PRIVACY INTERNATIONAL

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

Elizabeth Denham
Information Commissioner
Information Commissioners' Office
Wycliffe House, Water Ln
Wilmslow
SK9 5AF

Via email only: casework@ico.org.uk

26th April 2018

Dear Ms Denham,

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 our recent report 'Digital stop and search' (attached). The report examines the police's use of sophisticated and highly intrusive 'mobile phone extraction' technology, enabling them to download the entire content of someone's phone – whether a suspect, witness or victim – often without their consent or knowledge. The use of mobile phone extraction involves the extraction, retention and analysis of communications data and content.

We hope you will share our deep concerns about this unregulated power, and the potential for serious abuse. We request that you conduct a prompt and thorough investigation into this practice which appears to have taken place throughout the UK for at least six years.

We consider that this practice breaches the requirements of the Data Protection Act 1998, as set out in detail in this letter. We note in particular that:

Company Limited by Guarantee (England & Wales): 4354366
Registered Charity (England & Wales): 1147471

1) there is no clear legislation, policy framework, regulation or independent oversight in place for the police's use of this technology;
2) there is a lack of protection for the public's personal and sensitive personal data.
3) The unchecked use of this technology results in a lack of protection from any misuse and abuse of this technology;
4) the police are taking data from people's phones without obtaining a warrant;
5) 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
6) 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.

Individual police force responses

We have highlighted in the report issues relating to particular police forces including:

- Which police forces are using this technology; which are trialling this technology or intend to trial this technology.
- Which police forces have indicated the legal basis upon which they rely.
- Which do and do not have a local policy.
- Which state they are conducting a review (although despite repeated requests none have been disclosed).

We note on page 14 the confusing response from Greater Manchester Police.

All correspondence from the police is hyperlinked in the report and can be found here: https://www.documentcloud.org/search/projectid:36816-Mobile-Phone-Extraction [1]

Rather than simply addressing individual forces, we believe that the nature of this technology and its widespread use by police forces in the UK, calls for a wholesale review of this practice, in order to consider data protection breaches

[1] If you wish us to send the correspondence to you, please specify the means to do this as we have previously encountered problems sending large amounts of documents to the Information Commissioners' Office.

Company Limited by Guarantee (England & Wales): 4354366
Registered Charity (England & Wales): 1147471

which based on our review are likely to be endemic within the police forces using, trialling or intending to use this technology.

We note in particular the power of the Information Commissioner's Office to issue enforcement notices and serve data controllers with information notices. We believe that these powers should be exercised. The power to issue enforcement notices includes requiring the data controller to comply with the data protection principle or principles in question. We further note Schedule 9 powers of entry and inspection which we believe make be applicable in order to obtain additional information regarding the use of mobile phone extraction.

We also intend to write to the Investigatory Powers Commissioners' Office highlighting our concern that use of mobile phone extraction technology could be seen as 'interception' or 'equipment interference' and thus the practices to date constitute a criminal offence.

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.

We submit that processing of data extracted from mobile phones involves processing of personal data, including sensitive personal data.

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

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

Company Limited by Guarantee (England & Wales): 4354366
Registered Charity (England & Wales): 1147471

- 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. By way of example **Annex 1** is the extracted data from an HTC Desire and iPhone SE, both were used for around 12 months.

The red numbers are deleted items. You will see most items have drop down menus. As we note in the report, it is not only Cellebrite tools that enable extraction of deleted data. MSAB, another company with whom a number of UK police forces contract, has a product XRY Physical which allows access to "system and deleted data."

You will see 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

Company Limited by Guarantee (England & Wales): 4354366
Registered Charity (England & Wales): 1147471

- 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

Company Limited by Guarantee (England & Wales): 4354366
Registered Charity (England & Wales): 1147471

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 believe that it is essential that the police provide full transparency as to the capabilities of the devices they own, including that the types of data that can be extracted, which should be publicly updated on a regular basis in line with developments in the technology.

Data Protection Act 1998

We consider that police forces are using this technology in breach of current and future UK data protection standards, namely the Data Protection Act 1998 ("DPA") and the EU Law Enforcement Directive on the processing of personal data (once it is implemented through the Data Protection Bill).

Under the DPA the data extracted from mobile phones falls within the definition of "data" (§1)[2]; the police are "data controllers" (§1); and individual's

[2] §1(1)(a) is being processed by means of equipment operating automatically in response to instructions given for that purpose

Company Limited by Guarantee (England & Wales): 4354366
Registered Charity (England & Wales): 1147471

whose data is extracted is a "data subject" (§1). The extracted data, elaborated above, is clearly personal data or sensitive personal data.

Our report focused on the use of Self Service Kiosks and Hubs to extract data. We note that these are used by some forces to extract data in both low level and serious crimes.

We have not considered the role of High Tech Crime Units in mobile phone extraction and we have not considered whether other data processors are involved. For example, whether on certain occasions the police send mobile phones to private companies such as Cellebrite to conduct the extraction. We note that in January 2017 Cellebrite was itself hacked and media outlet Motherboard obtained 900 GB of data which 'includes customer information, databases' and 'The dump also contains what appears to be evidence files from seized mobile phones and logs from Cellebrite devices.'[3]

We are not aware to what extent, if at all, automated decision-taking is conducted based upon extracted data. We are not aware the extent to which data obtained via extraction is shared with third parties.

The data protection principles are set out in Schedule 1 and the conditions for lawful processing set out in Schedules 2 and 3 of the DPA .

Under Schedule 1:

- Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –
    - (a) at least one of the conditions in Schedule 2 is met, and
    - (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met
- Personal data shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes.
- Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
- Personal data shall be accurate, and where necessary, kept up to date.
- Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

[3] https://motherboard.vice.com/en_us/article/3daywj/hacker-steals-900-gb-of-cellebrite-data

Company Limited by Guarantee (England & Wales): 4354366
Registered Charity (England & Wales): 1147471

- Personal data shall be processed in accordance with the rights of data subjects under this Act.
- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
- Personal data shall not be transferred to a country or territory outside the EEA unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Schedule 2 sets out the conditions for processing personal data:

1. The data subject has given his consent to the processing;
2. The processing is necessary –
   a. For the performance of a contract to which the data subject is a party, or
   b. For the taking of steps at the request of the data subject with a view to entering into a contract.
3. The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.
4. The processing is necessary in order to protect the vital interests of the data subject.
5. The processing is necessary –
   a. For the administration of justice,
   b. For the exercise of any functions conferred on any person by or under any enactment,
   c. For the exercise of any functions of the Crown, a Minister of the Crown or a government department, or
   d. For the exercise of any other functions of a public nature exercised in the public interest by any person.
6. (1) The processing is necessary for the purposes of legitimate interests persuaded by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interest of the data subject.
   (2) The Secretary of State may by order specify particular circumstances in which this condition is, or is not, to be taken to be satisfied.

Schedule 3 sets out the conditions for processing sensitive personal data:

1. The data subject has given his explicit consent to the processing of the personal data.

Company Limited by Guarantee (England & Wales): 4354366
Registered Charity (England & Wales): 1147471

2. (1) The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment.
   (2) The Secretary of State may by order –
   (a) exclude the application of sub-paragraph (1) in such cases as may be specified, or
   (b) provide that, in such cases as may be specified, the condition in sub-paragraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.

3. The processing is necessary –
   (a) In order to protect the vital interests of the data subject or another person, in a case where –
      i. Consent cannot be given by or on behalf of the data subject, or
      ii. the data controller cannot reasonably be expected to obtain the consent of the data subject, or
   (b) In order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld.

4. The processing –
   (a) Is carried out in the course of its legitimate activities by any body or association which –
      (i) Is not established or conducted for profit, and
      (ii) Exists for political, philosophical, religious or trade-union purposes,
   (b) Is carried out with appropriate safeguards for the rights and freedoms of data subjects,
   (c) Relates only to individuals who either are members of the body or association or have regular contact with it in connect with its purposes, and
   (d) Does not involve disclosure of the personal data to a third party without the consent of the data subject.

5. The information contained in the personal data has been made public as a result of steps deliberately taken by the data subject.

6. The processing –
   (a) Is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings),

Company Limited by Guarantee (England & Wales): 4354366
Registered Charity (England & Wales): 1147471

(b) Is necessary for the purpose of obtaining legal advice, or
(c) Is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

7.
(1) the processing is necessary –
(a) for the administration of justice,
(b) for the exercise of any functions conferred on any person by or under an enactment, or
(c) for the exercise of any functions of the Crown, a Minister of the Crown, or a government department.
(2) The Secretary of State may by order –
(a) Exclude the application of sub-paragraph 91) in such cases as may be specified, or
(b) Provide that, in such cases as may be specified, the condition in sub-paragraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.

8. (1) The processing is necessary for medical purposes and is undertaken by ….

Further conditions are set out in the various statutory instruments made under paragraph 10 of Schedule 3.

Application of the Principles

In relation to the **first data protection principle**, "*Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –*

- *(a) at least one of the conditions in Schedule 2 is met, and*
- *(b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met."*

(a) Fairness

We note that fair processing requires transparency and information about the processing. As we note in the report, there has been a complete absence of consultation, independent oversight and transparency in relation to mobile phone extraction use, in particular the roll-out at local police stations via Self-Service Kiosks and Hubs.

Company Limited by Guarantee (England & Wales): 4354366
Registered Charity (England & Wales): 1147471

In order to be fair, the outcome of processing also must not be discriminatory to a particular group of Data Subjects.

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."*

(b) Lawfulness

In relation to lawfulness of the processing, there is a lack of clear statutory basis. As noted in our report, the few forces who disclosed local policies revealed contradicting beliefs as to the lawful basis.[4]

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

Company Limited by Guarantee (England & Wales): 4354366
Registered Charity (England & Wales): 1147471

We address other potential breaches below, however, it is clear that absent a proper legal basis, the collection of this personal data is in breach of the Data Protection Act 1998.

We note the reliance on section 20 PACE by the National Police Chief's Council, which we do not believe constitutes a valid legal basis for this collection. 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.

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

> "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.

(c) Potential exemption

It is noted that §29 exempts the first data protection principle in any case to the extent to which the application of those provisions to the data would be likely to prejudice prevention or detection or crime; apprehension or prosecution of offenders. However, compliance is still required with conditions in Schedule 2 and 3. In addition, it would be necessary to consider to what extent the effect is likely, in each case, to cause prejudice.

The ICO guidance states:

Company Limited by Guarantee (England & Wales): 4354366
Registered Charity (England & Wales): 1147471

"… the exemption applies, in any particular case, only to the extent that applying those provisions would be likely to prejudice the crime and taxation purposes. You need to judge whether or not this effect is likely in each case – you should not use the exemption to justify withholding subject access to whole categories of personal data if for some individuals the crime and taxation purpose are unlikely to be prejudiced."

"Personal data is also exempt from the non-disclosure provisions if:
- *the disclosure is for any of the crime and taxation purposes; and*
- *applying those provisions in relation to the disclosure would be likely to prejudice any of the crime and taxation purposes.*

The Act does not explain "likely to prejudice". However, our view is that for these exemptions to apply, there would have to be a substantial chance (rather than a mere risk) that complying with the provision would noticeably damage one or more of the crime and taxation purposes."

The ICO guidance goes on to note that if challenged the data controller must be prepared to defend their decision to apply the exemption.

In relation to the **second data protection principle**, that "*Personal data shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes.*"

We note, as mentioned, the apparent absence of one or more specified and lawful purposes. There is no national guidance to assist and the local guidance disclosed is contradictory.

We note issues around 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

Company Limited by Guarantee (England & Wales): 4354366
Registered Charity (England & Wales): 1147471

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."

Further, there is a lack of clarity on retention and deletion periods.

In relation to **the third data protection principle**, "*Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed*".

We are concerned that data cannot be limited during the extraction process.

As noted in our report and above, the Metropolitan Police disclosure states that it is not possible to limit what is extracted nor to isolate data that relates to specific date periods.

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[5].

In relation to the **fifth data protection principle,** "personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes."

Again, the lack of regulation of mobile phone extraction means there are no clear limits on how long the extracted data may be retained.

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

[5] page 9, https://privacyinternational.org/sites/default/files/2018-03/Digital%20Stop%20and%20Search%20Report.pdf
[6] page 28, https://privacyinternational.org/sites/default/files/2018-03/Digital%20Stop%20and%20Search%20Report.pdf

Company Limited by Guarantee (England & Wales): 4354366
Registered Charity (England & Wales): 1147471

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 by comparison the continued retention by the police of custody images and the recent announcement of the Science and Technology Committee of a probe into the failure to act almost six years after it was ruled unlawful by the High Court[9]. We believe that this should be a red flag in relation to whether the police may be in breach of the requirement to keep personal data for no longer than necessary, with respect to mobile phones. We note that Norman Lamb made the below statement, in relation to custody images, but which could apply to personal data extracted from mobile phones:

> "There are no real rules surrounding this. The police can store these facial images without any proper consideration of them, which raises fundamental significant civil liberty issues about what they are retaining about us. It includes people who have not been charged with any crime, or people who have been exonerated."

Given the issues we have identified, we do not believe there is or was compliance with the **sixth data protection principle** that "Personal data shall be processed in accordance with the rights of data subjects under this Act".

[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] http://www.independent.co.uk/news/uk/politics/police-mugshots-storing-not-charged-unlawful- home-office-minister-government-norman-lamb-a8168256.html

Company Limited by Guarantee (England & Wales): 4354366
Registered Charity (England & Wales): 1147471

Should access rights be applicable, given that individuals are in many cases unaware that data has been extracted, they are unable to exercise their access rights. This includes those individuals who are not the owner of the phone but whose data can be extracted from someone else's phone.

Even where individuals may be aware or may have given their passcode or pin number to access the phone, we question the level of informed consent. Given the lack of transparency it is unclear whether individuals are aware of the extent of data that can be extracted, informed of the types of data extracted or informed of their rights in relation to their data.

The **seventh data protection principle** requires that "Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data."

However, 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 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]

[10] https://www.theguardian.com/uk-news/2017/may/04/greater-manchester-police-

Company Limited by Guarantee (England & Wales): 4354366
Registered Charity (England & Wales): 1147471

In relation to the **eighth data protection principle** "Personal data shall not be transferred to a country or territory outside the EEA unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data," we are not aware whether personal data is being transferred outside the EEA and if it is what, if any, safeguards are in place.

Consent

We acknowledge that in some instances the police may seek consent from individuals prior to extracting data from their phones, for example by seeking their passcode / password. We do not believe that consent, in the context of mobile phone extraction, is compliant with the Data Protection Act. Consent, as defined in the Directive 95/46/EC – Article 2(h) states that:

> "the data subject's consent shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed."

Thus, consent must be freely given, with no coercion, informed, thus no ambiguity, specific to particular circumstances and involve a positive indication of Data Subject's wishes. We have seen no evidence to demonstrate consent would be informed, specific or free – given the clear imbalance of power between an individual and the police.

Further, we note the relevance of §53 Regulation of Investigatory Powers Act 2000 where it is an offence where a person fails to disclose passwords / passcodes. Thus, there exists the element of coercion.

Legal obligation / administration of justice

Whilst this technology is being operated by the police, it is evident that there is lack of clarity as to the legal basis upon which to they rely to use this technology. This undermines reliance, for example on 5(b) Schedule 2 and 7(b) Schedule 3 'exercise of any functions conferred on any person by or under any enactment.'

fined-victim- interviews-lost-in-post

Company Limited by Guarantee (England & Wales): 4354366
Registered Charity (England & Wales): 1147471

The National Police Chief's Council[11] 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)[12].

The reliance of some forces on section 20 of the Police and Criminal Evidence Act 1984 is unacceptable. This 34-year-old law significantly pre-dates the use of smartphones and indeed the entire digital era. Sir Peter Fahy, former Chief Constable of Greater Manchester Police agrees[13] 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.

Data Protection Bill

Part 3 of the draft Data Protection Bill currently progressing through Parliament implements the Law Enforcement Directive on the processing of personal data, which will replace the DPA for the processing of personal data by the police (as competent authorities) for law enforcement purposes as of May 2018. The provisions are similar to but strengthen and update those in the DPA. We therefore rely on our submissions made above in relation to the Data Protection Act 1998 and elaborate further in relation to the Data Protection Bill where appropriate.

Under Chapter 2 of Part 3 of the Data Protection Bill ["the Bill"], the six data protection principles are identified as:

- *Requirement that processing be lawful and fair*
- *Requirement that purposes of processing be specified, explicit and legitimate*
- *Requirement that personal data be adequate, relevant and not excessive.*
- *Requirement that data be accurate and kept up to date*
- *Requirement that personal data be kept for no longer than is necessary*

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

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

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

Company Limited by Guarantee (England & Wales): 4354366
Registered Charity (England & Wales): 1147471

- *Requirement that personal data be processed in a secure manner*

In relation to the first principle, the "*Requirement that processing be lawful and fair*", the Bill requires that in order to be lawful, processing is based on law and either –

(a) The data subject has given consent to the processing for that purpose, or
(b) The processing is necessary for the performance of a task carried out for that purpose by a competent authority.

As we have noted in detail above, we believe it is questionable whether the processing of data by the police using mobile phone extraction technology is based on law. Secondly, we question whether consent can be freely given if consent is obtained. If consent is not obtained processing must be necessary for the performance of a task carried out by a competent authority (i.e. the relevant police force). Given the volume of data that can be extracted and the lack of clarity as to whether all data of a particular type must be taken without time limitations, we believe there are questions to answer regarding the necessity of processing all this data.

We have noted that a large amount of the data extracted is likely to be sensitive. In these cases, processing is only permitted:

> "The first is where –
> (a) The data subject has given consent to the processing for the law enforcement purpose …
> (b) At the time when the processing is carried out the controller has an appropriate policy document in place."
>
> The second case is where –
> (a) The processing is strictly necessary for the law enforcement purpose,
> (b) The processing meets at least one of the conditions in Schedule 8, and
> (c) At the time when processing is carried out, the controller has an appropriate policy document in place."

As above, we question whether the processing is based on consent, whether it is strictly necessary and whether any other condition for sensitive processing is met. Furthermore, as we have noted in our report, few forces have a local policy and those policy documents that do exist are inadequate and would not

Company Limited by Guarantee (England & Wales): 4354366
Registered Charity (England & Wales): 1147471

meet the requirements of an appropriate policy document as specified in the Bill. We note the requirements in sensitive processing that the document:

> "(a) explains the controller's procedures for securing compliance with the data protection principles in connection with sensitive processing in reliance on consent of the data subject or in reliance on the condition in question, and
> (b) explains the controller's policies as regards the retention and erasure of personal data processed in reliance on the consent of the data subject or (as the case may be) in reliance on the condition in question, giving an indication of how long such personal data is likely to be retained."

We are not aware of any policies that meet these requirements. There is a complete absence of national guidance.

In relation to the second principle, the "*Requirement that purposes of processing be specified, explicit and legitimate*", we note our concerns regarding the absence of specific and explicit purpose and further question on what legal basis the extraction of personal data from mobile phones is legitimate. We are concerned that officers may not be authorised by law to process the data for any law enforcement purpose, let alone for other purposes.

The lack of independent oversight of the use of these technologies results in an absence of information as to whether in practice processing has been necessary and proportionate, including for other purposes.

The third principle is the "*Requirement that personal data be adequate, relevant and not excessive*", we have already set out above our concerns regarding the excessive and indiscriminate collection of data through mobile phone extraction.

The fourth principle is the "*Requirement that personal data be accurate and kept up to date*. The Bill specifies that in processing personal data for any of the law enforcement purposes, a clear distinction must be made between personal data relating to different categories of data subject, such as persons suspected of having committed of being about to commit a criminal offence, persons convicted of a criminal offence, persons who are or may be victims of a criminal offence and witnesses or other persons with information about offences. As far as we are aware no such distinction is made, and data is extracted wholesale from devices.

Company Limited by Guarantee (England & Wales): 4354366
Registered Charity (England & Wales): 1147471

In relation to the fifth data protection principle, the "*Requirement that personal data be kept for no longer than is necessary*" we note submissions above that there are no retention periods. According to the Bill, appropriate time limits must be established for the periodic review of the need for the continued storage of personal data for any of the law enforcement purposes. We do not believe this is taking place.

Our concerns regarding the sixth principle, the "*Requirement that personal data be processed in a secure manner*", are set out in the detail in relation to the DPA.

In relation to the 'rights of the data subject' we have raised above our concern in relation to instances where the individual is not informed data has been extracted from their phone; and the concern that many individuals' data will be obtained and retained by the police purely as a result of their interaction with the owner of the device. This effectively extinguishes the rights of the data subject.

The Bill puts certain obligations on controllers. We believe that police forces are failing in their role as data controllers to:

- Have legal basis upon which to use mobile phone extraction technologies;
- Implement appropriate technical and organisational measures to ensure, and to be able to demonstrate, that the processing of personal data complies with the requirements of Part 3 of the Bill.
- Include data protection policies.
- Implement appropriate technical and organisational measures which are designed to implement data protection principles in an effective manner, and to integrate into the processing itself the safeguards necessary for that purpose.
- Implement appropriate technical and organisational measures for ensuring that, by default, only personal data which is necessary for each specific purpose of the processing is processed. This applies to the amount of personal data collected, the extent of its processing, the period of its storage and its accessibility.

In addition, controllers must maintain a record of all categories of processing activities for which the controller is responsible. This must include the purposes of the processing and description of the categories of personal data.

Company Limited by Guarantee (England & Wales): 4354366
Registered Charity (England & Wales): 1147471

We believe that the type of processing is likely to result in a high risk to the rights and freedoms of individuals. In accordance with the Bill, the controller must prior to processing, carry out a data protection impact assessment. This must include:

(a) A general description of the envisaged processing operations;
(b) An assessment of the risks to the rights and freedoms of data subjects;
(c) The measure envisaged to address those risks;
(d) Safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this part, taking into account the rights and legitimate interests of the data subjects and other persons concerned.

Lack of independent oversight

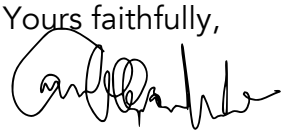
We note with concern that given the use of mobile phone extraction has largely been under the radar. There has been a lack of reviews into the use of this technology. The absence of independent oversight means that many failings, breaches of data protection principles, misuse and abuse of personal data and sensitive personal data will not have been identified.

We have written to every Police and Crime Commissioner in England and Wales and the Northern Ireland Board of Policing asking them to review the practice of mobile phone extraction within the relevant force for which they have responsibility.

We have also written to the Home Office and submitted within our recommendations that we believe there should be statutory independent oversight of the use of this technology.

However, it is extremely important, for all the reasons set out above, that this matter is investigated from a data protection perspective by the ICO as the independent data protection regulator and we look forward to hearing from you in this regard.

Yours faithfully,



Camilla Graham Wood
Privacy International

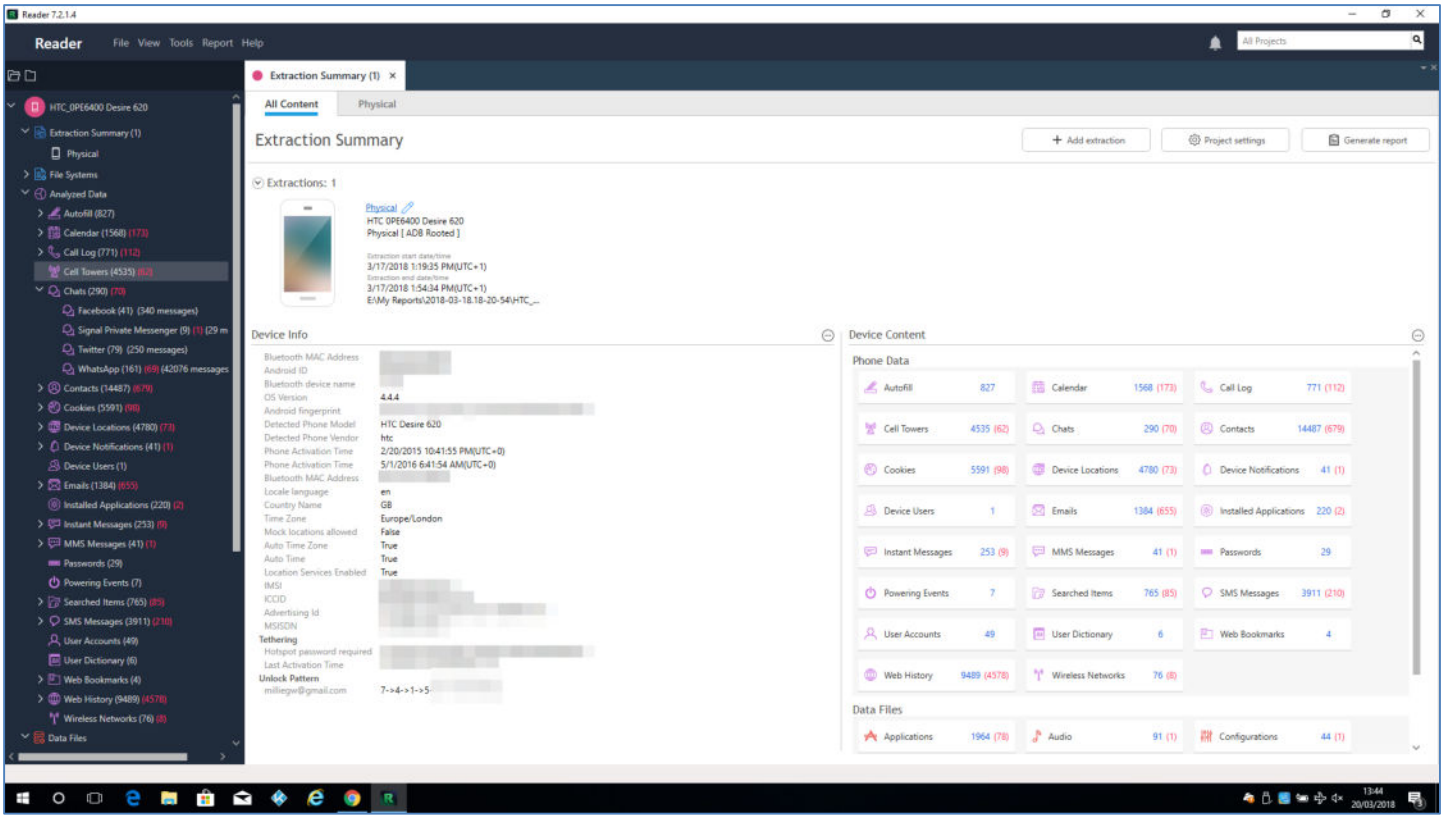
Company Limited by Guarantee (England & Wales): 4354366
Registered Charity (England & Wales): 1147471

Enc.
Letter to Home Office

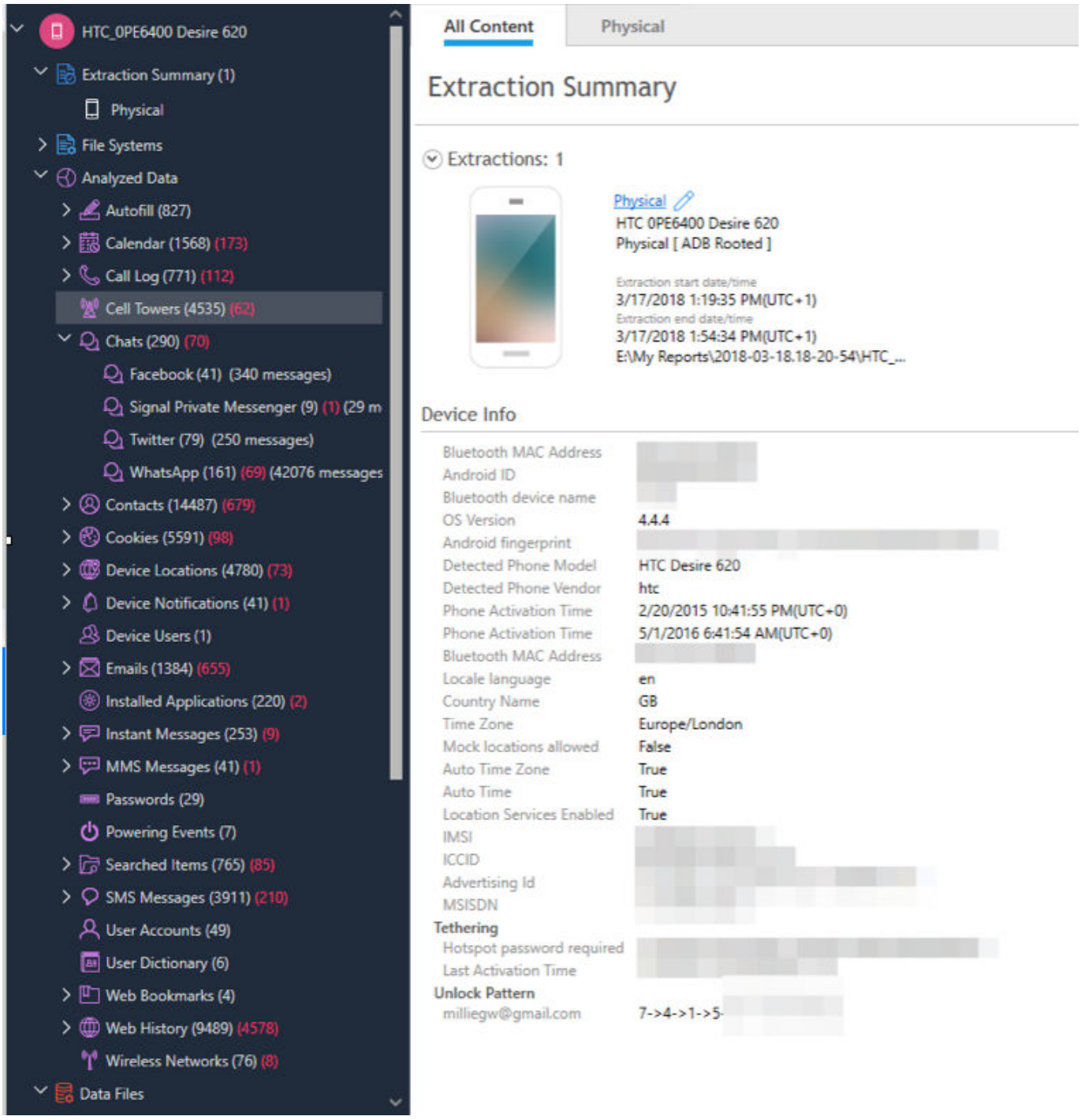
Company Limited by Guarantee (England & Wales): 4354366
Registered Charity (England & Wales): 1147471

Annex 1

HTC Desire

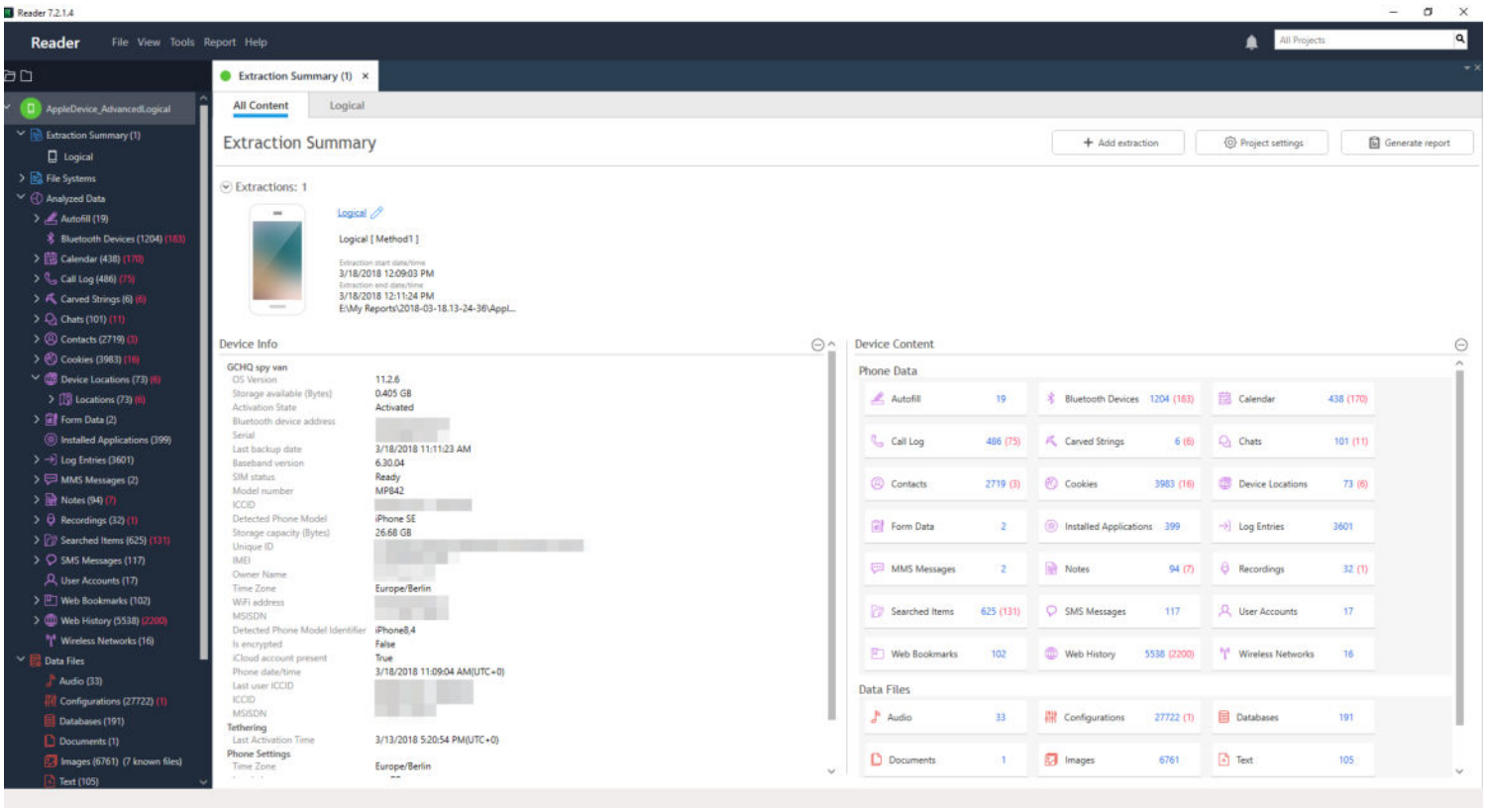


Company Limited by Guarantee (England & Wales): 4354366
Registered Charity (England & Wales): 1147471

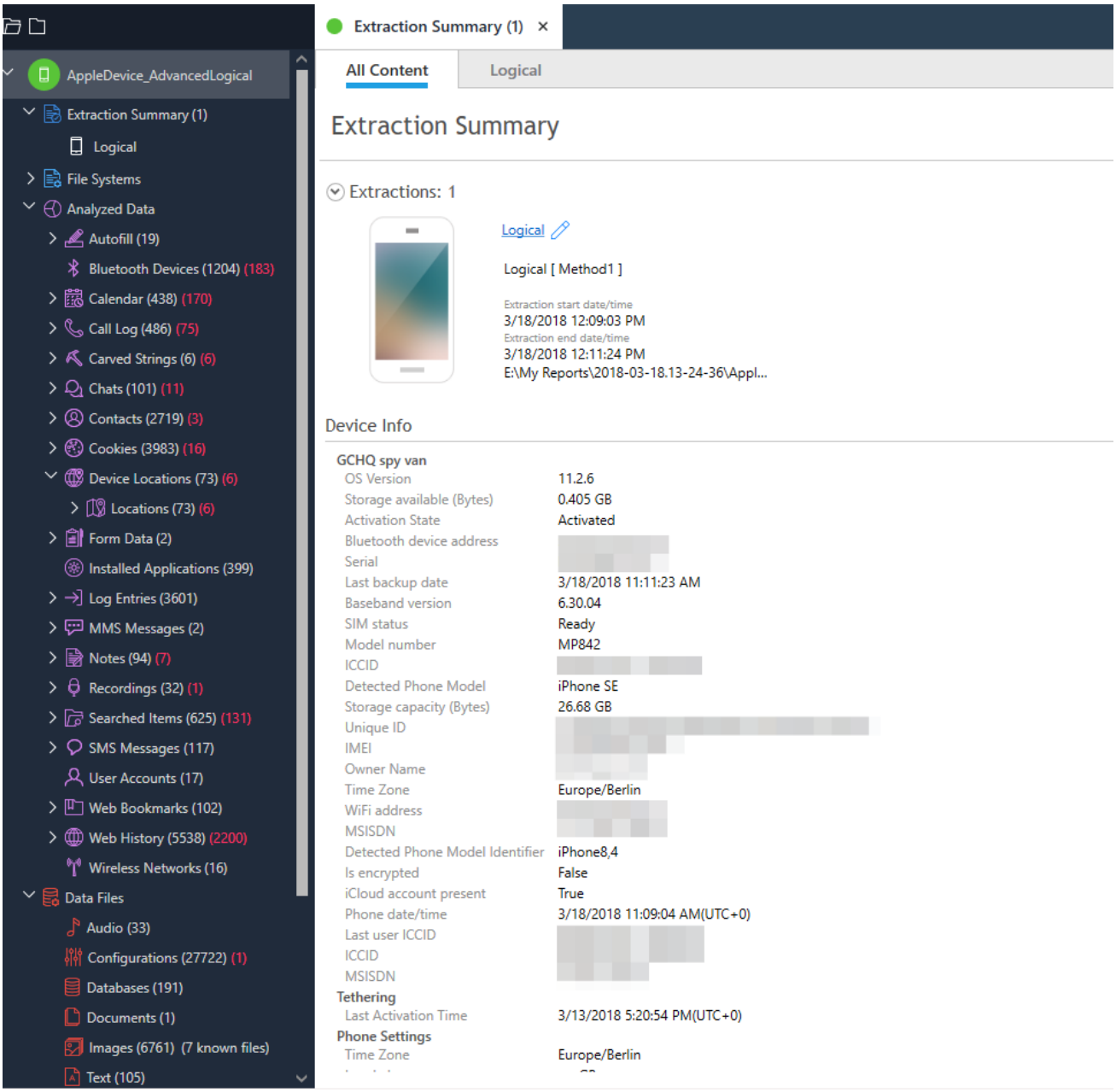


Company Limited by Guarantee (England & Wales): 4354366
Registered Charity (England & Wales): 1147471

iPhone SE



Company Limited by Guarantee (England & Wales): 4354366
Registered Charity (England & Wales): 1147471



Company Limited by Guarantee (England & Wales): 4354366
Registered Charity (England & Wales): 1147471