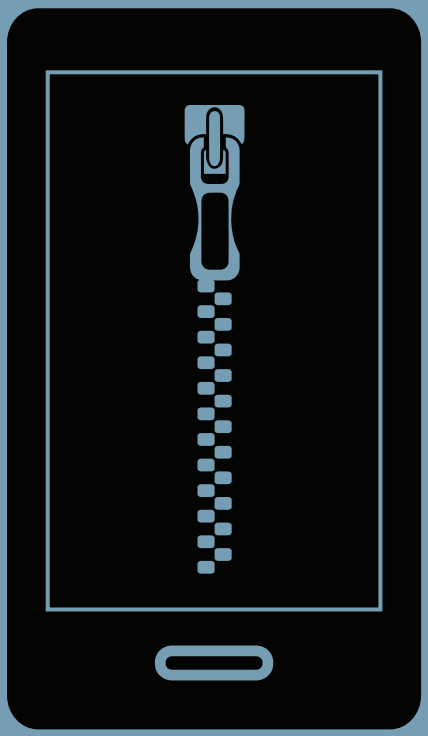
PRIVACY INTERNATIONAL

Digital stop and search: how the UK police can secretly download everything from your mobile phone



March 2018

Contents

Introduction	02
Background to the report	04
What is mobile phone extraction?	06
Types of data extracted	07
Which forces are using this technology?	10
The companies involved	15
Invisible data: the role of tech and mobile phone companies	18
Lawful basis	20
Lack of national guidance	22
Lack of local guidance	24
Procedures for carrying out extraction	25
Retention, deletion and individual rights	28
Business as usual	30
Security of data	31
Conclusion	33
Recommendations	35
Annex	36

Introduction

Unwarranted searches of mobile phones by the police

You could search a person, and their entire home and never find as much information as you can from searching their phone. Yet the police can take data from your phone without your consent, without your knowledge and without a warrant.

In the course of a search of your home, if the police confiscate your possessions, you are entitled to an inventory of those items. Yet if data is extracted from your devices, you may not even know this has taken place, let alone be told what kind of data the police have stored on their database.

We rely on and put trust in our phones. They reveal so much about our identity, saying more about us than we perhaps realise. They contain our photos, calendar, internet browsing, details of everywhere we go, our emails, social media, medical information, our online banking, our health and fitness data; they reveal our shopping habits, music tastes and political views; and hold a plethora of apps which generate and hold vast quantities of data. The data on our phones does not just relate to the us, the owner, but includes personal data, such as messages or photos, related to friends, family, employers and colleagues.

Privacy International has uncovered that in the UK police are using highly intrusive technology to extract and store data from individual's phones, on a questionable legal basis. The technology, which has been rolled out nationally following its use by the Metropolitan Police Service during the London Olympics in 2012, gives the police the ability to obtain data from our phones than we cannot access ourselves and which we do not know exists. Without public consultation or parliamentary scrutiny, the police want extraction of data to be standard procedure in all criminal investigations.

Documents obtained by Privacy International reveal an absence of national guidance and paucity of local policy, with the few documents disclosed exposing conflicting views between police forces as to the legal basis to search, download and store personal data. Further, many forces believe they can extract data from mobile devices without informing the owner, whether victim, witness or suspect. With no clear rules on deletion, the police believe they can keep data indefinitely, even if the individual is innocent of any crime.

Privacy International believes that a lack of any kind of warrantry or record keeping, and no independent oversight in relation to the exercise of mobile phone extraction powers, creates a serious risk of abuse and discriminatory practices.
As noted by David Lammy MP in The Lammy Review, Black and Minority Ethnic (BAME) individuals still face bias, including overt discrimination in parts of the justice system. David Lammy MP highlighted in conclusion to his review the risks

associated with developments in technology and the need for transparency. We believe that mobile phone extraction presents a danger of replicating or exacerbating existing discrimination.

Background to the report

In January 2017 Privacy International reported 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[1].

A 2015 review by the Police and Crime Commissioner (PCC) for North Yorkshire Police, 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 form[2] 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.

These disclosures, including a Metropolitan Police Service procurement document, which stated that 'in March 2016 there will be SSK in all 32 MPS Boroughs and 12 Hubs', indicated the increasing use of extractive technologies at local and district level by police in low level / volume crimes[3] as opposed to predominantly for serious crimes where devices are sent to the relevant High-Tech Crime Unit.

Concerned that there may be more 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) requests to every police force in the UK[4], asking whether they carry out mobile phone data extraction

1 https://medium.com/privacy-international/press-release-unauthorised-use-of-mobile-phone-examination-tools-by-police-have-undermined-acf8986d29c2
Serious crime is defined in section 93(4) of the Police Act 1997 as:
Conduct which
(a) involves the use of violence, results in substantial financial gain or is conducted by a large number of persons in pursuit of a common purpose or
(b) the offence or one of the offences is an offence for which a person who has attained the age of twenty-one and has no previous convictions could reasonably be expected to be sentenced to imprisonment for a term of three years or more.

2 An FSD9 Submission form appears to be a form confirming internal authorisation for use of mobile phone extraction.

3 ACPO (2009) Practice Advice on the Management of Priority and Volume Crime (The Volume Crime Management Model) (Second Edition) defines volume crime as:
…any crime which, through its sheer volume, has a significant impact on the community and the ability of the local police to tackle it. Volume crime often includes priority crimes such as street robbery, burglary and vehicle-related criminality, but can also apply to criminal damage or assaults.

4 England, Wales, Northern Ireland and Scotland

in low level crime cases using Self Service Kiosks and regional 'hubs', and, if so, what company or companies provided the extraction technology.

Despite it now being apparent that there has been a nationwide roll out of Self Service Kiosks and regional 'hubs', there is a paucity of public information, the little there is results from Freedom of Information Act requests made by Privacy International.

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 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?

What is mobile phone extraction?

The technology exists to recover digital evidence or data from mobile devices. Using an extractive device, the police can obtain a memory dump of data which can be saved and analysed. Depending on the hardware and software used, an extraction report will be generated, allowing investigators to see at a glance a persons' location, who they speak to and when, and potentially vast amounts of other revealing information.

When a Police Officer obtains a personal mobile device in the UK, Privacy International's understanding is that data extractions, at least in low level crimes, are carried out at one of three places:

1. Self Service Kiosks (SSK), where forensic analysis on the device is carried out within the local police force[5].

2. Frontline supported service 'Hubs', which can serve a number of forces[6].

3. Police forces may also equip officers with portable mobile phone extraction kits, which can carry out an analysis outside of any police facilities[7].

5 Bedfordshire Police, City of London Police, Derbyshire Constabulary, Devon and Cornwall Police, Dorset Police, Durham Constabulary, Gwent Police, Hampshire Constabulary, Kent Police, Lancashire Constabulary, Lincolnshire Police, Metropolitan Police Service, Northumbria Police, Staffordshire Police, Surrey Police, Norfolk Constabulary and Suffolk Constabulary, Thames Valley Police, West Midlands Police, Warwickshire Police, Wiltshire Police

6 British Transport Police, City of London Police, Devon and Cornwall Police, Dorset Police, Kent Police, Lancashire Constabulary, Lincolnshire Police, North Wales Police, Northumbria Police, Staffordshire Police, Wiltshire Police

7 British Transport Police, City of London Police, West Yorkshire Police

Types of data extracted

The technology available to the police has itself come on in leaps and bounds since 2012, when its use by UK police forces was reported by the BBC[8]. The disclosure we have obtained reveals that UK police forces contract with companies Cellebrite, MSAB and Radio Tactics (see below).

These companies which sell their products to UK police forces are not shy about their benefits. MSAB claims that:

> "If you've got access to a sim card, you've got access to the whole of a person's life"[9]

MSAB acknowledge that "the sheer amount of data stored [in mobile phones] is significantly greater today than ever before".[10] They claim their 'XRY software' is supplied to "97% of UK police forces" and is involved in a UK Cybercrime Pilot with a number of forces and 'digital experts' who work in the private sector[11].

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."[12] 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."[13] Even the police themselves highlight the breadth of information your mobile phone can hold. Leicestershire Police state on their website:

> "Think about the information stored it can reveal about you, your friends and your life? All of your calls, messages, who you know. It may have diary appointments, photographs and web browsing history."

Cellebrite tools can obtain "Entered locations, GPS fixes, favourite locations, GPS info[14]" 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

8 http://www.bbc.co.uk/news/technology-18102793

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

10 https://www.youtube.com/watch?v=QUjtZ6nW16s&feature=youtu.be accessed 3.07.2017

11 http://www.bbc.co.uk/news/av/uk-england-hampshire-35353966/portsmouth-unit-trials-volunteer-cyber-crimefighters

12 https://www.msab.com/products/xry/#logical accessed 4.7.2017

13 https://www.msab.com/products/xry/xry-cloud/ accessed 8.3.2018

14 http://www.cellebrite.com/Pages/portable-gps-forensics-physical-extraction-and-decoding-from-portable-gps-devices accessed 4.7.2017

of intact data, but also data that is hidden or has been deleted."[15]

The extent to which operational SSK based in local police stations can extract deleted data or whether they have to rely on their force High Tech Crime Unit (HTCU) is unclear. Derbyshire Constabulary disclosed their May 2013 'Guidance on the Use of Divisional Mobile Phone Examination Facilities which states:

> "It must be remembered at all times that the Kiosk is only able to read the live side of the phone and so no deleted information will be recovered. If it's known or suspected that the evidence that is required has been deleted the phone needs to be submitted to the HTCU for a physical read of the memory."

Derbyshire Constabulary's guidance refers to a 'red folder' containing "ACESO Validated Devices and Capabilities", which shows what can be automatically obtained and what will need to be manually photographed, although this document itself was not disclosed.

In addition to the personal information from your contacts, calls and messages, the police will also want data that is generated by mobile phone apps. As noted below, the device purchased by Avon and Somerset Constabulary provides the ability to "decode data from more than 1,500 mobile applications in minutes."

Highlighting the potential value of data from mobile apps, a recent murder investigation in Germany utilised metrics from the apps on individuals' phone. In that case, Apple's iPhone health app activity record stated that the suspect was "'climbing stairs,' which authorities were able to correlate with the time he would have dragged his victim down the river embankment, and then climbed back up."[16]

In addition to the types of data we might be able to assume police forces could extract, it is increasingly evident that data exists on devices that is beyond the knowledge of the user/consumer. We do not know what Cellebrite means when, for example, they refer to "inaccessible parts of the phone" and what may encompass the hidden and deleted data the police can access. This is likely to differ for each user, and be influenced by factors such as the operating system.
In addition, according to one document disclosed by the Metropolitan Police Service, it is not possible to limit what is extracted nor to isolate data that relates to specific date periods.

> '10.4 Handling Irrelevant Data
> When a SSE kiosk is used to obtain electronic data from a mobile device, it will obtain all data of a particular type, rather than just the individual data that is relevant to a particular investigation. For example, if a photograph on a 'witness' mobile phone is relevant, because it shows an offence being committed, then the kiosk will acquire all photographs on that phone, rather than just the photographs of the offence. If text messages to a victim of harassment are required to investigate the harassment allegations, then the

15 http://www.cellebrite.com/Pages/physical-extraction-of-mobile-data accessed 4.7.2017

16 https://motherboard.vice.com/en_us/article/43q7qq/apple-health-data-is-being-used-as-evidence-in-a-rape-and-murder-investigation-germany

kiosk will acquire all text messages on that phone.'

Wiltshire Police guidelines refer to 'collateral intrusion' of mobile phone extraction 'whereby data other than that requested by the officer is obtained. Collateral Intrusion is any infringement of the privacy of individuals who are not subject to the enquiry being conducted.'

The police may take all of an individual's photos or messages, which includes data related to third parties. However, it remains unclear what rights exist for the individual who owns the phone, let alone their acquaintances, who will have no idea the police may hold their data.

Despite the seemingly endless types of data that can be obtained there is no clear requirement to inform the individual.

If the police search your home or confiscate your possessions, you will receive an inventory list of those items[17]. However, if they extract data from your devices, you may not even be told that they have done so, let alone be told what kind of data they have extracted.

17 PACE 1984, Code B https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/117591/pace-code-b-2011.pdf

Which forces are using this technology?

We contacted 47, police forces and responses to our FOIA requests revealed the use of a range of security companies, including Cellebrite[18], ACESO[19] (part of Radio Tactics), Radio Tactics[20], XRY[21] (an MSAB product), MSAB[22] and Micro Systemation (MSAB)[23] who provide extractive tools to 26 UK police forces. (see Annex A)

The MET SSK are ACESO units "currently rented and maintained under an existing third-party arrangement with Radio Tactics"[24].

Twelve forces stated clearly they use SSK in both low-level and serious crimes[25]. This is concerning given the 2015 independent review, cited above, which identified that the use of SSK in serious crimes had undermined investigations. Hubs are used by 13 forces to extract mobile phone data in both low level and serious crimes[26].

Whereas SSK are based in individual police stations, thus are more 'in-house', Hubs refers to the sharing of resources between forces, thus a more 'central'

18 Used by: Avon and Somerset Constabulary; City of London Police, Gloucestershire Constabulary, Lancashire Constabulary, Lincolnshire Police, Northumbria Police, (UFED Infild Logical by Cellebrite UK Ltd), Warwickshire Police, West Mercia Police, British Transport Police
n.b. Avon and Somerset Constabulary stated in February 2017 that "At the time of this request Avon and Somerset Constabulary were not using downloading kiosks to carry out mobile phone data extract, however this is due to start. Low level crime would include drugs, assaults and public orders." They confirmed that they have Cellebrite tools and a disclosed contract with Cellebrite refers to 'F-UFD-15-032 UFED Infield Kiosk Logical'.
Gloucestershire Constabulary stated in early 2017 'The Constabulary is about to trial Cellebrite (UFED)' https://www.documentcloud.org/documents/4348937-Gloucestershire-Response-2017-0053.html

19 Used by: City of London Police, Durham Constabulary, Northumbria Police, (ACESO by Radio tactics), Staffordshire Police,

20 https://www.radio-tactics.com
Used by: Devon & Cornwall, Dorset Police, Durham Constabulary, Hampshire Constabulary, Thames Valley Police, Wiltshire Police

21 Used by: City of London Police

22 https://www.msab.com
Used by: Bedfordshire Police, Derbyshire Constabulary, Gwent Police, Norfolk Constabulary and Suffolk Constabulary, Surrey Police, British Transport Police

23 Used by: Kent Police, MET Police

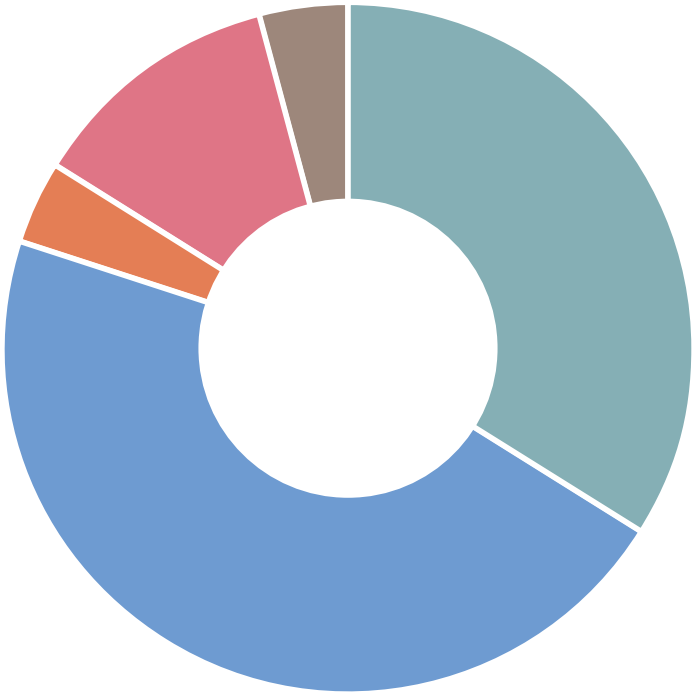
24 http://uk.prweb.com/releases/2012/5/prweb9498788.htm

25 Derbyshire Constabulary, Hampshire Constabulary, Lincolnshire Police, Metropolitan Police Service, Northumbria Police, Staffordshire Police, Norfolk Constabulary and Suffolk Constabulary, Surrey Police, Thames Valley Police, Wiltshire Police, Avon and Somerset Constabulary

26 British Transport Police, City of London Police, Devon & Cornwall, Dorset Police, Kent Police, Lincolnshire Police, Merseyside Police, Metropolitan Police Service, North Wales Police, Northumbria Police, Staffordshire Police, Surrey Police, Wiltshire Police

shared version of the SSK.

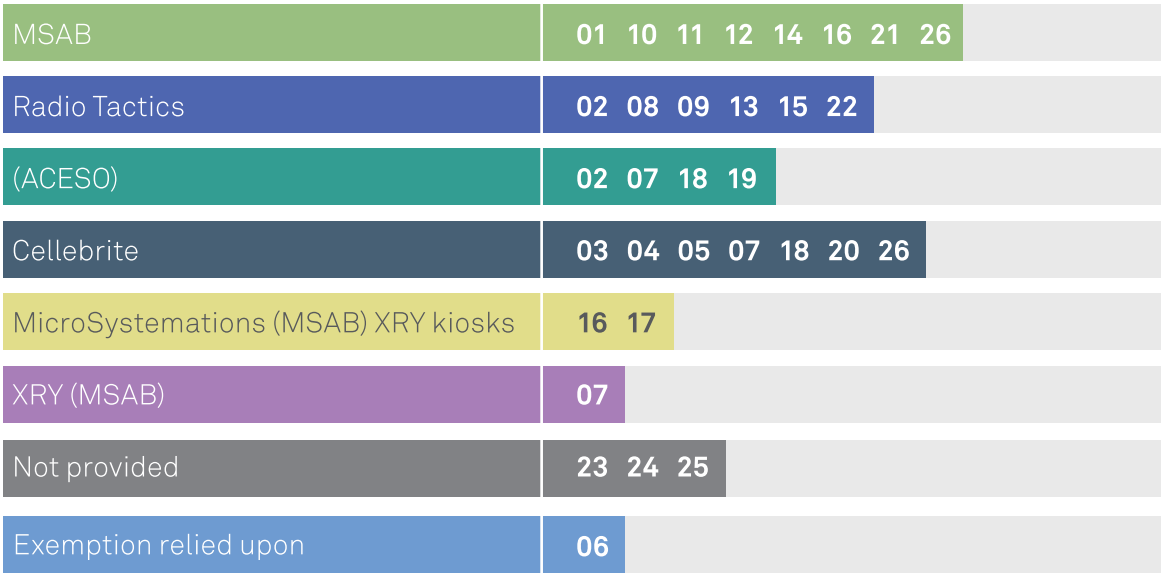
Forces using Self Service Kiosks (SSK) and/or Hubs



Forces using Self Service Kiosks and/or Hubs (26)

- SSK & Hubs - in low level crime (9)
- SSK & Hubs - in low level and serious crime i.e. all crimes (12)
- SSK & Hubs - unknown whether used in both or either low level or serious crime (1)
- Use of Hubs only (3)
- Use of Hubs and mobile units (1)

Technology used



01 Bedfordshire Police
02 Durham Constabulary
03 Lancashire Constabulary
04 Warwickshire Police
05 West Mercia Police
06 West Midlands Police
07 City of London Police
08 Devon and Cornwall Police
09 Dorset Police
10 Derbyshire Constabulary
11 Gwent Police
12 Norfolk Constabulary
13 Hampshire Constabulary
14 Suffolk Constabulary
15 Thames Valley Police
16 Kent Police
17 Metropolitan Police Service
18 Northumbria Police
19 Staffordshire Police
20 Lincolnshire Police
21 Surrey Police
22 Wiltshire Police
23 Merseyside Police
24 West Yorkshire Police
25 North Wales Police
26 British Transport Police

Out of the 47 police forces we contacted, five failed to provide a response[27]. We additionally contacted the Serious Fraud Office, National Police Chief's Council, College of Policing and Home Office.

27 Cleveland Police, Cumbria Constabulary, Essex Police, North Yorkshire Police, Sussex Police

Forces who failed to respond

Cleveland Police
Cumbria Constabulary
Essex Police
North Yorkshire Police
Sussex Police

For those who indicated they were not using mobile phone extraction:

- Three forces told us they were in the process of implementing or considering using SSK.
- Greater Manchester Police, South Wales Police and South Yorkshire Police and Cambridgeshire Constabulary stated they hold no information about the use of mobile phone extraction.
- Humberside Police, Police Service of Scotland and Dyfed-Powys Police stated they had trialled the kiosk product. Dyfed-Powys Police found at that point in time it did not suit the force's needs.
- Northamptonshire Police and Police Service of Northern Ireland state they have not trialled or used mobile phone extraction to date.

Forces about to trial Cellebrite or other extractive tools

Avon and Somerset Constabulary
Gloucestershire Constabulary
Leicestershire Police

Forces who have trialled mobile phone extraction but stated they do not currently use it

Cheshire Constabulary
Hertfordshire Constabulary
Humberside Police
Police Service of Scotland
Dyfed-Powys Police

Forces who state they hold no information / not trialled or used mobile phone extraction

Cambridgeshire Constabualry
Greater Manchester Police*
Northamptonshire Police
Nottinghamshire Police
South Yorkshire Police
Police Service of Northern Ireland
South Wales Police
Ministry of Defence Police

*We were aware from documents obtained by the Bristol Cable that financial reports showed expenditure by Greater Manchester Police with the firm Cellebrite, a high profile firm specialising in the production of extraction software, including: Cellebrite Mobile Synchronization Ltd E14000413/Q-24120D [April 2014]; Cellebrite Mobile Synchronization Ltd INU 16000000275 [June 2016]; Cellebrite Mobile Synchronization Ltd 74/102 [October 2014].

We queried Greater Manchester Police's response, which stated that they hold no information about mobile phone extraction. On 1 August 2017 Greater Manchester Police replied that "GMP does not have a contract in place at present with Cellebrite. Please note that although no contract is in place GMP do purchase from Cellebrite." On 6 September 2017 GMP confirmed purchases totalled £89,000 for new licenses, renewals and training. It remains unclear whether Cellebrite tools are used by GMP for mobile phone extractions.

The companies involved

As noted above, UK police forces use a range of security companies, namely Cellebrite, Radio Tactics, and MSAB. Extraction tools manufactured by security companies selling exclusively to government agencies vary in sophistication, but generally access data on devices and visualise it for easier analysis.

Cellebrite is one of the best-known phone 'crackers'. Founded in Israel, it is now owned by a Japanese conglomerate, which specialises in providing hacking devices and technologies to law enforcement. A CNN investigation reported that "for years, it has been the go-to resource for FBI agents breaking into suspects' phones."[28] FBI forensic expert Stephen Flatley has repeatedly praised the company, referring to them in January 2018 as an "evil genius"[29]. The company is not without controversy. Revealing the risks associated with this technology, an investigation by The Intercept[30] examined whether Cellebrite sells its wares to countries with poor human rights records. They concluded, based on evidence produced at the trial of human rights activist Abdali al-Singace, that Cellebrite sold to Bahrain and its technology was used to prosecute al-Singace, a victim of torture.

Cellebrite's 'Universal Forensic Extraction Device' (UFED), first launched in 2007, is a hand-held device. The UFED Ultimate "offers market-leading access to digital devices and unsurpassed capabilities to extract and decode every ounce of data." The capabilities and benefits include[31]:

- Ability to bypass pattern, password or PIN locks and overcome encryption challenges
- Access more data from a wider range of devices: access live, hidden and even deleted data from smartphones, feature phones, tablets, players, GPS devices, SIM cards, smart watches, mass storage devices and more.
- Identify and determine the strength of connections between people, places and events by viewing maps and timelines.

We were able to obtain additional information regarding UK police force contracts with Cellebrite through correspondence with Avon and Somerset Constabulary. A purchase order was disclosed as well as the contract with Cellebrite. The purchase order stated Avon and Somerset Constabulary had obtained an undisclosed number of 'F-UFD-15-032 UFED Infield Kiosk Logical'. Cellebrite describes the UFED InField as[32]:

28 http://money.cnn.com/2016/03/31/technology/cellebrite-fbi-phone/

29 https://motherboard.vice.com/en_us/article/59wkkk/fbi-hacker-says-apple-are-jerks-and-evil-geniuses-for-encrypting-iphones accessed 12.01.2018

30 https://theintercept.com/2016/12/08/phone-cracking-cellebrite-software-used-to-prosecute-tortured-dissident/

31 https://media.cellebrite.com/wp-content/uploads/2017/05/Datasheet_UFED-Ultimate_LTR_26jul2017_WEB.pdf accessed 11.01.2018

32 https://media.cellebrite.com/wp-content/uploads/2017/06/Datasheet_UFED-InField_LTR_26jul2017_

> "A flexible, platform-agnostic solution that gives field personnel the tools to quickly access and triage digital evidence with a forensically sound process. Whether deployed in-car on a rugged device or at a police station, border check point or airport, first responders and investigators can get actionable insights when minutes matter most."

It provides "real time extractions" and states "Authorized field personnel can directly extract passwords, disable or bypass user locks and decode data from more than 1,500 mobile applications in minutes".

MSAB[33], based in Stockholm, has been involved with mobile communications since 1984. Current products include:

- XRY Logical: access and recover live and file system data from the device on the crime scene
- XRY Physical: lets examiners bypass the operating system to dump all the raw data from the device. This memory dump gives you access to system, protected and deleted data, and also allows you to overcome security and encryption challenges on locked devices.
- XRY Cloud: recovers data beyond the mobile device itself from connected cloud-based storage by using the tokens on mobile devices that enable apps to function without the need for users to re-enter their login details. This is particularly useful when looking for social media data and app-based information for services such as Facebook, Google, iCloud, Twitter, SnapChat, WhatsApp, Instagram and more.

Radio Tactics is a UK based company, established in 2003[34] and incorporated in January 2013[35]. They appear to have had involvement with the UK police for a number of years. Dr James Hart, whose police experience is stated to include extensive operational and command experience at the Metropolitan Police Service and New Scotland Yard, held the position of Chairman in 2012[36]. A now deleted section of their website[37] states that in 2004:

> "After meeting with the Thames Valley Police HTCU [High-Tech Crime Unit], the newly formed 'Radio Tactics Limited' began developing its first product; the Forensic SIM Toolkit (FST). Within eight months, FST had been delivered to its first customer and by the end of the following year it had a presence in over two thirds of the UK's law enforcement agencies."

Our FOIA requests have focused on use of mobile phone extraction in low level crimes, however we note their website reveals Radio Tactics have worked with the Serious & Organised Crime Agency (SOCA) to provide "a covert capability in

WEB.pdf accessed 23.01.2018

33 https://www.msab.com/products/

34 https://web.archive.org/web/20120623211103/http://www.radio-tactics.com:80/about/our-people

35 https://beta.companieshouse.gov.uk/company/08348844

36 https://web.archive.org/web/20120623211103/http://www.radio-tactics.com:80/about/our-people

37 https://web.archive.org/web/20131109021546/http://www.radio-tactics.com/about/our-history

situations when time and secrecy are of the essence."[38]

Whilst our report focuses on mobile phones, the range of accessible devices is not limited to smart phones. Derbyshire Constabulary's local force guide indicates that the ACESO kits they use are capable of reading data stored not only on mobile phone handsets but more generally from "SIM cards and memory cards." The Metropolitan Police Service's Digital Control Strategy refers to the forensic opportunity of new devices including "e.g. infotainment systems in cars, SMART TVs" and the Metropolitan Police Service SSK Working Instructions apply to "mobile devices, media cards/USB sticks, SIM cards, Satellite Navigation Systems and Tablet devices".

38 https://web.archive.org/web/20131109021546/http://www.radio-tactics.com/about/our-history

Invisible data: The role of tech and mobile phone companies

It is clear that there is an unacceptable paucity of information from the police in relation to what can be, and what is extracted from mobile phones. This is combined with a lack of clarity from manufacturers and powerful tech companies about the full range of data a phone generates about its user, and out of all that mass of data, what can be extracted.

The few media stories that do arise on this matter highlight just how little we know about how our devices work and how they can be manipulated. For example, in May 2017 it was revealed that Uber could tag iPhones with a persistent identity that allowed it to identify devices uniquely, even after a phone had been wiped[39]. In a separate story Apple gave Uber access to users' iPhone data without their knowledge[40].

In August 2017, Privacy International sent subject access requests – a mechanism available under data protection law allowing individuals access to their data – to Apple, seeking to understand what data could be held on internet connected devices but beyond the customer's reach and not stored on the companies' servers. For data held on their iPhones and other Apple devices, the question was posed to Apple:

> "…I seek data that is on the Apple iPhone device, the Apple iPad and Apple MacBook Air, to which I cannot access using the Apple user interface. This is data that is not held on Apple servers, including iCloud, but is data that is held on the devices."

Apple replied that:

> "I refer specifically to your request for access to data on the device(s) that are in your possession. The right to access to personal data relates to personal data stored on what is known as a relevant filling system. Absent possession of the device and even then, there are limitations that are known to you, Apple has no means to know or report the content of a customer's device(s) and thus we are unable to provide the data that you seek. We are neither a data controller nor a data processor in relation to any such data on your device. I am including for ease of reference the definition of relevant filing system from the Acts:

39 http://www.macworld.com/article/3192943/ios/uber-s-not-alone-in-tracking-users-when-apps-are-deleted.html accessed 4.7.2017 & www.nytimes.com/2017/04/23/technology/travis-kalanick-pushes-uber-and-himself-to-the-precipice.html

40 http://www.telegraph.co.uk/technology/2017/10/06/uber-app-could-secretly-record-iphone-users-screens/

> "'relevant filing system' means any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible."

Incidentally, it was reported in November 2017 that new features on Apple's iOS 11 aimed at protecting personal data from thieves and other intruders would also make it 'harder for cops to extract your data'[41]. Any iPhone plugged into an unfamiliar computer asks the user if they wish to trust the machine before exchanging data. iOS 11 will not only require a tap to trust a new computer, but it would also require the user to re-enter the phone's passcode too.

> "That means that even if the forensic analysts do seize a phone while it's unlocked or use its owner's finger to unlock it, they will still need a passcode to offload its data to a program where it can be analysed wholesale. They can still flip through the data on the phone itself. But if the owner refuses to divulge the passcode, they can't use forensic tools to access its data in the far more digestible format for analysis."[42]

This would limit the ability of intruders to get hidden and deleted data, and access otherwise inaccessible parts of the device and cloud storage via apps.

Apple's iOS 11 also has an 'S.O.S mode'. If you tap the phone's home button five times, it will launch a new lock screen and disables biometrics log-in.

However, the above advancements by Apple do not answer the wider question of data on the device that is beyond the user's control. In addition, not everyone uses an iPhone or will have the latest version of either the handset or operating system. Nor, we would argue, should they have to in order to ensure their data is protected and they maintain control of their own data. In the era of mobile phone extraction, transparency is needed - including from large technology companies such as Apple – so that individuals are aware of all the data their devices hold about them.

We selected Apple devices for the purpose of a subject access request, whose aim was to focus on the issue of data held on the device itself, because they are relatively unique in that they have control over the many apps, the operating system on the device, and how the hardware interacts with the OS. We can only assume that the situation is even more complicated with other mobile phones where the manufacturer is more distant from the hardware selection, the vendor may be different than the manufacturer, and the operating system is decided upon by another party – most often Google. Depending on the device, there may be the additional complexity of the versions of the operating system, and the degree to which that operating system has significant control over the hardware.

41 https://www.wired.com/story/apples-ios-11-will-make-it-even-harder-for-cops-to-extract-your-data/

42 https://www.wired.com/story/apples-ios-11-will-make-it-even-harder-for-cops-to-extract-your-data/

Lawful basis

It is of serious concern that amongst the various police forces who have disclosed their local guidance, there is uncertainty as to the legal basis under which they can extract data from mobile phones.

Whilst the National Police Chief's Council have stated[43] that police use of mobile phone kiosks is governed by Section 20 of the Police and Criminal Evidence Act 1984 (PACE)[44], which grants police the "power to require any information stored in any electronic form" this view is not consistently held, as demonstrated from the conflicting local guidance of a number of polices forces.

Local policies were disclosed by the Derbyshire Constabulary, Gwent Police, Metropolitan Police Service (SSK guidance and Control Strategy), Norfolk Constabulary and Suffolk Constabulary, Northumbria Police, Wiltshire Police and West Yorkshire Police.

43 https://www.documentcloud.org/documents/4349039-NPCC.html

44 Police and Criminal Evidence Act 1984

Police force	Legal basis
National Police Chief's Council	Section 20 Police and Criminal Evidence Act 1984 (PACE)
Derbyshire Constabulary	No clear legal basis identified
Gwent Police	No clear legal basis identified
Metropolitan Police Service	Sections 18, 19, 22, 32 PACE Whilst the Metropolitan Police guidance indicates reliance on PACE, they do not refer to section 20 and instead at Appendix A in their guidance refers specifically to Sections 18(1)(a)(b), 19(1), 22, 32(2)(a) and (b) and consent to conduct extraction. Their guidance states that: "5.1 Officers and staff are reminded that only data contained within the device is retrievable using PACE… 5.2 … Suspects: An officer can exercise his/her powers under PACE in obtaining material which is relevant to an investigation. Victims and Witnesses: … explicit consent obtained prior to the examination taking place… 5.3 Where consent is not provided … an officer may consider exercising his / her powers to obtain the required information.
Norfolk Constabulary	No clear legal basis identified
Suffolk Constabulary	No clear legal basis identified
Northumbria Police	There is no statutory power to 'examine' any item under PACE. 'Powers exist to seize and retain for examination but the power to examine is drawn from common law powers.'
Wiltshire Police	Refers more generally to statutory powers (s.32, s.18(1) PACE); however, these powers relate to entry to premises. Refers to the requirement for 'informed consent' or 'authorisation to interfere with the phone under Part III of the Police Act 1997'. It goes on to state that if the device has been seized 'lawfully' then the examination is lawful.
West Yorkshire Police	No clear legal basis identified

Lack of national guidance

The absence of a clear legal basis is accompanied by a lack of national guidance. However, there appears to be additional confusion as to whether there exists national guidance. Lancashire Constabulary informed us in their response that "There is a National guidance from NPIA". The National Policing Improvement Agency (NPIA) was replaced by the College of Policing between November 2011 and December 2012. We contacted the College of Policing and asked them for a copy of the current or draft policy / guidance in relation to the use of mobile phone extraction.

The College of Policing stated:

> "Further to our emails and after discussion with the relevant subject matter experts in the College, I write to confirm the following:
> - The College of Policing has not provided National guidance in this area as referenced in the letter sent to you by Lancashire Constabulary.
> - We understand that the Metropolitan Police are likely to have a policy and/or guidance given their work in this area but this is of course, not national guidance."

In addition, Deputy Chief Constable (DCC) Nicholas Baker stated[45] in January 2017 that:

> "We work with the forensic science regulator and associated network of experts to ensure that police forces have the necessary guidance to deploy these tools effectively and within the provisions of the law. Attaining accreditation and improving standards for digital forensics is a top priority for the police service that we will continue to work towards." [emphasis added]

Privacy International asked the National Police Chiefs' Council for guidance referred to by DCC Baker and noted that DCC Baker's statement referred to the Forensic Science Regulator's Codes of Practice and Conduct.[46] The NPCC stated that:

> "The Regulator's codes are helpful here in that they specify accreditation requirements for digital forensics including "the screening or recovery of data from a device using an off the shelf tool for factual reporting" e.g. mobile phone kiosks."

45 https://www.theguardian.com/uk-news/2017/jan/13/police-warrant-search-mobile-phones-campaigners-privacy-international

46 https://www.gov.uk/government/publications/forensic-science-providers-codes-of-practice-and-conduct-2016

They stated that in order to comply, police forces must be able to demonstrate that central configuration, control, environmental and competence requirements are in place:

> "DCC Baker has recommended that forces adopt this as part of their implementation of quality standards. All forces are currently implementing quality standards in digital forensics."

We contacted the Forensic Science Regulator to ask for the reports/reviews which have been conducted into the police use of mobile phone extraction tools. We were referred to page 4 of the codes of practice which provide little detail and told that "The Regulator has not produced reviews, reports or guidance additional to that contained in the Statement of Accreditation Requirements on this topic."

Lack of local guidance

Wiltshire Police state in their guidelines that "Currently there are no specific guidelines available in respect of mobile phone seizure and examination." Two police forces stated they have no local guidance or policy[47] and Surrey Police relied upon section 31(1)(a) Freedom of Information Act to refuse disclosure of guidance and policy.

Thames Valley Police and Hampshire Constabulary stated they rely on the Digital Investigation and Intelligence document[48]. Staffordshire Police stated they are looking at the issue of guidance under ISO 17025, which is the quality standard for forensics carried out in a laboratory setting and ISO 17020 which specifies requirements for competence of bodies performing inspection and for the impartiality and consistency of inspection activities.

Northumbria Police and City of London Police state they rely on manuals supplied by suppliers. The City of London Police stated:

> "The City of London Police uses the training guidance and manual supplied by our suppliers. Due to this we are unable to supply you with a copy of this manual…There is no policy as such to refer to apart from the obvious that you have to be trained and lawfully seized to undertake an examination."

We are concerned that some of the processes or procedures that do exist are written by the technology manufacturers, not by the police, thus abrogating responsibility for designing policing procedures to private companies.

Six forces stated the guidance is currently being "developed"[49] and two stated it was under review but did not disclose a draft version[50]. We followed up, several months later, with those forces who stated guidance was being developed, but were told the process was ongoing.

47 Durham Constabulary, Kent Police

48 http://www.npcc.police.uk/documents/reports/Digital%20Investigation%20and%20Intelligence%20Policing%20capabilities%20for%20a%20digital%20age%20April%202015.pdf

49 Avon and Somerset Constabulary, Devon & Cornwall, Dorset Police, Lancashire Constabulary, Lincolnshire Police,

50 Bedfordshire Police, Warwickshire Police

Procedures for carrying out extraction

In the local policies/guidance documents disclosed, there are details as to the procedures that should be in place when extractions are carried out.

Northumbria Police has a guidance procedure for ACESO mobile phone examination and "Guidance for Supervisors" in addition to the ACESO manuals (which have not been disclosed) which states that "All submissions for ACESO mobile phone examination must be authorised by a supervisor; Sergeant or Inspector." The Guidance further requires the investigating officer to complete the ACESO1 form: "It is their responsibility to precis the case and to justify the examination of each exhibit within the context of the case they are investigating. They will also be required to explain how the data types requested are proportionate and necessary in that particular case." The Sergeant of Inspector should only authorise the requested examination if they are satisfied that the exhibit has been lawfully seized (or consent has been given); and examination is justified; and the data types requested are proportionate. In addition,

> "When considering an application, the supervisor should have regard to factors like: How is the exhibit attributed to the subject? What is the likely relevance of material on the phone to the investigation? Are the data types requested proportionate and necessary?
>
> The Sergeant or Inspector must authorise the request by signing the ACESO1 form and making comment.
>
> If after discussion with the OIC the Supervisor is willing to authorise acquisition of some, but not all, of the requested data types, this should be made this clear [sic] in the comments section. Although the form is an electronic form on the web page it must be printed off by the OIC and presented to Sergeant or Inspector to authorise and sign … will be retained by the OIC as case papers (Unused in most cases)."

There has been no detailed independent oversight of this process, therefore it is unclear for example to what extent the comments fully detail consideration of the application as set out above. The example given in the guidance for what an authorisation might look like indicates a lack of detail:

> "Based on the information provided to me by (OIC), I am satisfied that the action proposed is justified for the enquiry, proportionate to what is sought to be achieved and that the activity does not require an authority for Directed or Intrusive surveillance. I authorise the examination of the device for the download of the data requested above."

As with Northumbria Police, Derbyshire Constabulary's guidance, whose stated purpose is to outline the procedure in relation to seizure, handling and submission of items for examination using the ACESO kiosk, dated May 2013, utilises a form. In this case it is a Form 56 – Phone Examination Request which is submitted by the OIC when they want a device examined, to record the rationale for the specific information required. The examination request must be approved and endorsed by an inspector who assesses proportionality, legitimacy and necessity. It is unclear if the assessment itself is recorded or whether the form is simply signed by the inspector. The submissions are all recorded on the 'Derbyshire Constabulary ACESO log'.

In addition to the authorisation form and the data extracted (in this case onto a CD), there may be accompanying documentation in the form of the examiners contemporaneous notes, pro-forma statement and photographs. The guidance sets out the procedure that should be followed by the examiner, which presumably should be recorded in their contemporaneous notes and available as part of disclosure to ensure that procedures were followed.

It should be noted that the Wiltshire Police guidance states that "the officer in the case may produce a sanitized version of the report prepared by the Phone Examiner, and this report will only contain data which is pertinent to the case." They note that all data is disclosable. It may depend on whether or not individuals or their representatives are aware that additional material may be available.

The Derbyshire Constabulary's guidance states that the extracts and report can be used during the suspect PACE interview process and used for a charging decision.

Whilst Derbyshire Constabulary's guidance appears to relate to ACESO units and refers to ACESO a number of times, in their FOIA response, they stated they in fact use forensics tools supplied by another company, MSAB.

Gwent Police's "XRY Kiosk mobile device extraction policy and procedure" and the Metropolitan Police's "Self-Service Equipment Kiosk Local Working Instructions Version 1.1" contain similar to information to that identified in Derbyshire Constabulary's guidance. The Metropolitan Police Service use a Form 105 for the submission process.

Wiltshire Police guidance considers potential for unlawful interception of communication and references the Regulation of Investigatory Powers Act 2000 noting that:

> "In relation to forensic examinations it is important to be aware that S.1 of the Regulation of Investigatory Powers Act 2000 (RIPA) 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."

The only other force to explicitly reference the risks identified by the Wiltshire Police guidance relating to RIPA is Gwent Police who briefly state that "Once in police possession any calls, texts or data transfers received by the device may constitute a communication breach in relation to RIPA."

Whilst, for example, Derbyshire Constabulary's guidance states that for preservation of evidence the phone should be switched off by the OIC, the handset examination steps state that the date and time displayed by the phone should be obtained, indicating the phone may be turned on. It does go on to note that "handsets that can be powered on and off using keys should be examined in a Faraday bag." However, there does not appear to be a clear warning of the risks associated with turning the phone on and potentially intercepting communications without the requisite legal basis.

Retention, deletion and individuals' rights

The speed at which extraction kiosks have been rolled out contrasts with the comparative lack of necessary public information raises concerns. For example, it is unclear:

(1) Whether victims, witnesses and suspects, including those released without charge or found innocent, are aware that personal information may have been taken from their phones without their knowledge.
(2) If consent is given by the user to the police force to extract data from mobile phones, how informed is that consent;
(3) What happens to the vast amount of data that is copied from the device;
(4) Whether data is shared with other bodies;
(5) If this data is deleted, and if so, after how long; and
(6) How securely the data is stored.

The use of SSK, purpose-built terminals in police stations to extract data, was, we understand, first trialled in 2012, in 18 Metropolitan Police Service boroughs[51]. The BBC reported on Metropolitan Police Service implementation of the system to extract mobile phone data from suspects held in custody, including call history, texts and contacts. This would be retained "regardless of whether any charges are brought."[52]

In relation to individual rights, the guidance provided by Derbyshire Constabulary indicates that extraction is often carried out without the device user's knowledge, stating:

> "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 on Guardian[53] where there is no evidence to support their link to criminality."

The lack of clarity as to the rights of individuals - whether or not they are asked to consent to the extraction; what, if any, consent or notification procedures are set

51 http://www.bbc.co.uk/news/technology-18102793

52 http://www.bbc.co.uk/news/technology-18102793

53 Guardian appears to refer to a storage database.

out in guidance documents; whether or not consent is actually lawfully required; and what rights individuals have in respect of the data - all need to be urgently addressed.

The Metropolitan Police Service SSK Local Working Instructions make passing reference to retention however they do not state which statutory obligations they are referring to, nor provide any evidence of oversight. They simply state "10.2 Where data is considered to have no policing purpose then the organisation has a statutory obligation to delete that data." The Derbyshire Constabulary Guidance refers to MOPI time frames. There is nothing specific in these guidelines which relates to data extracted from mobile phones.

Added to this is the lack of independent oversight or review. A number of forces stated they were currently undertaking reviews[54] of SSK. Despite repeated requests over the course of several months for the results of these reviews, including to Bedfordshire Police, Cheshire Constabulary, Devon and Cornwall Police, Durham Constabulary, we were told the reviews are ongoing and have not yet been completed.

Other forces confirmed no review[55] has been conducted. Despite stating that they do not use and had not trialled mobile phone extraction, Nottinghamshire Police stated in their response that they had conducted a review of SSK. Thames Valley Police stated that "Mobile phone kiosk downloading was included within our last HMIC PEEL effectiveness inspection". However, the available report dated 2016 and published in November 2017 does not appear to include such information.

54 Bedfordshire Police, Cheshire Constabulary, City of London Police, Durham Constabulary, Hampshire Constabulary, Hertfordshire Constabulary, Lancashire Constabulary, Merseyside Police, Staffordshire Police, Norfolk Constabulary and Suffolk Constabulary, Warwickshire Police, West Midlands Police, Devon and Cornwall Police

55 Avon and Somerset Constabulary, Derbyshire Constabulary, Gwent Police, Lincolnshire Police, Metropolitan Police Service

Business as usual

With plans to roll out extraction points now a reality it appears the police are keen to use extractive tools on a regular basis. The Metropolitan Police Service in a 2015 procurement document, obtained by the Bristol Cable, refer to the 'ingestion of data from tens of thousands of digital devices annually at dozens of different locations' and to 'maintenance [of the data] for an indefinite period extending for many years'.

Gwent Police state that their extraction kiosk "is designed to allow non-complex mobile device extraction to become 'business as usual for trained officers.'" The Metropolitan Police Digital Control Strategy, states that 'By default OICs[56] will be expected to attempt to examine digital devices on Self-Service Equipment (SSE).'

A 2017 report by Big Brother Watch, 'Police Access to Digital Evidence',[57] revealed that 93% of UK police forces are extracting data from digital devices including mobile phones, laptops, tablets and computers. To illustrate the numbers the report states that in 2016 alone, Derbyshire Constabulary extracted data from 635 computers and 680 mobile phones/tablets. For the period 2013 – 2016, the Metropolitan Police Service extracted data from 46,400 devices.

We are concerned that police forces are obtaining vast quantities of personal data about people not charged with any crime without their consent, for indefinite periods[58] without clear oversight, guidance or legislation. These concerns are amplified by the results of Privacy International's research. Based on responses to our FOIA requests, correspondence with the National Police Chief's Council and Forensic Science Regulator, there is no national guidance and a paucity of local guidance. The guidance that does exist is varied and often inconsistent.

56 OIC: Officer in Charge

57 https://bigbrotherwatch.org.uk/wp-content/uploads/2017/11/Police-Access-to-Digital-Evidence-Embargoed-1.pdf

58 The Metropolitan Police Service in a 2015 procurement document refer to the 'ingestion of data from tens of thousands of digital devices annually at dozens of different locations' and to 'maintenance [of the data] for an indefinite period extending for many years.' https://medium.com/privacy-international/press-release-unauthorised-use-of-mobile-phone-examination-tools-by-police-have-undermined-acf8986d29c2

Security of data

The risks associated with the inadequacy of the local guidance and absence of national guidance are underlined by the independent reviews on mobile phone extraction carried out in 2015, which formed part of the January 2017 disclosure[59].

The North Yorkshire Police report suggests local police forces are not yet ready to handle these highly intrusive tools, and it raises questions about whether other police forces have adopted these technologies appropriately. The Police have lost files, undermined serious investigations and failed to safeguard people's personal data.

The reports obtained in January 2017 exemplify a lax attitude towards encryption in relation to mobile phone data[60] which is reflected in the fact that it is not addressed in sufficient detail in the local policy documents disclosed. This in turn must be viewed in light of repeated serious failings in protecting sensitive information and various data breaches by the Police reported over the years.

We note that only Gwent Police, West Yorkshire Police and the Metropolitan Police Service guidance reference encryption of extracted data, albeit briefly.

In May 2017 Greater Manchester Police were 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."[61]

In March 2017 it was reported that technologies from the Police National Computer (PNC) systems through to the Automatic Number Plate Recognition (ANPR) databases are "increasingly being used by officers for non-work related reasons" according to the Police Federation. Andy Ward, Deputy General Secretary and Head of Crime said they were seeing about two cases a week involving data breaches[62].

59 https://medium.com/privacy-international/press-release-unauthorised-use-of-mobile-phone-examination-tools-by-police-have-undermined-acf8986d29c2

60 A report from 2015 by the Police and Crime Commissioner for North Yorkshire Police revealed that in half the cases sampled, there was a failure to receive authorisation for the use of mobile phone extraction tools and inadequate data security practices, failure to encrypt data and loss of files. https://medium.com/privacy-international/press-release-unauthorised-use-of-mobile-phone-examination-tools-by-police-have-undermined-acf8986d29c2

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

62 https://www.theregister.co.uk/2017/03/22/coppers_persistently_breaching_data_protecton_laws_with_pnc_and_anpr/

In July 2016, in a report entitled 'Safe in Police hands?', Big Brother Watch revealed that over 800 members of policing staff accessed personal information without a policing purpose between June 2011 and December 2015:

> "Specific incidents show officers misusing their access to information for financial gain and passing sensitive information to members of organised crime groups".[63]

63 https://www.bigbrotherwatch.org.uk/wp-content/uploads/2016/07/Safe-in-Police-Hands.pdf

Conclusion

Across the country the police have expanded their use of mobile phone extraction without public attention and without effective oversight. It is not enough to rely on PACE to search mobile phones - a piece of legislation written long before a phone became a device that could be used as a pocket surveillance tool. Traditional search practices, where no warrant is required, are wholly inappropriate for such a deeply intrusive search.

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 other electronic devices, Privacy International believes that PACE is insufficient and outdated to justify its wholesale extraction. There must be a clear legal basis for such action, national and local guidance, and the police should be required to obtain a judicially-authorised warrant prior to using extractive tools.

As noted in the landmark US ruling of Riley v California[64], 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 a 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".

The confusion between forces about whether PACE can or cannot be used for the extraction itself, the lack of a national guidance and reliance on laws that are not fit for the digital age, must be seen in the wider context of transparency and accountability, particularly in light of the Lammy Review, into experiences of Black, Asian and Minority Ethnic (BAME) individuals in the criminal justice system. A lack of national guidance inevitably means a lack of clear process and procedure for record keeping and audit trails across police forces. Combined with the apparent absence of independent oversight, this creates a significant risk of abuse and inability to examine whether mobile phone extraction powers can be used in unfair and discriminatory ways.

We call for an urgent review on the use of mobile phone extraction. There remain serious questions over when it is appropriate to obtain mobile phone data, what

64 https://www.supremecourt.gov/opinions/13pdf/13-132_8l9c.pdf

authorisation is necessary for extraction, how extracted data is stored, what volume of data is taken from individuals without their knowledge, how long it is retained and when it is deleted, what are the rights of individuals with regard to that data, and the lack of independent oversight.

We urge the government to consider the general requirement for a warrant before a search can take place.

Recommendations

- An immediate independent review into this practice should be initiated by the Home Office and/or College of Policing with consultations taken from the public, civil society, and industry as well as government authorities.
- Guidance aimed at the public regarding their rights must be published.
- The police must have a warrant issued on the basis of reasonable suspicion by a court before forensically examining anyone's smartphone, or otherwise accessing any content or communications data stored on the phone.
- A clear legal basis must be in place to inspect, collect, store and analyse data from devices. It must be considered whether such intrusive technology should only be used in serious crimes.
- There must be adequate safeguards to ensure intrusive powers are only used when necessary and proportionate.
- The analysis of necessity and proportionality should include any effect the police action may have on the security and integrity of the mobile phone examined, or mobile devices more generally.
- The owner and user(s) of any phone examined should be notified that the examination has taken place.
- Anyone who has had their phone examined shall have access to an effective remedy where any concerns regarding lawfulness can be raised.
- Cybersecurity standards should be agreed and circulated, specifying how data must be stored, when it must be deleted, and who can access.
- There must be independent oversight of the compliance by government authorities of the lawful use of these powers.
- All authorities who use these powers must purchase relevant tools through procurement channels in the public domain and regularly update a register of what tools they have purchased, including details on what tools they have, the commercial manufacturer, and expenditure amounts.

Annex

List of the 47 police forces contacted and summary responses

Forces using Self Service Kiosks (SSK) and/or Hubs

Police force	Use of SSK only - in low-level crime	Technology used
Bedfordshire Police	Low-level crime	MSAB
Durham Constabulary	Used in majority of crime	Radio Tactics, (ACESO) (MSAB)
Lancashire Constabulary	Low-level crime	Cellebrite
Warwickshire Police	Low-level crime	Cellebrite
West Mercia Police	Low-level crime	Cellebrite
West Midlands Police	Low-level crime	This information is exempt by virtue of Section 31(1)(a)(b), please see the detailed Public Interest rationale, at the end of the questions

Police force	Use of SSK only - in low-level and serious crime i.e. all crime	Technology used
Derbyshire Constabulary	Low-level and serious crime	MSAB
Gwent Police	Used when "appropriate"	MSAB
Norfolk Constabulary	Low-level and serious crime	MSAB
Hampshire Constabulary	Low-level and serious crime	Radio Tactics (ACESO)
Suffolk Constabulary	Low-level and serious crime	MSAB
Thames Valley Police	Low-level and serious crime	Radio Tactics

Police force	Use of SSK & Hubs in low-level crime	Technology used
City of London Police	Low-level crime	Cellebrite, (ACESO) (Radio Tactics), XRY (MSAB)

Devon and Cornwall Police	Low-level crime	Radio Tactics
Dorset Police	Low-level crime	Radio Tactics

Police force	**Use of SSK & Hubs in low-level and serious crime**	**Technology used**
Kent Police	Low-level and serious crime	MSAB MicroSystemations (MSAB) XRY kiosks
Metropolitan Police Service	Low-level and serious crime	MicroSystemations (MSAB) XRY kiosks
Northumbria Police	Low-level and serious crime	Cellebrite, ACESO (Radio Tactics)
Staffordshire Police	Low-level and serious crime	ACESO (Radio Tactics)
Lincolnshire Police	Low-level and serious crime	Cellebrite
Surrey Police	Low-level and serious crime	MSAB

Police force	**Use of SSK & Hubs – unknown low-level or serious crime**	**Technology used**
Wiltshire Police	Unknown	Radio Tactics

Police force	**Use of Hubs only - unknown low-level or serious crime**	**Technology used**
Merseyside Police	Unknown	Not provided
West Yorkshire Police	Unknown	Not provided
North Wales Police	Unknown	Not provided

Police force	**Use of Hubs and mobile units - unknown low-level or serious crime**	**Technology used**
British Transport Police	Unknown	Cellebrite, MSAB

Forces who failed to respond

Cleveland Police
Cumbria Constabulary
Essex Police

North Yorkshire Police	
Sussex Police	

Forces not currently using SSK/Hubs but about to trial Cellebrite or other extractive tools for the first time

Avon and Somerset Constabulary	"At the time of this request Avon and Somerset Constabulary were not using downloading kiosks to carry out mobile phone data extract, however this is due to start. Low level crime would include drugs, assaults and public orders." They confirmed that they have Cellebrite tools and a disclosed contract with Cellebrite refers to 'F-UFD-15-032 UFED Infield Kiosk Logical."
Gloucestershire Constabulary	"The Constabulary is about to trial Cellebrite (UFED)"
Leicestershire Police	"There are plans to implement a kiosk product to supplement our existing capacity but, at this time, we do not operate these kiosks. There is a trial ongoing in relation to the use of a kiosk product with a view to utilising these in investigations."

Forces who have trialled mobile phone extraction but stated they do not currently use it

	If your police force is not currently using mobile phone extraction kiosks, have you trialled this?
Cheshire Constabulary	"Yes"
Hertfordshire Constabulary	"Yes"
Humberside Police	"Humberside Police has trialled using mobile phone extraction kiosks"
Police Service of Scotland	"We have previously trialled the use of kiosks in the East of Scotland for low-level crime, defined as that which appears from the outset to be a case likely to be prosecuted at 'summary' level."
Dyfed-Powys Police	"I can confirm that Dyfed Powys Police did trial the kiosk product and found that it did not suit the forces' needs."

Forces who state they hold no information / not trialled or used mobile phone extraction

Cambridgeshire Constabulary
Greater Manchester Police
Northamptonshire Police
Nottinghamshire Police
South Yorkshire Police
Police Service of Northern Ireland
South Wales Police
Ministry of Defence Police

Privacy International
62 Britton Street, London EC1M 5UY
United Kingdom

Phone +44 (0)20 3422 4321
www.privacyinternational.org
Twitter @privacyint

UK Registered Charity No. 1147471