 services (including those of the emergency services). Government's concerns centre on four areas: (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. (2) Jamming: Publishing the requested information could enable the jamming of radio signals. (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. (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. • 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. • Government is also concerned that disclosure of the requested information on mobile sites would set a precedent for disclosure in response to requests about other geographic areas, resulting in further aggregation of information on mobile sites.

	• 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. • We have also taken into account the fact that 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. • There have been a significant number of attacks on mobile sites 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	
• There is a fairly limited public interest in disclosing detailed information on the specific location of mast attacks and more significant weight should be attached to avoid the prejudice which would be caused by disclosure as well as the adverse impact of further attacks.	

Annex B

Section 31(1) of the Act: ***"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;"***	
Factors for disclosure	**Factors for withholding**
• Enabling the public to gain a better understanding of mast attacks.	• Disclosure of detailed information about mast attacks (in particular police crime reference numbers and detailed descriptions) may prejudice the detection of crime by compromising open investigations. • Disclosure of this information may also prejudice the prevention of crime by facilitating the possibility of criminal offences being carried out to the extent the information may suggest certain masts may be more vulnerable to attacks or indicate certain types of attacks may have been or could be more successful. • 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
• There is a fairly limited public interest in disclosing detailed information on mast attacks and more significant weight should be attached to avoid the prejudice which would be caused by disclosure as well as the adverse impact of further attacks.

Annex C

Section 43(2) of the FOI Act provides that: ***"Information is exempt information if its disclosure under this Act would, or would be likely to, prejudice the commercial interests of any person (including the public authority holding it)."***	
Factors for disclosure	**Factors for withholding**
• Enabling the public to gain a better understanding of mast attacks.	• Disclosure of detailed information about mast attacks provided by MNOs is likely to prejudice their commercial interests to the extent that it contains commercially sensitive information such as technical requirements, details of specific equipment used, the layout of a mobile site etc. • Releasing this information would also put Ofcom in a detrimental position in terms of whether MNOs may be prepared to release information to Ofcom in the future which may undermine our ability to carry out our functions going forward. It is important that Ofcom protects commercial information provided to it by third parties so that it maintains their trust.
Reasons why public interest favours withholding information	
• There is a fairly limited public interest in disclosing detailed information on mast attacks and more significant weight should be attached to avoid the prejudice which would be caused by disclosure.	