

2nd March 2020

[request-643119-41b624f1@whatdotheyknow.com](mailto:request-643119-41b624f1@whatdotheyknow.com)

Dear Torr Robinson

**Freedom of Information Request – Reference No:20200535**

**REQUEST**

*I am aware that companies are selling technologies to law enforcement that allow them to take vast quantities of personal data from cloud-based apps and accounts. You can read more [<https://privacyinternational.org/long-read/3300/cloud-extraction-technology-secret-tech-lets-government-agencies-collect-masses-data>].*

*I make the following request for documents/information under the Freedom of Information Act:*

- 1. Do you use mobile phone extraction technology that includes cloud analytics / cloud extraction capabilities e.g. Cellebrite UFED Cloud Analyser, Magnet Axiom Cloud or Oxygen Forensics Cloud Extractor*
- 2. Do you have other technologies that allow you to access cloud-based accounts and extract this data.*
- 3. Please provide a copy of the relevant Data Protection Impact Assessment.*
- 4. Please provide a copy of the relevant local and/or national guidance/standard operating procedure/policy.*
- 5. Please confirm the legal basis you rely on to conduct cloud analytics/extraction.*

**RESPONSE**

South Yorkshire Police can neither confirm nor deny that we hold any information relevant to this request by virtue of the following exemptions:

**Section 24(2) National Security**  
**Section 31(3) Law enforcement**

Section 24 and Section 31 are both qualified exemptions and as such there is a requirement to evidence any harm that confirming or denying that any other information is held, in addition to considering the public interest.

Harm in confirming information is held:

Modern day policing is intelligence led and law enforcement depends upon the development of intelligence and the gathering and security of evidence in order to disrupt criminal behaviour and bring offenders to justice. As criminals adapt and exploit new technology, the police need to respond by overcoming hi-tech barriers in order to meet their responsibilities. In this case the information relates to the extraction of data from individuals' mobile devices, albeit victim or offender. By revealing whether information is held in relation to the specific technology, will in itself be revealing tactical information which would

undermine the process of preventing or detecting crime and the apprehension of prosecution of offenders.

#### Factors favouring confirming or denial – S31

Confirming or denying that South Yorkshire Police force holds information would raise the general public's awareness around techniques used to extract information from mobile phones and show responsibility to delivery of effective operational law enforcement.

#### Factors against confirming or denying – S31

By confirming or denying whether information is held could compromise South Yorkshire Police forces law enforcement capabilities and the effectiveness of the force will be reduced. To confirm or deny if information is held could undermine current and/or future strategies when carrying out investigations and gathering evidence may be compromised.

The personal safety of individuals is of paramount importance to the Police Service and must be considered in response of every release. A disclosure under Freedom of Information is a release to the world and, in this case, confirming or denying if the information is held in relation to gathering evidence from mobile phones, would undermine the evidence gathering process of any investigative inquiry relating to offences, some of which may be serious cases such as murder or rape.

#### Factors favouring confirming or denial – S24

Confirming or denial that any information exists relevant to the request would lead to a better informed public and the public are entitled to know how public funds are spent. The information simply relates to national security and disclosure would not actually harm it.

#### Factors against confirming or denial - S24

To confirm or deny whether South Yorkshire Police force hold any information would allow inferences to be made about the nature and extent of national security related activities which may or may not take place. This could enable terrorist groups to take steps to avoid detection, and as such, confirmation or denial would be damaging to national security.

By confirming or denying any policing arrangements of this nature would render national security measures less effective. This would lead to the compromise of ongoing or future operations to protect the security or infra-structure on the UK and increase the risk of harm to the public.

#### Balancing Test

As always the Freedom of Information Act has a presumption of disclosure, unless when balancing the competing public interest factors the prejudice to the community outweighs the benefits. In this case, there is an argument for confirming or denying, inasmuch as the public have a right to know that every effort is made to gather all relevant evidence, including extracting data from mobile phones, but this must be balanced against the negative impact these disclosures can make.

Law Enforcement is reliant on community engagement, intelligence and evidence gathering and when it is appropriate, information is given to the public. What has been established in this case is the fact that confirming or denying that information relating to technologies used when extracting data would be harmful and have an adverse effect on the investigative process and on the public prevention or detection of crime and the apprehension or prosecution of offenders. This places the victims of such offending at a greater risk towards their health and wellbeing and is not an action the Police Service would be willing to take. These negatives outweigh any tangible community benefit and therefore the balance does not favour disclosure at this time.

If you are unhappy with the way your request for information has been handled, you can request a review by following the advice contained in the separate notice enclosed with this correspondence:

If you remain dissatisfied with the handling of your request or complaint, you have a right to appeal to the Information Commissioner at:

The Information Commissioner's Office,  
Wycliffe House,  
Water Lane,  
Wilmslow,  
Cheshire, SK9 5AF.  
Telephone: 08456 306060 or 01625 545745  
Website: [www.ico.gov.uk](http://www.ico.gov.uk)

Yours sincerely

Louise Holmes  
Information Compliance Clerk  
South Yorkshire Police  
Information Compliance Unit  
Professional Standards Department  
Unit 20 Sheffield 35A Business Park  
Churchill Way  
Sheffield  
S35 2PY

Please note that police forces in the United Kingdom are routinely required to provide information and statistics to government bodies and the recording criteria is set nationally. However, the systems used for recording these figures are not generic, nor are the procedures used locally in capturing the data. It should be noted that for these reasons this forces response to your questions should not be used for the comparison purposes with any other response you may receive.

South Yorkshire Police provides you the right to request a re-examination of your case under its review procedure (copy enclosed). If you decide to request such a review and having followed the Constabulary's full process you are still dissatisfied, then you have the right to direct your comments to the Information Commissioner who will give it consideration.

The South Yorkshire Police in complying with their statutory duty under sections 1 and 11 of the Freedom of Information Act 2000 to release the enclosed information will not breach the Copyright, Designs and Patents Act 1988. However, the rights of the copyright owner of the enclosed information will continue to be protected by law. Applications for the copyright owner's written permission to reproduce any part of the attached information should be addressed to The Force Solicitor, South Yorkshire Police, Police Headquarters, 5 Carbrook Hall Road, Sheffield, S9 2EG

## **Appeal Process for Freedom of Information**

Using this process will not affect your right to appeal directly to the Information Commissioner. However, it will usually be quicker if matters can be resolved locally using this process.

### ***Who can appeal?***

Anyone who has requested information from the Force in writing can appeal within 20 working days from the date of the response provided. If you have requested information and you are not satisfied with the way we have dealt with your request, you can use the appeal process to have it looked at again. If someone who requested information would like to appeal but cannot do so themselves you can appeal on their behalf, but it will help us if you make it clear that you are doing so.

### ***What can I appeal about?***

You can appeal about the range, amount and format of information we have sent following a request. You can also appeal about the way a request was handled – for example, the time it took to respond, or the way letters were worded.

### ***How do I appeal?***

You can appeal by writing, emailing or faxing your appeal/complaint to the address below. To deal with your appeal as quickly as possible, it will help if you can give us as much information as you can about the request made, such as the reference number, and the reason for your appeal/ complaint.

### ***What happens to my appeal?***

Once we have enough details to identify the request you are concerned about, a qualified person, other than the initial decision maker, will deal with the internal review.

### ***How long does it take?***

Whatever their conclusion, you will be informed of the result as soon as possible, and in any case within 20 days of submitting your appeal.

If you are still not satisfied, you may then appeal to the Information Commissioner.

### ***Appeal Address***

**Information Compliance Unit South Yorkshire Police Professional Standards  
Department Unit 20 Sheffield 35A Business Park Churchill Way Sheffield S35 2PY**

Email [foi@southyorks.pnn.police.uk](mailto:foi@southyorks.pnn.police.uk)