




Immigration
Enforcement

Immigration Enforcement Secretariat
Sandford House
41 Homer Road
Solihull
West Midlands
B91 3QJ


[request-810089-
c7b8ff4d@whatdotheyknow.com](mailto:request-810089-c7b8ff4d@whatdotheyknow.com)

www.gov.uk/home-office

Monday 13 December 2021

Dear 

Re: Freedom of Information request – 67110

Thank you for your email of 23 November, in which you ask for information in relation to the practices of Immigration Enforcement and Border Force when seizing and extracting data from mobile phones (and other digital devices) of migrants, and any related policies or guidance documents.

Your request, which is set out in the attached **Annex A**, has been handled as a request for information under the Freedom of Information Act 2000 (FOIA).

I am able to disclose some of the information that you have requested. For ease of reference, these have been laid out using the number sequence contained within your request.

1. Immigration Enforcement confirm the existence of the current policy on Digital Device Extraction governing the seizure of mobile phones (and other digital devices) at lorry drops and detention centres. The policy was published on 7 July 2021 and as disclosed in your email can be found at: [Digital device extraction policy \(publishing.service.gov.uk\)](https://publishing.service.gov.uk)
2. Immigration Enforcement confirm the existence of the current policy governing any subsequent data extraction from mobile phones (and other digital devices) seized at lorry drops and detention centers. The policy as requested is the same as disclosed in your email and can be found at: [Guidance overview: Immigration Enforcement: digital device extraction policy - GOV.UK \(www.gov.uk\)](https://www.gov.uk)
3. Immigration Enforcement confirm the existence of a privacy and data protection impact assessment relating to digital devices. A redacted copy of 'Immigration Enforcement Criminal and Financial Investigation Kiosk Use' was released to Privacy International in August 2021, together with accompanying public interest tests relating to the exempt sections. Detention Services Order 05/2018 sets out Home Office policy on mobile phones, internet enabled devices and cameras in immigration removal centres, residential short-term holding facilities, the pre-departure accommodation and during escort: <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attach>

[ment_data/file/917908/Mobile_phones_and_cameras_in_immigration_removal_centres.pdf](#)

4. Immigration Enforcement does not hold the information on the number of mobile phones (and other digital devices) that were seized within the criteria requested, namely lorry drops and detention centres, and separately, the number of these from which data was extracted in the last year (October 2020 - October 2021).
5. Immigration Enforcement neither confirm nor deny whether we hold the information that you have requested in question 5. Section 31(3) of the FOIA absolves us from the requirement to say whether or not we hold information, if compliance with Section 1(1)(a) would, or would likely to, prejudice any of the matters mentioned in Section 31(1) and the public interest falls in favour of neither confirming nor denying. An explanation of 31(3) is set out in the attached **Annex B**.

This response should not be taken as conclusive evidence that the information you have requested is or is not held by the Home Office.

6. The Home Office / Immigration Enforcement have not made any referrals to the Forensic Science Regulator.

We can confirm that the policy(ies) or guidance on the procedure for reporting and treating errors in the conduct of digital forensics by Immigration Enforcement is due to be finalised and published in early 2022. However, after careful consideration we have decided that this information is exempt from disclosure under Section 22(1) of FOIA as the information is intended for future publication. Arguments for and against disclosure in terms of the public interest, with the reasons for our conclusion, are set out in **Annex B**.

Section 22 (1) provides that information can be withheld if -

- (a) the information is held by the public authority with a view to its publication, by the authority or any other person, at some future date (whether determined or not),
- (b) the information was already held with a view to such publication at the time when the request for information was made, and
- (c) it is reasonable in all the circumstances that the information should be withheld from disclosure until the date referred to in paragraph (a).

Although Immigration Enforcement were not present at the meeting, we can confirm there were no general instructions or requirements provided to commercial digital forensics software providers as a result of the Digital Forensics Specialist Group meeting held on 13 June 2019.

If you are dissatisfied with this response you may request an independent internal review of our handling of your request by submitting a complaint within two months to foirequests@homeoffice.gsi.gov.uk, quoting reference **67110** If you ask for an internal review, it would be helpful if you could say why you are dissatisfied with the response.

As part of any internal review the Department's handling of your information request would be reassessed by staff who were not involved in providing you with this response. If you were to remain dissatisfied after an internal review, you would have a right of complaint to the Information Commissioner as established by section 50 of the FOIA.

A link to the Home Office Information Rights Privacy Notice can be found in the following link. This explains how we process your personal information:

<https://www.gov.uk/government/publications/information-rights-privacy-notice>

Yours sincerely,

Immigration Enforcement Secretariat

ImmigrationEnforcementFOIPQ@HomeOffice.gov.uk

-----Original Message-----

From: Privacy International <request-810089-c7b8ff4d@whatdotheyknow.com>

Sent: 23 November 2021 17:37

To: FOI Requests <FOIRequests@homeoffice.gov.uk>

Subject: 67110 - Freedom of Information request - Mobile phone seizures and extraction at lorry drops and detention centres

Do you trust this email? This email originated from outside the Home Office or came from a Home Office system that has not been certified. Please exercise caution before opening attachments or clicking on links within this email or any suspicious email, particularly from unknown senders.

Dear Home Office,

I write on behalf of Privacy International to make a request for information under the Freedom of Information Act 2000.

I seek information in relation to the practices of Immigration Enforcement and Border Force seizing and extracting data from the mobile phones (and other digital devices) of migrants, and any related policies or guidance documents.

BACKGROUND INFORMATION

It has previously been reported

<https://gbr01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fbylinetimes.com%2F2021%2F08%2F26%2Fhome-offices-secret-inhumane-policy-of-seizing-phones-of-refugees-arriving-on-boats-and-extracting-their-data-exposed%2F&data=04%7C01%7CJosie.Amponsah%40homeoffice.gov.uk%7C797bbe6842294a99cd4108d9b413e603%7Cf24d93ecb2914192a08af182245945c2%7C0%7C0%7C637738819814227709%7CUnknown%7CTWFpbGZsb3d8eyJWljojMC4wLjAwMDAiLCJQIjoiV2luMzliLCJBTil6lk1haWwiLCJXVCI6Mn0%3D%7C3000&sdata=Wq6q5H7a3%2BaS3PCASc1xZ%2BG5MlpQ9TVV%2B5InJ1c9IRU%3D&reserved=0>) that the Home Office "has been carrying out a secret policy of seizing the phones of more than 7,000 refugees arriving in the UK by boat for data extraction".

We know from these reports and from your response to a previous FOIA request that the Home Office has a policy

<https://gbr01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.gov.uk%2Fgovernment%2Fpublications%2Fimmigration-enforcement-digital-device-extraction-policy&data=04%7C01%7CJosie.Amponsah%40homeoffice.gov.uk%7C797bbe6842294a99cd4108d9b413e603%7Cf24d93ecb2914192a08af182245945c2%7C0%7C0%7C637738819814227709%7CUnknown%7CTWFpbGZsb3d8eyJWljojMC4wLjAwMDAiLCJQIjoiV2luMzliLCJBTil6lk1haWwiLCJXVCI6Mn0%3D%7C3000&sdata=8jTcZETe4OQ1AF3bpy%2FwUkSVOd8tqwfWZakeUwc8YSY%3D&reserved=0>) in place setting out the conditions under which Immigration Enforcement officers can seize and extract data from mobile phones.

Some sources also indicate that seizure of phones may be occurring not just at boat arrivals, but also at "lorry drops" and at immigration detention centres:

- "Reporting of lorry drops - 7.33 The call handler also asks for the name, nationality and date of birth of each migrant, their intentions ("usually to claim [asylum] or find work"), and prompts the reporting officer to "consider collecting and bagging all mobile phones and SIM cards and any pieces of paper containing anything appearing to show names, addresses or phone numbers in the UK". Again, these are mentioned in the NPCC aide memoire." (p.40, ICIBI report "An inspection of the Home Office's response to in-country clandestine arrivals ('lorry drops') and to irregular migrants arriving via 'small boats' (May 2019 – December 2019)" - available at

[https://gbr01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fassets.publishing.service.gov.uk%2Fgovernment%2Fuploads%2Fsystem%2Fuploads%2Fattachment_data%2Ffile%2F933953%2FAn%20inspection%20of%20the%20Home%20Office%20s%20response%20to%20in-country%20clandestine%20arrivals%20lorry%20drops%20and%20to%20irregular%20migrants%20arriving%20via%20small%20boats.pdf&data=04%7C01%7CJosie.Amponsah%40homeoffice.gov.uk%7C797bbe6842294a99cd4108d9b413e603%7Cf24d93ecb2914192a08af182245945c2%7C0%7C0%7C637738819814227709%7CUnknown%7CTWFpbGZsb3d8eyJWljiMC4wLjAwMDAiLCJQIjoiV2luMzliLCJBTil6Ik1haWwiLCJXVCI6Mn0%3D%7C3000&sdata=rdPzmsmao1iRyWaysaBek%2BgZx8LLyp0xDr7OREW0u3s%3D&reserved=0\)](https://gbr01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fassets.publishing.service.gov.uk%2Fgovernment%2Fuploads%2Fsystem%2Fuploads%2Fattachment_data%2Ffile%2F933953%2FAn%20inspection%20of%20the%20Home%20Office%20s%20response%20to%20in-country%20clandestine%20arrivals%20lorry%20drops%20and%20to%20irregular%20migrants%20arriving%20via%20small%20boats.pdf&data=04%7C01%7CJosie.Amponsah%40homeoffice.gov.uk%7C797bbe6842294a99cd4108d9b413e603%7Cf24d93ecb2914192a08af182245945c2%7C0%7C0%7C637738819814227709%7CUnknown%7CTWFpbGZsb3d8eyJWljiMC4wLjAwMDAiLCJQIjoiV2luMzliLCJBTil6Ik1haWwiLCJXVCI6Mn0%3D%7C3000&sdata=rdPzmsmao1iRyWaysaBek%2BgZx8LLyp0xDr7OREW0u3s%3D&reserved=0)

- "The mobile phone situation in detention centres is also pretty terrible. On arrival smartphones are confiscated and replaced with basic phones (without cameras)." (Article on Medium by Ruth Hennell, based on submissions to Detention Inquiry - available at [https://gbr01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fmedium.com%2F%40TheRehn%2Fthe-uk-home-office-has-just-officially-banned-access-to-social-media-and-instant-messaging-to-6f46ba798d0&data=04%7C01%7CJosie.Amponsah%40homeoffice.gov.uk%7C797bbe6842294a99cd4108d9b413e603%7Cf24d93ecb2914192a08af182245945c2%7C0%7C0%7C637738819814227709%7CUnknown%7CTWFpbGZsb3d8eyJWljiMC4wLjAwMDAiLCJQIjoiV2luMzliLCJBTil6Ik1haWwiLCJXVCI6Mn0%3D%7C3000&sdata=NdKq2yXUFGz%2FYZ%2B%2B5azPF7Zy%2BqEzZuIGCxf6sNUsj8%3D&reserved=0\)](https://gbr01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fmedium.com%2F%40TheRehn%2Fthe-uk-home-office-has-just-officially-banned-access-to-social-media-and-instant-messaging-to-6f46ba798d0&data=04%7C01%7CJosie.Amponsah%40homeoffice.gov.uk%7C797bbe6842294a99cd4108d9b413e603%7Cf24d93ecb2914192a08af182245945c2%7C0%7C0%7C637738819814227709%7CUnknown%7CTWFpbGZsb3d8eyJWljiMC4wLjAwMDAiLCJQIjoiV2luMzliLCJBTil6Ik1haWwiLCJXVCI6Mn0%3D%7C3000&sdata=NdKq2yXUFGz%2FYZ%2B%2B5azPF7Zy%2BqEzZuIGCxf6sNUsj8%3D&reserved=0)

[https://gbr01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fmedium.com%2F%40TheRehn%2Fthe-uk-home-office-has-just-officially-banned-access-to-social-media-and-instant-messaging-to-6f46ba798d0&data=04%7C01%7CJosie.Amponsah%40homeoffice.gov.uk%7C797bbe6842294a99cd4108d9b413e603%7Cf24d93ecb2914192a08af182245945c2%7C0%7C0%7C637738819814227709%7CUnknown%7CTWFpbGZsb3d8eyJWljiMC4wLjAwMDAiLCJQIjoiV2luMzliLCJBTil6Ik1haWwiLCJXVCI6Mn0%3D%7C3000&sdata=NdKq2yXUFGz%2FYZ%2B%2B5azPF7Zy%2BqEzZuIGCxf6sNUsj8%3D&reserved=0\)](https://gbr01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fmedium.com%2F%40TheRehn%2Fthe-uk-home-office-has-just-officially-banned-access-to-social-media-and-instant-messaging-to-6f46ba798d0&data=04%7C01%7CJosie.Amponsah%40homeoffice.gov.uk%7C797bbe6842294a99cd4108d9b413e603%7Cf24d93ecb2914192a08af182245945c2%7C0%7C0%7C637738819814227709%7CUnknown%7CTWFpbGZsb3d8eyJWljiMC4wLjAwMDAiLCJQIjoiV2luMzliLCJBTil6Ik1haWwiLCJXVCI6Mn0%3D%7C3000&sdata=NdKq2yXUFGz%2FYZ%2B%2B5azPF7Zy%2BqEzZuIGCxf6sNUsj8%3D&reserved=0)

- "When you're in the fort you don't have contact with anybody, you can't contact anybody, your phone is taken away from you." (Oral Evidence to Detention Inquiry, APPG on Refugees and APPG on Migration Joint Parliamentary, Inquiry into the Use of Immigration Detention, 2014 - available at

[https://gbr01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fdetentioninquiry.files.wordpress.com%2F2015%2F02%2Ffirst-evidence-session-transcript.pdf&data=04%7C01%7CJosie.Amponsah%40homeoffice.gov.uk%7C797bbe6842294a99cd4108d9b413e603%7Cf24d93ecb2914192a08af182245945c2%7C0%7C0%7C637738819814227709%7CUnknown%7CTWFpbGZsb3d8eyJWljiMC4wLjAwMDAiLCJQIjoiV2luMzliLCJBTil6Ik1haWwiLCJXVCI6Mn0%3D%7C3000&sdata=17Bp2NYCp5HbW4Mtu553uNut9pKce9MCR2fSHEFP0iA%3D&reserved=0\)](https://gbr01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fdetentioninquiry.files.wordpress.com%2F2015%2F02%2Ffirst-evidence-session-transcript.pdf&data=04%7C01%7CJosie.Amponsah%40homeoffice.gov.uk%7C797bbe6842294a99cd4108d9b413e603%7Cf24d93ecb2914192a08af182245945c2%7C0%7C0%7C637738819814227709%7CUnknown%7CTWFpbGZsb3d8eyJWljiMC4wLjAwMDAiLCJQIjoiV2luMzliLCJBTil6Ik1haWwiLCJXVCI6Mn0%3D%7C3000&sdata=17Bp2NYCp5HbW4Mtu553uNut9pKce9MCR2fSHEFP0iA%3D&reserved=0)

REQUEST FOR INFORMATION

We are therefore seeking information in relation to seizure of, and any subsequent data extraction from, migrant and asylum seekers' mobile phones (and other digital devices) at these two points of control in their migration journeys: lorry drops and immigration detention centres.

We hereby request access to the following information:

1. Please confirm the existence of, and provide, the current policy(ies) governing the seizure of mobile phones (and other digital devices) at lorry drops and detention centres.
 2. Please confirm the existence of, and provide, the current policy(ies) governing any subsequent data extraction from mobile phones (and other digital devices) seized at lorry drops and detention centres - if different from the policy already disclosed (<https://gbr01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.gov.uk%2Fgovernment%2Fpublications%2Fimmigration-enforcement-digital-device-extraction-policy&data=04%7C01%7CJosie.Amponsah%40homeoffice.gov.uk%7C797bbe6842294a99cd4108d9b413e603%7Cf24d93ecb2914192a08af182245945c2%7C0%7C0%7C637738819814227709%7CUnknown%7CTWFpGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzliLCJBTiI6I1haWwiLCJXVCi6Mn0%3D%7C3000&sdata=8jTcZETe4OQ1AF3bpy%2FwUkSVOd8tqwfWZakeUwc8YSY%3D&reserved=0>).
 3. Please confirm the existence of, and provide, any privacy and data protection impact assessment(s) undertaken regarding the seizure of and data extraction from mobile phones (and other digital devices) by Immigration Enforcement and Border Force at lorry drops and detention centres.
 4. Please provide recorded information on the number of mobile phones (and other digital devices) that were seized at lorry drops and detention centres, and separately, the number of these from which data was extracted, in the last year (October 2020 - October 2021).
 5. If data extraction from mobile phones (and other digital devices), and subsequent analysis of data, is undertaken through the use of technical tools developed by third party providers (such as digital forensics software providers), please provide any agreements entered between these providers and the Home Office.
 6. According to minutes (https://gbr01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fassets.publishing.service.gov.uk%2Fgovernment%2Fuploads%2Fsystem%2Fuploads%2Fattachment_data%2Ffile%2F881164%2FDFSG_2019_06_13_Minutes.pdf&data=04%7C01%7CJosie.Amponsah%40homeoffice.gov.uk%7C797bbe6842294a99cd4108d9b413e603%7Cf24d93ecb2914192a08af182245945c2%7C0%7C0%7C637738819814237708%7CUnknown%7CTWFpGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzliLCJBTiI6I1haWwiLCJXVCi6Mn0%3D%7C3000&sdata=RzocGHmxQWzDBequ9u8WQFXZIKpUCCqhqtZCzc117E%3D&reserved=0) of a meeting of the Digital Forensics Specialist Group that took place on 13 June 2019 which the Home Office attended as co-chair, "[t]here had been an increase of referrals to the Regulator concerning digital forensics", including "inaccuracies, misinterpretation, evidence handling which included loss of data, overwriting of data, and sending data to the wrong individuals or organisations". The minutes indicated that "It was agreed by the DFSG the software providers should do more to investigate and resolve the errors as soon as possible, and also update all FSP's that use their software."
- Please provide recorded information on the number of referrals made by the Home Office to the Forensic Science Regulator - in relation to Immigration/Border enforcement (whether in respect of actions by Immigration Officers and/or Police officers) - in 2018-2019; 2019-2020; 2020-2021.
 - Please provide any current policy(ies) or guidance on the procedure for reporting and treating errors in the conduct of digital forensics by Immigration Enforcement and Border

Force, as well as any instructions or requirements provided to digital forensics software providers, that were produced as a result of what was agreed in this meeting.

If our request requires any clarification please do not hesitate to contact us. We are willing to limit our request should that be necessary and kindly request you identify what would assist you in being able to respond. Thank you for your time and we look forward to your response.

Yours faithfully,

Lucie Audibert

Legal Officer

Privacy International

Freedom of Information request – 63509 Freedom of Information request from Lucie Audibert, (reference 67110)

Information requested

See Annex A.

Response

Some of the exemptions in the FOIA, referred to as ‘qualified’ exemptions, are subject to a public interest test (PIT). This test is used to balance the public interest in disclosure against the public interest in maintaining the exemption. We must carry out a PIT where we are considering using any of the qualified exemptions in response to a request for information.

The ‘public interest’ is not necessarily the same as what interests the public. In carrying out a PIT we consider the greater good or benefit to the community as a whole if the information is released or not. Transparency and the ‘right to know’ must be balanced against the need to enable effective government and to serve the best interests of the public.

The FOIA is ‘applicant blind’. This means that we cannot, and do not, ask about the motives of anyone who asks for information. In providing a response to one person, we are expressing a willingness to provide the same response to anyone.

Question 5 falls for exemption under Section 31(3).

Question 6 falls for exemption under Section 22(1).

Section 31(3)

Considerations in favour of confirming whether or not we hold the information

There is a general public interest in openness and transparency in government, which will serve to increase public trust. To confirm or deny if any information is held in relation to investigative activities, procedures and policy would support openness and transparency within government. Confirming or denying whether certain technology is used in the process of investigations would serve to inform and educate the public about an issue related to immigration crime and national security.

Considerations in favour of neither confirming nor denying whether we hold the information

To confirm that information is held would suggest that the Home Office / Immigration Enforcement use cloud analytics and/or cloud extraction. Conversely, to confirm that information is not held would suggest that the Home Office / Immigration Enforcement do not utilise such technology. Any response the Home Office might provide on this issue - be it a confirmation or denial - would be of significant value to those involved in immigration crime and would allow organised crime groups to build a picture of investigative measures and practices that may or may not be in place for protecting vulnerable individuals and tackling criminality. There is also a strong public interest in maintaining the security of the country by prosecuting those involved in immigration crime,

and confirming or denying whether information is held in relation to investigative procedures, activity and technology has the potential to prejudice the prevention and detection of crime and negatively impact on national security.

Conclusion

We conclude that the balance of the public interest lies in neither confirming nor denying whether we hold the information. This response should not be taken as confirmation that the information you have requested is or is not held by the Home Office.

Section 22(1)

Considerations in favour of disclosing the information

There is a general public interest in the disclosure of information to ensure departmental transparency and accountability. The release of the requested information would help to assure the public of the processes Immigration Enforcement has in place for reporting errors while dealing with digital forensics.

Considerations in favour of maintaining the exemption

It is in the public interest to ensure that the publication of official information is properly assessed. Immigration Enforcement must ensure that the information intended for publication meets the standards and requirements set for departmental publications. It would not be in the public interest for Immigration Enforcement to release information during the draft stage, prior to the necessary review and approval stages.

Conclusion

We conclude that the balance of the public interest lies in maintaining the exemption and withholding the information.