PRIVACY INTERNATIONAL

62 Britton Street
London EC1M 5UY
United Kingdom
Phone +44 (0)20 3422 4321
www.privacyinternational.org

Independent Office for Police Conduct (IOPC)
PO Box 473
Sale
M33 0BW

Via email only: enquiries@policeconduct.gov.uk

26th April 2018

Dear Sir/Madam,

RE: Privacy International report, ***'Digital stop and search: how the UK police can secretly download everything from your mobile phone'***

We write in relation to the above report (attached). The report examines the police's use of sophisticated and highly intrusive 'mobile phone extraction' technology. The use of mobile phone extraction involves the extraction, retention and analysis of communications data and content.

We wish to submit a complaint in relation to the use of this technology by 26 police forces in the UK:

- Bedfordshire Police
- Durham Constabulary
- Lancashire Constabulary
- Warwickshire Police
- West Mercia Police
- West Midlands Police
- City of London Police
- Devon and Cornwall Police
- Dorset Police
- Derbyshire Constabulary

- Gwent Police
- Norfolk Constabulary
- Hampshire Constabulary
- Suffolk Constabulary
- Thames Valley Police
- Kent Police
- Metropolitan Police Service
- Northumbria Police
- Staffordshire Police
- Lincolnshire Police
- Surrey Police
- Wiltshire Police
- Merseyside Police
- West Yorkshire Police
- North Wales Police
- British Transport Police

We were informed by Avon and Somerset Constabulary, Gloucestershire Constabulary and Leicestershire Police that they were about to trial the use of mobile phone extraction technologies in 2017, therefore we assume this will have commenced by now. We therefore include these further three forces in our complaint.

This complaint relates to direction and control matters. The use of mobile phone extraction technologies relates to the direction and control of a police force by its chief officer. As stated in the statutory guidance:

> "A direction and control matter means a matter relating to the direction and control of a police force by its chief officer or a person for the time being carrying out that chief officer's functions."[1]

We wish to complain on the basis that:

1) there is no clear legislation, policy framework / operational policing policy, regulation or independent oversight in place for the police's use of this technology;

[1] paragraph 29, Schedule 3, Police Reform Act 2002

2) the use of mobile phone extraction technology is in breach of the Data Protection Act 1998.
3) there is a lack of protection for the public, their personal and sensitive personal data, from misuse and abuse of this technology;
4) this is often taking place secretly, without individuals - whether they are suspects, witnesses or even victims of crime - being informed that content and data from their phone is being downloaded and stored indefinitely by the police; and
5) without any kind of record keeping or national statistics, any abuse of this technology or unfair targeting of minority groups is likely to go unnoticed.

In light of the above, we submit that there has been a failure of the Chief Officer to effectively carry out operational management decisions, draft operational policing policies, make organisation decisions and set policing standards with respect to mobile phone extraction.

David Lammy, MP for Tottenham and author of the 2017 Lammy Review into the treatment of, and outcomes for Black, Asian and Minority Ethnic individuals in the criminal justice system, said of Privacy International's report:

> *"The lack of transparency around new policing tools such as mobile phone extraction is a serious cause for concern. There are no records, no statistics, no safeguards, no oversight and no clear statement of the rights that citizens have if their mobile phone is confiscated and searched by the police.*
>
> *My Review of our criminal justice system found that individuals from ethnic minority backgrounds still face bias in parts of our justice system, and it is only because we have transparency and data collection for everything from stop and search incidents to crown court sentencing decisions that these disparities are revealed and we are able to hold those in power to account. Without the collection and audit of data about the use of mobile phone extraction powers scrutiny will be impossible.*
>
> *Given the sensitive nature and wealth of information stored on our mobile phones there is significant risk of abuse and for conscious or unconscious bias to become a factor without independent scrutiny and in the absence of effective legal safeguards.*

We entrust so much personal information to our phones that the police having the power to download every message and photo we have sent or received without any rights and protections is another worrying example of regulations not keeping up with advances in technology."

Data protection

We enclose a copy of our complaint to the Information Commissioners' Office which sets out in detail the breaches of the Data Protection Act 1998.

Lawful basis

As noted above, there is a lack of clear statutory basis. Our report sets out that the few forces who disclosed local policies revealed contradicting beliefs as to the lawful basis.[2]

The National Police Chief's Council[3] have stated that police use of mobile phone kiosks is governed by Section 20 of Police and Criminal Evidence Act 1984, which grants the police the "power to require any information stored in electronic form". However, this view is not consistently held, as demonstrated from the conflicting local guidance of a number of police forces (see pages 20 – 21 of our report)[4]. Further, the section 20 power is parasitic on lawful entry onto premises, which is unlikely to apply in many cases. For example, if an individual is arrested or attends a police station as a witness and their phone is extracted with or without their knowledge.

Sir Peter Fahy, former Chief Constable of Greater Manchester Police agrees[5] that legislation has not kept up with technology and some officers are unaware of how they should and should not be using mobile phone extraction tools. There must be new legislation which addresses the nature of modern policing and the sophisticated new technology available to the police.

In addition, it relates to 'seizure' of property, such as the phone itself, rather than extraction and retention of data on the phone.

---

[2] pages 20 – 21 https://privacyinternational.org/sites/default/files/2018-03/Digital%20Stop%20and%20Search%20Report.pdf

[3] https://www.documentcloud.org/documents/4349039-NPCC.html

[4] https://www.privacyinternational.org/sites/default/files/2018-03/Digital%20Stop%20and%20Search%20Report.pdf

[5] http://www.bbc.co.uk/news/uk-43507661

"20. Extension of powers of seizure to computerised information.
(1) Every power of seizure which is conferred by an enactment to which this section applies on a constable who has entered premises in the exercise of a power conferred by an enactment shall be construed as including a power to require any information stored in any electronic form contained in a computer and accessible from the premises to be produced in a form in which it can be taken away and in which it is visible or form which it can be readily be produced in a visible and legible form.

The reliance by the Metropolitan Police Service on sections 18, 19 and 22 PACE, again relates to powers of entry, search and seizure related to premises. The reliance upon section 32 further appears misguided as this relates to a search of an individual upon arrest, seizure of what may be found, but does not specify search of electronic devices.

Without lawful basis upon which to use mobile phone extraction technology, we submit there has been a failure of direction and control by the Chief Officer to permit the use of these intrusive technologies.

Retention and deletion

Further, there is a lack of clarity on retention and deletion periods. With regard to this, we are concerned about the volume of data obtained through a mobile phone extraction and the technical issues with limiting extractions to certain types and dates. For example, the Metropolitan Police Service state that:

> *"When a SSE kiosk is used to obtain electronic data from a mobile device, it will obtain all data of a particular type, rather than just the individual data that is relevant to a particular investigation.*
>
> *For example, if a photograph on a 'witness' mobile phone is relevant because it shows an offence being committed, then the kiosk will acquire all photographs on that phone, rather than just the photographs of the offence. If text messages to a victim of harassment are required to investigate the harassment allegations, then the kiosk will acquire all text messages on that phone."*

As noted in our report, when the BBC reported on the Metropolitan Police Service implementation of Self-Service Kiosks, they stated that data would be retained "regardless of whether any charges are brought."[6]

A Metropolitan Police procurement document from 2015 refers to the 'ingestion of data from tens of thousands of digital devices annually at dozens of different locations' and to 'maintenance [of the data] for indefinite period extending many years.'[7]

We note that a few forces refer to the MOPI time frames, being the Management of Police Information. These do not provide specific retention periods. They do however state that "Retaining every piece of information collected is, however, impractical and unlawful. Consideration must be given to the types of information that need to be retained."[8]

It is unclear in relation to data extracted from mobile phones whether reviews are conducted and what audit and supervision is in place.

We note that using this technology obtains a huge amount of personal data relating to third parties who may have nothing to do with an investigation, yet their data is obtained and retained by the police. Only Wiltshire police appear to note the collateral intrusion of this technology[9].

Without clear operational policing policies on retention and deletion of extracted data, we believe there has been a failure of direction and control by the Chief Officer.

Security of data

As we note in the report, there have been significant failings to process data in a secure manner. A report from 2015 by the Police and Crime Commissioner for North Yorkshire reveals that in half the cases sampled, there was a failure

[6] page 28, https://privacyinternational.org/sites/default/files/2018-03/Digital%20Stop%20and%20Search%20Report.pdf
[7] page 13, https://assets.documentcloud.org/documents/3280381/MPS-Digital-Cyber-and-Communications-Forensics.pdf
[8] https://www.app.college.police.uk/app-content/information-management/management-of-police-information/retention-review-and-disposal-of-police-information/
[9] page 9, https://privacyinternational.org/sites/default/files/2018-03/Digital%20Stop%20and%20Search%20Report.pdf

to receive authorisation for the use of mobile phone extraction tools. Poor training resulted in practices which undermined prosecution of serious crime offences such as murder and sexual offences. The report goes on to highlight inadequate data security practices, the failure to encrypt data even though the capacity existed, and lost files which may contain intimate details of people never charged with a crime. The report concludes with 8 recommendations, notes there was a limited assurance procedure being followed appropriately and considered further review necessary. It is unclear whether remedial steps have been taken following this damning report.

There have been repeated serious failings in protecting sensitive information and various data breaches by the police reported over the years, as noted in our report. In May 2017 when Greater Manchester Police ("GMP") was fined £150,000 after interviews with victims of violent and sexual crimes, stored unencrypted on DVD's, got lost in the post. The Information Commissioner's Office said that GMP 'was cavalier in its attitude to this data and showed scant regard for the consequences that could arise by failing to keep the information secure.'[10]

Without clear operational policing policies on security of extracted data, we believe there has been a failure of direction and control by the Chief Officer.

Types of personal data and sensitive personal data extracted

Mobile phone extraction enables the collection and retention of vast quantities of communications data and content data, including personal and sensitive personal data of both the device user and many others with whom the user interacts. Yet the legal basis is unclear, the safeguards seemingly absent and independent oversight distinctly lacking.

Without clear operational policing policies setting out the types of data that can be extracted and consideration of the volume of personal and sensitive information, and permitting the extraction of this without lawful basis, we believe there has been a failure of direction and control by the Chief Officer.

There is the additional risk that data could include items subject to legal privilege and journalistic material.

[10] https://www.theguardian.com/uk-news/2017/may/04/greater-manchester-police-fined-victim- interviews-lost-in-post

Disclosure we have received from UK police note that Cellebrite UFED enables extraction of:

- Device information: Phone number, IMEI, IMSI, MEID, ESN, MAC ID
- Phonebook – Contact Name and Numbers
- Call Logs
- Text and picture messages
- Videos and Pictures (in some cases with GeoTag-location info) and creation date and time
- Audio files
- Emails and Web Browsing Information
- GPS and location information
- Social Networking messages and contacts
- Deleted data – call logs, messages, emails
- PIN lock and pattern lock
- Attached media or memory card data (pictures, files, app data located on media card)
- Wireless networks connected to the device.

Privacy International extracted two android phones and one iPhone using the Cellebrite UFED Touch 2. The following device information has been extracted using the Cellebrite UFED:

- Bluetooth MAC address
- Android ID
- Bluetooth device name
- Operating System
- Android fingerprint
- Detected Phone Model
- Detected Phone Vendor
- Phone Activation Time
- Locale language
- Country name
- Time zone
- Mock locations allowed
- Auto time zone
- Auto time
- Location services enabled
- IMSI
- ICCID

- Advertising id
- MSISDN
- Tethering: hotspot password required; last activation time
- Unlock pattern

There are three different extraction processes provided by a Cellebrite UFED Touch 2, Logical, File System and Physical.

A physical extraction was carried out on the devices and extracted:

- Autofill
- Calendar
- Call Log
- Cell Towers to which the phone had connected
- Chats: Facebook; Signal PM; Twitter; WhatsApp
- Contacts
- Cookies
- Device locations
- Device notifications
- Device users
- Emails
- Installed Applications
- Instant Messages
- MMS Messages
- Passwords
- Powering events
- Searched Items
- SMS Messages
- User Accounts
- Web Bookmarks
- Web History
- Wireless Networks

In addition, under 'Data Files', the Cellebrite UFED noted: applications; audio (e.g. audio recordings); configurations; databases; documents; images; text; uncategorised.

Cellebrite claims that it can obtain "comprehensive data extractions, even to inaccessible partitions of the device" and access to hidden and deleted data.

In addition to the data that is physically on the device MSAB's XRY Cloud allows recovery "from beyond the mobile device itself from connected-cloud based

storage … without the need for users to re-enter their login details." They state, "This is particularly useful when looking for online social medial data and app-based data for services such as Facebook, Google, iCloud, Twitter, SnapChat, WhatsApp, Instagram and more."

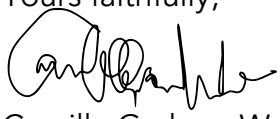
Cellebrite's UFED Cloud Analyzer uses login credentials that can be extracted from the device to pull history of text searches, visited pages, voice search recording and translations from Google web history and view text searches conducted with Chrome and Safari on iOS devices backed-up iCloud. UFED Cloud Analyzer provides the ability to extract, preserve and analyse public domain and private social media data, instant messaging, file storage and other cloud based content. Unless login credentials are changed, it allows you to continue to track online behaviour even if you are no longer in possession of the phone.

As noted in our report, Avon and Somerset have disclosed a contract with Cellebrite for a F-UFD-15-032 UFED Infield Kiosk Logical. This provides the ability to decode data from more than 1,500 mobile applications in minutes.

The companies we know that are used by UK police are Cellebrite; MSAB and Radio Tactics. Additional detail as to the data that the various devices they sell can extract can be found on their respective websites.

We look forward to hearing from you.

Yours faithfully,



Camilla Graham Wood
Privacy International

Cc
Chief Constable for:

- Bedfordshire Police
- Durham Constabulary
- Lancashire Constabulary
- Warwickshire Police
- West Mercia Police

- West Midlands Police
- City of London Police
- Devon and Cornwall Police
- Dorset Police
- Derbyshire Constabulary
- Gwent Police
- Norfolk Constabulary
- Hampshire Constabulary
- Suffolk Constabulary
- Thames Valley Police
- Kent Police
- Metropolitan Police Service
- Northumbria Police
- Staffordshire Police
- Lincolnshire Police
- Surrey Police
- Wiltshire Police
- Merseyside Police
- West Yorkshire Police
- North Wales Police
- British Transport Police
- Avon and Somerset Constabulary
- Gloucestershire Constabulary
- Leicestershire Police