PRIVACY INTERNATIONAL

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

Lord Justice Sir Adrian Fulford
IPCO
PO Box 29105
London
SW1V 1ZU

via email: info@ipco.gsi.gov.uk

1st August 2018

Dear Lord Justice Fulford,

RE: Digital stop and search: regulatory and oversight issues

We attach a copy our report, "Digital Stop and Search: how the UK police can secretly download everything from your mobile telephone" (the Report).

Introduction

We are concerned that the use of mobile phone extraction technology (the technology) by the police may in some (or all) circumstances constitute either an interception of communications, related communications data or communications data (for simplicity's sake referred to as "interception of communications") or equipment interference (EI). If it does, then the conduct engaged in is subject to your oversight.

Based on our research, we are not aware that police forces have applied for authorisation for extraction under the Regulation of Investigatory Powers Act 2000 (RIPA 2000) or now under the Investigatory Powers Act 2016 (IPA 2016) as would be required if extraction constituted interception or EI. We note that the Report was compiled prior to the commencement of the Investigatory Powers Act 2016 (IPA 2016) but in our view, there is no material difference in the interception provisions that replace those referred to below. The IPA notably includes a new targeted EI warrant provision which was not present in previous law, calling into question all police EI activities prior to the commencement of the IPA 2016, Part 5.

The report examines the use by police forces of the technology, which, in summary, enables them to download the entire content of an individual's phone – whether suspect, witness or victim – often without their knowledge or consent. The use of the

technology involves the extraction, retention and analysis of the content of communications, relevant communications data and communications data.

The report focused on the use of Self Service Kiosks (SSK), Hubs (which can serve a number of forces) and mobile extraction kits to extract data. We note that some forces use the technology to extract data without distinction in both low level and serious crimes. In this context we invite you to consider the content of this letter in light of the decision of *The Secretary of State for the Home Department v Watson and Others* C-698/15.

Based on our research, it is clear that the legal basis upon which police forces rely on in order to engage in this conduct is, at best, confused and at worst, plainly wrong. The apparent failure of the Home Office to address this serious situation is inexcusable. We hope you will be in a position to confirm the conduct falls within your remit and critically assess its legality.

We are concerned that:

- The use of mobile phone extraction constitutes either or both the interception of communications or EI.
- There may have been a failure by the police to properly authorise the use of mobile phone extraction that constituted an interception under RIPA 2000.
- That no foreseeable and accessible legal regime was in place to authorise mobile phone extraction that constituted EI prior to the enactment of IPA 2016, Part 5 – and that Part 5 still does not accord with the requirements of Article 8 and 10 of the European Convention on Human Rights (ECHR).
- There is a lack of independent oversight of the use of this technology.
- The use of this technology prior to the creation of the IPCO should have fallen within the statutory oversight of one or more of your predecessors.
- The current use of the technology should fall within the remit of the IPCO, but it is not clear your oversight is being applied.

We recommend that you:

- Conduct an urgent review into the use of the technology by the police, including by, if necessary, consulting the Technology Advisory Panel.
- Conduct an urgent review into the legal basis for the use of the technology by the police, as well as its necessity and proportionality.

What is mobile phone extraction: a summary

The Report sets out the nature and scope of extraction. In summary:

- It exists for the purposes of recovering digital data from mobile devices
- The police can save the “memory dump” obtained and analyse it
- An extraction report may, subject to the nature of the technology used, be generated
- Investigators are able to see at a glance an individual’s location, who they speak to and when, and potentially vast amounts of other personal and intrusive information (including emails, pictures, diary entries and much else) both about

the individual and those with whom that person interacts, both actively and passively

The Report includes descriptions from some of the companies with which the police contract[i]. The intrusiveness of mobile phone extraction can be best encapsulated by one of those companies, MSAB, which claims that, "If you've got access to a SIM card, you've got access to the whole of a person's life."[1]

An idea of its scope can be seen in the Cellebrite F-UFD-15-032 UFED Infield Kiosk Logical, acquired by Avon and Somerset Police. This provides the ability to decode data from more than 1,500 mobile applications in minutes. [2]

Types of data extracted

The technology enables the collection, retention and use of vast quantities of content and data, including personal and sensitive personal data of both the device user and many others with whom the user interacts.

There is the additional risk that data extracted could include items subject to legal professional privilege and journalistic material as those terms are defined in sections 263 and 264 of the Investigatory Powers Act 2016 (IPA 2016).

Disclosure we have received from the UK police forces in response to Freedom of Information requests 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 geo tag 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 and 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 A is the extracted data from an HTC android phone and an 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

[1] https://www.msab.com/2016/01/21/xry-demo-at-uk-cybercrime-pilot/ accessed 3.07.2017

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

data. MSAB, another company with whom a number of UK police forces contract, has a product XRY Physical that allows access to “system and deleted data.”

The ability to access hidden and deleted data, beyond the knowledge of the user, may also be relevant to determining whether the conduct constitutes covert surveillance under Part II of RIPA 2000, requiring either separate or combined authorisation.

There are three different extraction processes provided by a Cellebrite UFED Touch 2, being logical, file system and physical.

A physical extraction was carried out on the HTC device and logical extraction on the iPhone (see Annex A) and extracted:

- Autofill
- Bluetooth Devices
- Calendar
- Call Log
- Carved Strings[3]
- Cell Towers to which the phone had connected
- Chats: Facebook; Signal PM; Twitter; WhatsApp
- Contacts
- Cookies
- Device locations
- Device notifications
- Device users
- Form Data
- Emails
- Log Entries
- 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 parts of the device” and access to hidden and deleted data.

Legal basis

[3] https://forensicswiki.org/wiki/File_Carving

It is of serious concern that amongst the various police forces that have disclosed their local guidance, there is uncertainty and inconsistency as to the legal basis under which they can extract data from mobile phones: see pages 20-24 of the Report.

The National Police Chief's Council[4] has stated that police use of mobile phone kiosks is governed by s. 20 of the Police and Criminal Evidence Act 1984 ("PACE"), which grants police the "power to require any information stored in any electronic form". However, s. 20, PACE is a power exercisable only (a) on premises; and (b) by "a constable who has entered [those] premises in the exercise of a power conferred by an enactment". We do not consider that s. 20 PACE, which is parasitic on lawful entry onto premises can apply in anything other than a specific set of narrow circumstances.

The Metropolitan Police Service relies on ss. 18,19,22 and 32 PACE and the Wiltshire Police on s. 32 PACE as possible legal bases for the use of the technology. However, these provisions generally relate to powers on premises contingent on a lawful basis existing for the presence of officers for the purposes of exercising them. The power in s. 32 is exercisable only on arrest.

British Transport Police informed us that, "primarily the legislation relied upon would be the Police and Criminal Evidence Act 1984, Misuse of Drugs Act 1971 and the Coroners and Justice Act 2009". The complete absence of reference to any specific power relied upon is of considerable concern, in particular, following the recent findings of the Investigatory Powers Tribunal against this force in *Davies v British Transport Police* [IPT/17/93/H].

We believe urgent consideration is needed, particularly in the context of whether mobile phone extraction could constitute an interception of communications and/or EI and in particular as to the former, whether section 20 PACE (or other PACE provisions relied upon by other police forces) constitutes the exercise of a "statutory power" for the purposes of section 1(5)(c) RIPA 2000 or section 6(1)(c)(ii) IPA. Further, we believe that the extreme intrusion caused by mobile phone extraction should not be so readily permitted. Instead, even when incident to lawful entry onto premises or an arrest, it must be separately authorised by a warrant that strictly assesses the necessity and proportionality of the intrusion.

Consent

The information we have obtained reveals that consent is not always sought. British Transport Police informed us in response to a question whether they 'seek consent from individuals, whether victim, witness or suspect, before you extract data from their device' that "victims and witnesses would be asked for their consent".

The guidance provided by Derbyshire Constabulary indicates that extraction is often carried out without the device user's knowledge, stating:

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

> "The acquisition and storage of people's personal data without their knowledge is something that public services should only do when it is lawful to do so. There is no requirement to keep all data from examinations. Officers need to understand and assess whether it is proportionate to keep this data.
>
> Acquisitions will be kept in line with current MOPI time frames and the data produced will form part of a crime or summons file. If there are no criminal charges or no further action is taken then officers should only keep personal data on individuals where it can be evidenced through either crime or intelligence that they are linked to criminality. There is no requirement to place all contacts of an individual or Guardian where there is no evidence to support their link to criminality."[5]

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 or password. We do not believe however that consent, in the context of mobile phone extraction, is informed and sufficient to authorise the intrusion. 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.

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."

Consent must be freely given, with no coercion, informed (and therefore must be given without ambiguity), specific to particular circumstances and involve a positive indication of the 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.

If UK authorities are to be permitted to access information extracted from mobile phones in secret or without consent, the European Convention of Human Rights Articles 8 and 10 require there to be a sufficiently precise legal regime in place which contains adequate information as to the basis for state interference with the rights in question and which provides safeguards against abuse of power and arbitrary use. In our view, there is no such regime in place governing the use of the technology.

In the context of the interception of communications, consent has particular legal significance (see below).

Interception and EI

Police forces have given limited if any consideration to the potential that use of mobile phone extraction could constitute an interception of communications or EI. Of the few

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

forces who have a local policy, only two explicitly reference RIPA 2000: Wiltshire Police and Gwent Police.

Wiltshire Police's policy provides that:

> "In relation to forensic examinations it is important to be aware that s.1 of the Regulation of Investigatory Powers Act 2000 makes it an offence for any person to intentionally and without lawful authority, intercept a communication in the course of its transmission. Under this Act a communication also includes stored communications such as e-mail, voice mail, text messages awaiting delivery to the handset and answer phone messages … In order to access any of this information there must be a lawful power to do it, e.g. search warrant, production order, examination of an item seized as evidence with consent and an authorisation for directed surveillance or by way of an intercept warrant."

Gwent Police's policy provides that "once in police possession any calls, texts or data transfers received by the device may constitute a communication breach in relation to RIPA."

In passing, whilst of some reassurance that reference is made to RIPA 2000, Wiltshire Police refer to "forensic examination" (as opposed to extraction) and the policy is plainly wrong in implying that only communications "awaiting delivery" are caught by the provisions: *R v Coulson* [2013] WLR (D) 262 (see further below). Reference by Gwent Police to a "communication breach" as opposed to a criminal offence is also of concern.

Interception

Privacy International has sought to provide transparency in relation to the widespread use of mobile phone extraction by the police. However, we are limited in what we have been able to uncover and the level of detail, utilising the power of the Freedom of Information Act 2000.

We therefore encourage you and your office to carry out an investigation into the extent to which mobile phone extraction constitutes interception in certain circumstances.

We note for example, that it may require consideration of how the process operates, the software and hardware used; the data extracted; the extraction of content and communications data and the implications of communications content and communications data being received after the phone has been seized and/or during the course of an extraction.

If use of mobile phone extraction constitutes interception of phone calls, emails, web-browsing and other communications of individuals living in the UK, the authorities should have complied with the legal regime set out in the RIPA 2000, which is now being replaced by the IPA 2016.

RIPA Part I Chapter I covers the interception of communications. The interception of communications requires a warrant to be issued by the Secretary of State pursuant to s. 5, RIPA 2000, unless there is some other legal basis that makes it lawful. Section 5 sets out the conditions for the granting of a warrant, including that it is necessary on grounds of national security, or for the purpose of preventing or detecting serious crime or other grounds set out in section 5(3). Part I Chapter II RIPA 2000 provides for the acquisition, retention and disclosure of "communication data", namely data held by a person providing a telecommunication service (section 21(4)).

Section 1 of RIPA 2000 creates the offence of unlawful interception where the interception takes place in the course of its transmission intentionally and without lawful authority. Lawful authority is provided for in ss. 3 and 4. This includes consent: s 3(1)(a)-(b) and (2)(a) RIPA 2000. It is important to note that in the present context consent of the person sending the communication is not sufficient and must include the intended recipient. Where only the sender consents, concurrent authority under Part II RIPA 2000 is mandatory.

Section 2(2) RIPA 2000 defines interception in the course of its transmission. It is now established, following *Coulson* that:

> 26. The scope of the provision is put beyond doubt, in our view, by the reference in section 2(7) to the system by means of which "the communication is being, or has been, transmitted". The words "has been transmitted" are totally inconsistent with the appellants' suggestion that the extension is limited to transient storage prior to first access. These words make entirely clear that the **course of transmission may continue notwithstanding that the voicemail message has already been received and read by the intended recipient.**
>
> 28. Furthermore, we are led to the same conclusion on the application of the mischief rule. As Fulford L.J. put it:
>
> > "I accept, therefore, that the period of storage covered by the section does not come to an end on first access or collection by the intended recipient, but it **continues for so long as the system is used to store the communication**, **and whilst the intended recipient has access to it in this way**. In a comprehensive fashion, this covers the vice that in my view the provision was intended to address, namely unauthorized access to communications, whether oral or text, whilst they remain on the system by which they were transmitted. As the prosecution submits, unlawful access and intrusion is not somehow less objectionable because the message has been read or listened to by the intended recipient before the unauthorized access takes place."

The Interception of Communications Code of Practice 2016[6] states:

---

6 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/496064/53659_CoP_Communications_Accessible.pdf

3.8 Section 2 of RIPA defines 'telecommunication service' as any service that consists in the provision of access to, and of facilities for making use of, any telecommunication system. Section 2(8A) of RIPA makes clear that any service which consists in or includes facilitating the creation, management or storage of communications transmitted, or that may be transmitted, by means of such a system are included within the meaning of 'telecommunications service'. Internet based services such as web-based email, messaging applications and cloud-based services are, therefore, covered by this definition. The definition of a 'telecommunications service' in RIPA is intentionally broad so that it remains relevant for new technologies.

3.22 Section 2(7) of RIPA defines a communication in the course of its transmission as including any time **when the communication is being stored on the communication system** in such a way as to enable the intended recipient to collect it or otherwise have access to it. **Making the contents of a communication stored in this way available to a person other than the sender or intended recipient therefore constitutes interception.** A communication remains in the course of its transmission regardless of whether the communication has previously been read, viewed or listened to. A communication stored in this way remains in the course of its transmission.

3.23 Stored communications may also be accessed by means other than a warrant. For example, if a communication has been stored on a communication system it may be obtained with lawful authority by means of an existing statutory power such as a production order (under the Police and Criminal Evidence Act 1984) or a search warrant. A production order is an order from a circuit judge who must be satisfied that i) an indictable offence has been committed, ii) the person holds the material and iii) the material will be of substantial value to the investigation and iv) it is in the public interest that the material should be produced.

The Interception of Communications draft Code of Practice dated February 2017[7] (reflecting the position under the IPA 2016) is not materially different as to the definition of interception.

We believe, the research upon which the Report is based, and the provisions set out in RIPA 2000, demonstrates that an interception of communications may occur through mobile phone extraction. Given the paucity of information we have received from the police as to how they use this technology we are not able to take our analysis further than we have but, in our view, significant and serious issues have been sufficiently highlighted such to justify our invitation for you to investigate the matter. To be clear, this is not limited to the possibility of offences having been committed or a failure to obtain proper consent of both parties to the communication or concurrent authority under Part II RIPA but has significant implications for any criminal charges brought or proceedings instituted where the fruits of a download have been relied upon as part of the evidence in the case. This is the effect of s. 17 RIPA and case law.

---

7 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/593748/IP_Act_-_Draft_Interception_code_of_practice_Feb2017_FINAL_WEB.pdf

Furthermore, on the subject of criminal proceedings, we are concerned in light of the public debate on the subject of disclosure and the recent publication of the Justice Committee's report[8] that, in many cases, there may have been a failure to deal with digital downloads in accordance with the Criminal Procedure and Investigations Act 1996.

We have considered the position under the IPA 2016 and do not consider any of the provisions in this Act materially changes the concerns raised above.

EI

In addition, or alternatively, Privacy International considers the use of the technology constitutes EI. If it does, the effect of the decision in *Privacy International v Secretary of State for Foreign and Commonwealth Affairs* [IPT 14/85/CH], is that such conduct was at least unlawful in relation to the intelligence services prior to the publication of the EI Code of Practice in March 2015.

The effect of EI is that it constitutes a trespass or criminal offence in respect of the property (for example under the Computer Misuse Act 1990). Prior to the IPA coming into force, there was no legally accessible and foreseeable power under which the police could obtain an EI warrant. While the government has claimed the police could obtain warrants to authorise EI under PA 1997, Part III, we disagree this power was sufficiently clear with necessary safeguards to satisfy the requirements of Articles 8 and 10 of the ECHR.

We also question the legality, necessity and proportionality of targeted EI warrants issued under IPA 2016, Part 5[9]. That concern does not, however, excuse the police for obtaining such warrants when they carry out EI, which we think includes use of the mobile phone extraction technology.

The Equipment Interference Code of Practice[10] issued under the IPA 2016 states:

> 2.2 The definition of equipment is technology neutral. Examples of the types of equipment captured by the definition include devices that are "computers" for the purposes of the CMA, such as … smart phones…"
>
> 3.2 … Equipment interference can be carried out either remotely or by physically interacting with the equipment.

---

[8] https://www.parliament.uk/business/committees/committees-a-z/commons-select/justice-committee/inquiries/parliament-2017/disclosure-criminal-cases-17-19/

[9] https://privacyinternational.org/report/1150/privacy-international-submission-science-and-technology-committee-draft-investigatory

http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/draft-investigatory-powers-bill-committee/draft-investigatory-powers-bill/written/26371.pdf

[10] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/593753/IP_Act_-_Draft_EI_code_of_practice_Feb2017_FINAL_WEB.pdf

> 3.3 Equipment interference operations vary in complexity. At the lower end of the complexity scale, an equipment interference agency may covertly download data from a subject's mobile device when it is left unattended…"

In light of the above it appears clear that downloading data from an individuals' mobile phone, using mobile phone extraction, would also constitute EI. Since a targeted EI warrant was not available until the enactment of Part 5 of the IPA 2016, then there is a very real risk that police forces in England and Wales have been engaging in widespread criminal conduct with impunity.

Requirement for a warrant

Searching a mobile phone is not like searching a home or even a physical body search. A phone search is far more exhaustive, because of the vast amount of personal data that we now store on our devices. Modern mobile phones are not just phones, but mini computers that hold thousands of pictures, videos and apps and track our location, all of which can reveal so much about us, and potentially even our friends' and family's political, sexual and religious identities.

Given the sensitive nature and breadth of data stored on mobile phones and electronic devices, Privacy International believe that police should be required to obtain a judicially-authorised warrant prior to and specifically in relation to the using of extractive tools.

As noted in the landmark US ruling of Riley v California[11], an element of pervasiveness characterises mobile phones with data that can go back years and shed light on nearly every aspect of a person's life. The US Supreme Court ruled that whilst data on mobile phone is not immune from search, a warrant is generally required before such a search, even in connection with an arrest. The warrant requirement was held to be "an important working part of our machinery of government", not merely "an inconvenience to be somehow 'weighed' against the claims of police efficiency".

Conclusion

In our view, the Report reveals cogent evidence of the proliferation of the technology and the complete absence of any effective legal basis for its use. This is both a significant violation of privacy and has implications for criminal justice (both in terms of the integrity of some convictions and the disclosure exercise). The need for you to review the position is, for the reasons set out above, important and urgent.

We look forward to hearing from you. If you require any further information from us, please do not hesitate to request it.

Please see Annex B for a short background to the Report. The results of our investigation are detailed in our report in which all responses from police are hyperlinked. Since our report we have:

[11] https://www.supremecourt.gov/opinions/13pdf/13-132_8l9c.pdf

- Submitted a complaint under the Data Protection Act to the Information Commissioner[12]; (under investigation)
- Complained to the Home Office[13] (no response)
- Written to HMIC and the College of Policing (no response);
- Submitted further FOIA requests (responses received to date can be provided).

Kind regards,

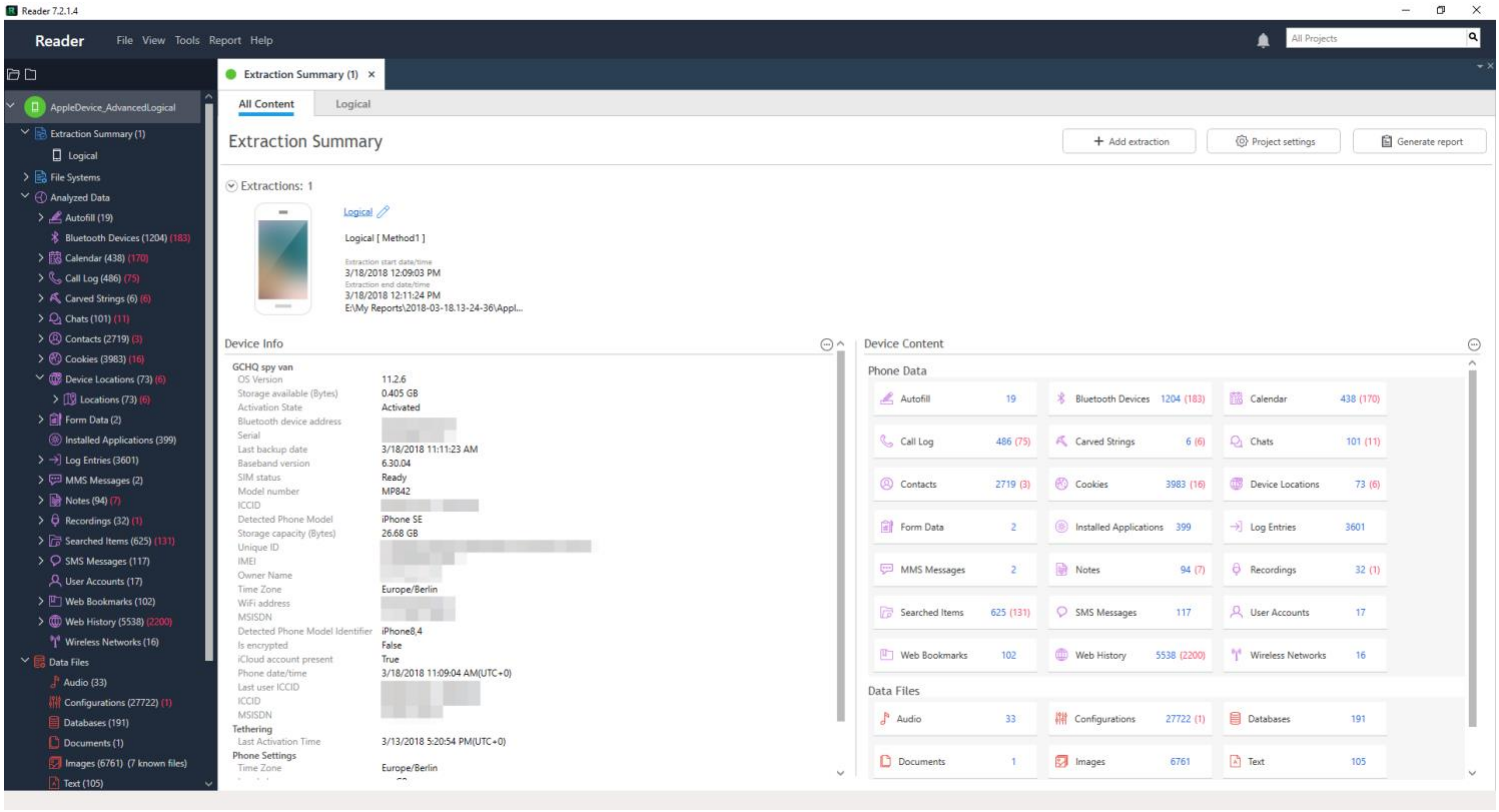
Camilla Graham Wood
Solicitor
Privacy International

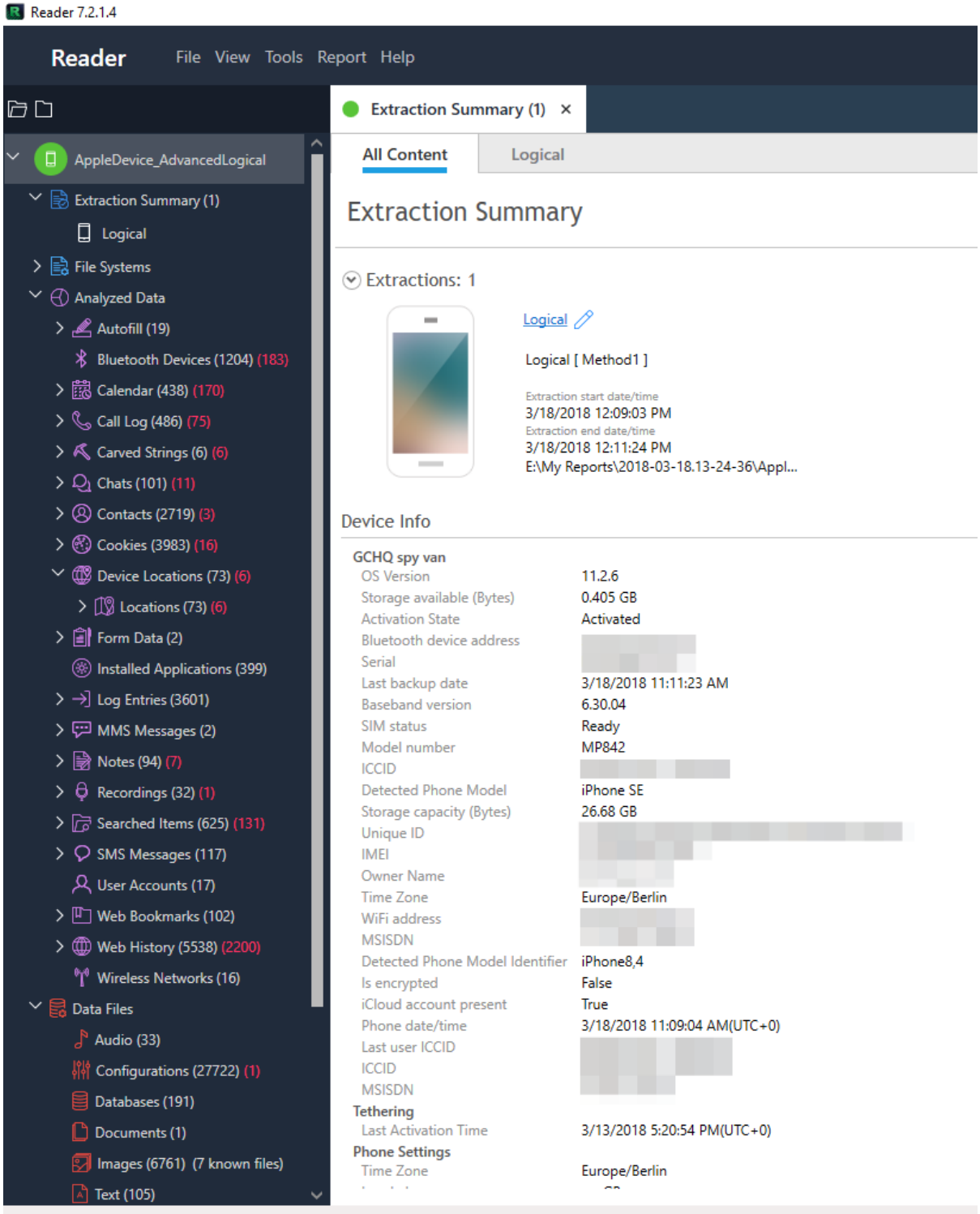
Annex A

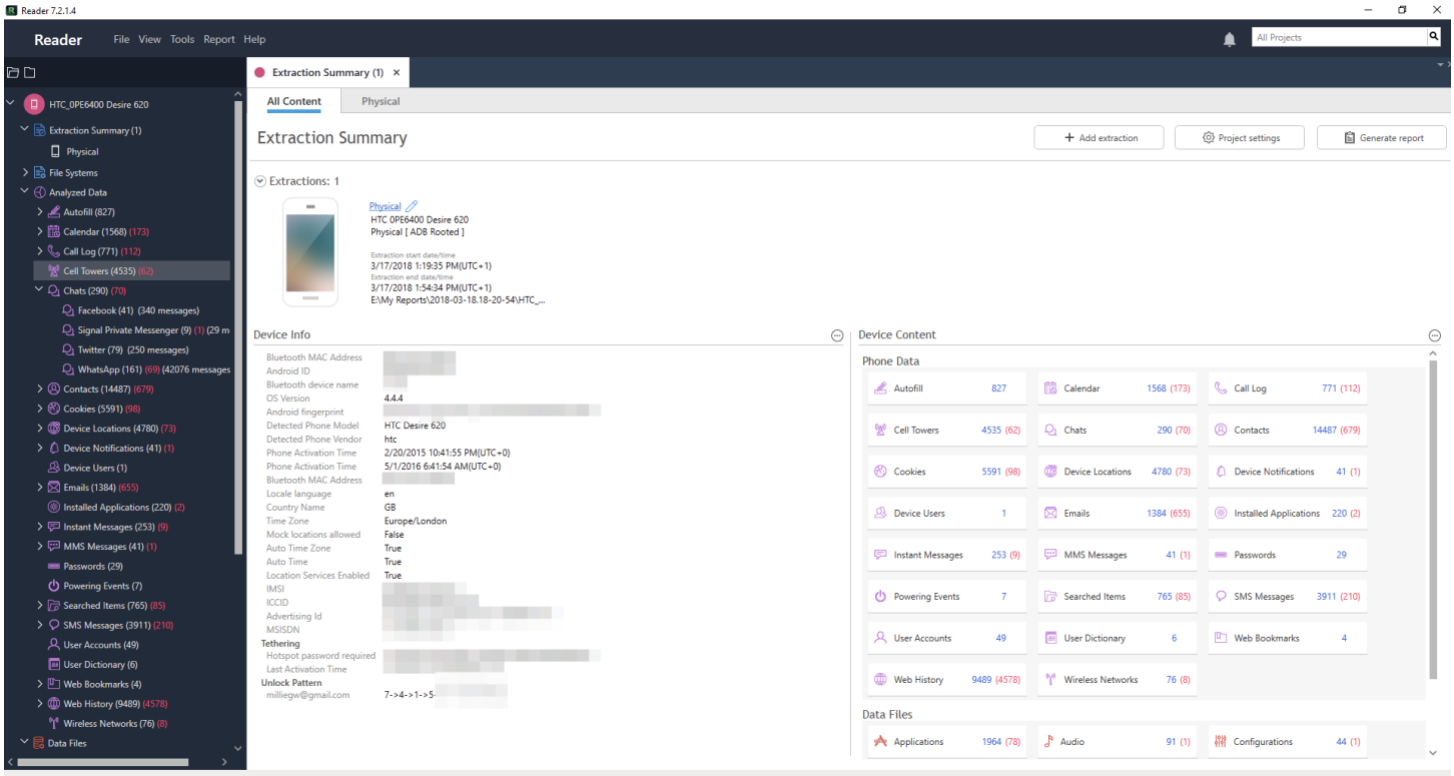
You will see the following device information has been extracted using the Cellebrite UFED:

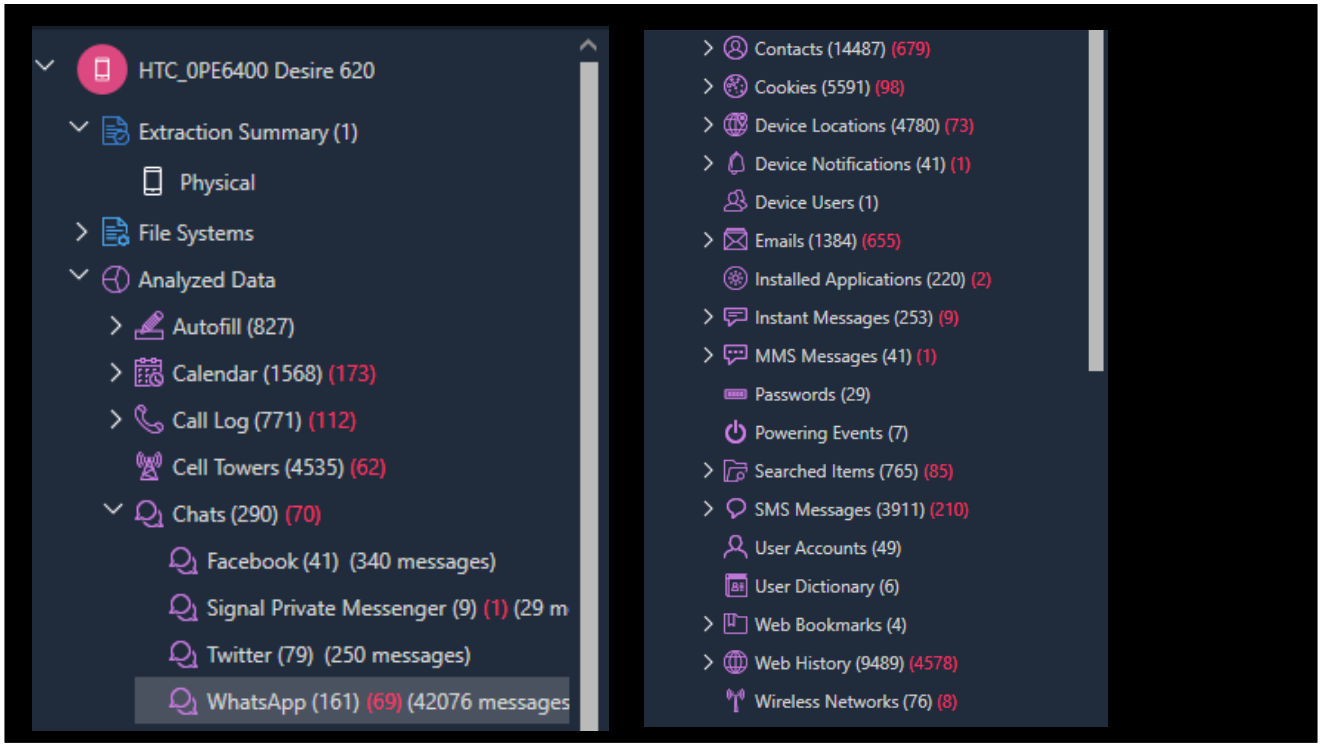
- Bluetooth MAC address
- Android ID
- Bluetooth device name
- Operating System
- Android fingerprint
- Detected Phone Model
- Detected Phone Vendor
- Phone Activation Time
- Locale language
- Country name
- Time zone
- Mock locations allowed
- Auto time zone
- Location services enabled
- IMSI
- ICCID
- Advertising id
- MSISDN
- Teathering: hotspot password required; last activation time
- Unlock pattern

[12] https://privacyinternational.org/sites/default/files/2018-04/Complaint%20to%20ICO%20about%20Mobile%20Phone%20Extraction%2026th%20April%202018.pdf
[13] https://privacyinternational.org/sites/default/files/2018-04/Letter%20to%20Home%20Office%20about%20Mobile%20Phone%20Extraction%2028th%20March%202018%20.pdf
https://privacyinternational.org/sites/default/files/2018-04/Follow%20up%20letter%20to%20Home%20Office%20about%20Mobile%20Phone%20Extraction%2026th%20April%202018.pdf


Reader 7.2.1.4
Reader
File View Tools Report Help
All Projects
Extraction Summary (1)
AppleDevice_AdvancedLogical
Extraction Summary (1)
Logical
File Systems
Analyzed Data
Autofill (19)
Bluetooth Devices (1204) (183)
Calendar (438) (170)
Call Log (486) (75)
Carved Strings (6) (6)
Chats (101) (11)
Contacts (2719) (3)
Cookies (3983) (16)
Device Locations (73) (6)
Locations (73) (6)
Form Data (2)
Installed Applications (399)
Log Entries (3601)
MMS Messages (2)
Notes (94) (7)
Recordings (32) (1)
Searched Items (625) (131)
SMS Messages (117)
User Accounts (17)
Web Bookmarks (102)
Web History (5538) (2200)
Wireless Networks (16)
Data Files
Audio (33)
Configurations (27722) (1)
Databases (191)
Documents (1)
Images (6761) (7 known files)
Text (105)
All Content
Logical
Extraction Summary
+ Add extraction
Project settings
Generate report
Extractions: 1
Logical
Logical [Method1]
Extraction start date/time
3/18/2018 12:09:03 PM
Extraction end date/time
3/18/2018 12:11:24 PM
E:\My Reports\2018-03-18.13-24-36\Appl...
Device Info
GCHQ spy van
OS Version 11.2.6
Storage available (Bytes) 0.405 GB
Activation State Activated
Bluetooth device address
Serial
Last backup date 3/18/2018 11:11:23 AM
Baseband version 6.30.04
SIM status Ready
Model number MP842
ICCID
Detected Phone Model iPhone SE
Storage capacity (Bytes) 26.68 GB
Unique ID
IMEI
Owner Name
Time Zone Europe/Berlin
WiFi address
MSISDN
Detected Phone Model Identifier iPhone8,4
Is encrypted False
iCloud account present True
Phone date/time 3/18/2018 11:09:04 AM(UTC+0)
Last user ICCID
ICCID
MSISDN
Tethering
Last Activation Time 3/13/2018 5:20:54 PM(UTC+0)
Phone Settings
Time Zone Europe/Berlin
Device Content
Phone Data
Autofill 19
Bluetooth Devices 1204 (183)
Calendar 438 (170)
Call Log 486 (75)
Carved Strings 6 (6)
Chats 101 (11)
Contacts 2719 (3)
Cookies 3983 (16)
Device Locations 73 (6)
Form Data 2
Installed Applications 399
Log Entries 3601
MMS Messages 2
Notes 94 (7)
Recordings 32 (1)
Searched Items 625 (131)
SMS Messages 117
User Accounts 17
Web Bookmarks 102
Web History 5538 (2200)
Wireless Networks 16
Data Files
Audio 33
Configurations 27722 (1)
Databases 191
Documents 1
Images 6761
Text 105


Reader 7.2.1.4
Reader
File View Tools Report Help
Extraction Summary (1)
AppleDevice_AdvancedLogical
Extraction Summary (1)
Logical
File Systems
Analyzed Data
Autofill (19)
Bluetooth Devices (1204) (183)
Calendar (438) (170)
Call Log (486) (75)
Carved Strings (6) (6)
Chats (101) (11)
Contacts (2719) (3)
Cookies (3983) (16)
Device Locations (73) (6)
Locations (73) (6)
Form Data (2)
Installed Applications (399)
Log Entries (3601)
MMS Messages (2)
Notes (94) (7)
Recordings (32) (1)
Searched Items (625) (131)
SMS Messages (117)
User Accounts (17)
Web Bookmarks (102)
Web History (5538) (2200)
Wireless Networks (16)
Data Files
Audio (33)
Configurations (27722) (1)
Databases (191)
Documents (1)
Images (6761) (7 known files)
Text (105)
All Content
Logical
Extraction Summary
Extractions: 1
Logical
Logical [Method1]
Extraction start date/time
3/18/2018 12:09:03 PM
Extraction end date/time
3/18/2018 12:11:24 PM
E:\My Reports\2018-03-18.13-24-36\Appl...
Device Info
GCHQ spy van
OS Version 11.2.6
Storage available (Bytes) 0.405 GB
Activation State Activated
Bluetooth device address
Serial
Last backup date 3/18/2018 11:11:23 AM
Baseband version 6.30.04
SIM status Ready
Model number MP842
ICCID
Detected Phone Model iPhone SE
Storage capacity (Bytes) 26.68 GB
Unique ID
IMEI
Owner Name
Time Zone Europe/Berlin
WiFi address
MSISDN
Detected Phone Model Identifier iPhone8,4
Is encrypted False
iCloud account present True
Phone date/time 3/18/2018 11:09:04 AM(UTC+0)
Last user ICCID
ICCID
MSISDN
Tethering
Last Activation Time 3/13/2018 5:20:54 PM(UTC+0)
Phone Settings
Time Zone Europe/Berlin


Reader 7.2.1.4
Reader
File View Tools Report Help
All Projects
Extraction Summary (1)
All Content
Physical
Extraction Summary
Add extraction
Project settings
Generate report
Extractions: 1
Physical
HTC 0PE6400 Desire 620
Physical [ADB Rooted]
3/17/2018 1:19:35 PM(UTC+1)
3/17/2018 1:54:34 PM(UTC+1)
E:\My Reports\2018-03-18.18-20-54\HTC_...
Device Info
Bluetooth MAC Address
Android ID
Bluetooth device name
OS Version
4.4.4
Android fingerprint
Detected Phone Model
HTC Desire 620
Detected Phone Vendor
htc
Phone Activation Time
2/20/2015 10:41:55 PM(UTC+0)
Phone Activation Time
5/1/2016 6:41:54 AM(UTC+0)
Bluetooth MAC Address
Locale language
en
Country Name
GB
Time Zone
Europe/London
Mock locations allowed
False
Auto Time Zone
True
Auto Time
True
Location Services Enabled
True
IMSI
ICCID
Advertising Id
MSISDN
Tethering
Hotspot password required
Last Activation Time
Unlock Pattern
milliegw@gmail.com
7->4->1->5
Device Content
Phone Data
Autofill 827
Calendar 1568 (173)
Call Log 771 (112)
Cell Towers 4535 (62)
Chats 290 (70)
Contacts 14487 (679)
Cookies 5591 (98)
Device Locations 4780 (73)
Device Notifications 41 (1)
Device Users 1
Emails 1384 (655)
Installed Applications 220 (2)
Instant Messages 253 (9)
MMS Messages 41 (1)
Passwords 29
Powering Events 7
Searched Items 765 (85)
SMS Messages 3911 (210)
User Accounts 49
User Dictionary 6
Web Bookmarks 4
Web History 9489 (4578)
Wireless Networks 76 (8)
Data Files
Applications 1964 (78)
Audio 91 (1)
Configurations 44 (1)
HTC_0PE6400 Desire 620
Extraction Summary (1)
Physical
File Systems
Analyzed Data
Autofill (827)
Calendar (1568) (173)
Call Log (771) (112)
Cell Towers (4535) (62)
Chats (290) (70)
Facebook (41) (340 messages)
Signal Private Messenger (9) (1) (29 m
Twitter (79) (250 messages)
WhatsApp (161) (69) (42076 messages
Contacts (14487) (679)
Cookies (5591) (98)
Device Locations (4780) (73)
Device Notifications (41) (1)
Device Users (1)
Emails (1384) (655)
Installed Applications (220) (2)
Instant Messages (253) (9)
MMS Messages (41) (1)
Passwords (29)
Powering Events (7)
Searched Items (765) (85)
SMS Messages (3911) (210)
User Accounts (49)
User Dictionary (6)
Web Bookmarks (4)
Web History (9489) (4578)
Wireless Networks (76) (8)
Data Files


HTC_0PE6400 Desire 620
Extraction Summary (1)
Physical
File Systems
Analyzed Data
Autofill (827)
Calendar (1568) (173)
Call Log (771) (112)
Cell Towers (4535) (62)
Chats (290) (70)
Facebook (41) (340 messages)
Signal Private Messenger (9) (1) (29 m
Twitter (79) (250 messages)
WhatsApp (161) (69) (42076 messages
Contacts (14487) (679)
Cookies (5591) (98)
Device Locations (4780) (73)
Device Notifications (41) (1)
Device Users (1)
Emails (1384) (655)
Installed Applications (220) (2)
Instant Messages (253) (9)
MMS Messages (41) (1)
Passwords (29)
Powering Events (7)
Searched Items (765) (85)
SMS Messages (3911) (210)
User Accounts (49)
User Dictionary (6)
Web Bookmarks (4)
Web History (9489) (4578)
Wireless Networks (76) (8)

Annex B: Background to Privacy International's report

In January 2017 Privacy International reported[14] on an investigation by independent media co-operative the Bristol Cable into the unauthorised use of mobile phone examination tools by the police, which had undermined investigations into serious crimes.

A 2015 review by the Police and Crime Commissioner (PCC) for North Yorkshire Police[15], obtained by the Bristol Cable, revealed that there was a failure by the force to receive authorisation for mobile phone extraction in half the cases sampled, noting "In 25/50 examination files an FSD9 submission form2 was not evidenced, as a result limited assurance can be provided that the examination was undertaken in compliance with Force procedure."

The PCC report concluded that: poor training resulted in practices that had undermined prosecution of serious crime offences including murder and sexual assault; and found serious breaches of data security practices, including the failure to encrypt people's data even though the capacity existed; and the loss of files potentially containing intimate details of people never charged with a crime.

The documents obtained by Bristol Cable included a Metropolitan Police Service procurement document[16], which stated that 'in March 2016 there will be SSK in all 32 MPS Boroughs and 12 Hubs'. This indicated the increasing use of extractive technologies at local and district level by police in low level / volume crimes as opposed to predominantly for serious crimes where devices are sent to the relevant High-Tech Crime Unit.

Concerned at the widespread use of this technology accompanied by little transparency, Privacy International, focusing on the use of SSK and Hubs, submitted Freedom of Information Act (FOIA)[ii] requests to every police force in the UK, asking whether they carry out mobile phone data extraction in low level crime cases using Self Service Kiosks and regional 'hubs, and, if so, what company or companies provided the extraction technology.

The results of our investigation are detailed in our report in which all responses from police are hyperlinked. Since our report we have:

- Submitted a complaint under the Data Protection Act to the Information Commissioner[17]; (under investigation)

[14] https://medium.com/privacy-international/press-release-unauthorised-use-of-mobile-phone-examination-tools-by-police-have-undermined-acf8986d29c2
[15] https://assets.documentcloud.org/documents/3259663/North-Yorkshire-Police-Mobile-Phone-Examination.pdf
[16] https://www.documentcloud.org/documents/3280381-MPS-Digital-Cyber-and-Communications-Forensics.html
[17] https://privacyinternational.org/sites/default/files/2018-04/Complaint%20to%20ICO%20about%20Mobile%20Phone%20Extraction%2026th%20April%202018.pdf

- Complained to the Home Office[18] (no response)
- Written to HMIC and the College of Policing (no response);
- Submitted further FOIA requests (responses received to date can be provided);

[i] MSAB's XRY Physical allows access to "system and deleted data and can use extra functionality to help overcome security and encryption challenges on locked devices."[i] 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 media data and app-based data for services such as Facebook, Google, iCloud, Twitter, Snapchat, WhatsApp, Instagram and more."[i]

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 media data and app-based data for services such as Facebook, Google, iCloud, Twitter, SnapChat, WhatsApp, Instagram and more."

Cellebrite tools can obtain "Entered locations, GPS fixes, favourite locations, GPS info"[i] and provide "comprehensive data extractions, even to inaccessible partitions of the device … Physical extraction provides a bit-by-bit copy of the entire flash memory of a mobile device. This extraction method not only enables the acquisition of intact data, but also data that is hidden or has been deleted."[i]

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 searched conducted with Chrome and Safari on iOS devices backed-up iCloud. UFED Cloud Analyser 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.

[ii] We asked the following questions: 1. Does your police force carry out mobile phone data extract in low level crime cases using self-service / downloading kiosks? Please provide your definition of low-level crime. 2. Does your police force carry out mobile phone data extract in serious rimes using self-service / downloading kiosks. 3. If your police force is not currently using mobile phone extraction kiosks, have you trialled this. 4. Does your police force use Hubs to carry out mobile phone data extract in low level crimes? 5. Does your police force use Hubs to carry out mobile phone data extract in serious crimes? 6. Do you centrally record

[18] https://privacyinternational.org/sites/default/files/2018-04/Letter%20to%20Home%20Office%20about%20Mobile%20Phone%20Extraction%2028th%20March%202018%20.pdf
https://privacyinternational.org/sites/default/files/2018-04/Follow%20up%20letter%20to%20Home%20Office%20about%20Mobile%20Phone%20Extraction%2026th%20April%202018.pdf

mobile phone data extracted from kiosks? 7. If you have a mobile phone extraction kiosk, please provide the name of the company which provides the hardware / software / to whom pay a license for the relevant tools. 8. Please confirm whether or not a review has been conducted into the use of self-service kiosk. Please note below PEEL report and North Yorkshire Police report by way of example. 9. Please provide copies of the current relevant force level and/or national level guidance for the use of downloading kiosks. 10. Please provide copies of the current relevant force level and/or national level policy for the use of downloading kiosks. 11. How many officers carry mobile phone examination kits on patrol and/or in vehicles and/or for other operational use in (a) low level crimes? (b) serious crimes?