DIGITAL STRIP SEARCHES:

The police's data investigations of victims

July 2019

BIG BROTHER WATCH
DEFENDING CIVIL LIBERTIES, PROTECTING PRIVACY

bigbrotherwatch.org.uk
@bbw1984

ABOUT BIG BROTHER WATCH

Big Brother Watch exposes and challenges threats to our privacy, our freedoms and our civil liberties at a time of enormous technological change in the UK.

We work to roll back the surveillance state and protect the rights of everyone in the UK to be free from unfair intrusion.

We campaign to protect freedoms in Parliament and through the courts. We produce unique research and investigations, and seek to educate and empower the public.

Big Brother Watch is a cross–party, non-party, independent non-profit organisation leading the protection of privacy and civil liberties in the UK. In our pursuit for change, we use advocacy and campaigns; parliamentary lobbying; public interest litigation; research and investigations that inform policy and public debate; and public education and empowerment.

CONTACT

Silkie Carlo
Director
Email: silkie.carlo@bigbrotherwatch.org.uk

Griff Ferris
Legal and Policy Officer
Email: griff.ferris@bigbrotherwatch.org.uk

24hr media line: 07730 439257

www.bigbrotherwatch.org.uk

CONTENTS

EXECUTIVE SUMMARY

The widespread use of mobile phones and other digital devices in people's everyday lives means we increasingly leave a data trail everywhere we go.

Our digital footprints can reveal where we have been and when, who we have spoken to, the content of our private conversations and, via our internet history, even some of our innermost thoughts.

More and more, such data is being sought in criminal investigations. Clearly, data from devices can be highly relevant to investigations, particularly if the offence involves digital communications. But our research has revealed that police are seeking masses of personal data by default that is not relevant to an investigation at all, and may not be lawful.

The scale and depth of the police's mobile phone searches are incomparable with the police's legislative powers to carry out physical searches. It would amount to police searching someone's property and taking copies of all photographs, documents, letters, films, albums, books and files.

These would be intrusive searches even for most suspects of crime. But now, police are carrying out these intrusive digital searches against victims of crime.

Police, pressured by the Crown Prosecution Service, are demanding victims sign blank cheque "consent" forms allowing access to their digital lives, warning them that the investigation will likely be discontinued if they refuse. The police use mobile phone extraction tools to download the contents of victims' mobile phones and digital devices.

Victims who do give blanket consent to these digital interrogations are afforded no protections. All the data taken from their devices, which can even include their social media accounts, can be kept by the police for up to 100 years. Victims are told that if there is evidence of any suspected offences found in that digital information, police will subject them, or a person they have communicated with such as a friend or family member, to a criminal investigation.

These digital strip searches are not only cruel, invasive and causing major delays to investigations - they breach victims' fundamental rights and obstruct justice. These

invasive practices are highly likely to infringe victims' data protection and privacy rights protected by the Data Protection Act and the Human Rights Act.

Our research shows that these digital interrogations have been used almost exclusively for complainants of rape and serious sexual offences so far. But since police chiefs formalised this new approach to victims' data through a national policy in April 2019, they claim they can also be used for victims and witnesses of potentially any crime.

The searches appear to be driven by a generalised suspicion of complainants, and mobile data trails are increasingly being seen as character references. By analysing victims' digital lives, police attempt to infer "evidence" from information spanning years, analysing what kind of person they are, examining who they have relationships with, and even speculating about their state of mind.

Victims are faced with an impossible choice – the pursuit of justice or the protection of their privacy. No one should be faced with such a choice.

This creeping norm of using data trawls to treat victims like suspects marks a disturbing, radical change within our criminal justice system. Anyone of us could become a victim of a crime and suddenly find our private lives subject to intense digital scrutiny. Those who refuse will be exempt from justice.

This report is the first comprehensive examination of this new policy. In conclusion, we propose urgent reforms that would make the most of the opportunities digital evidence can bring to criminal justice, whilst protecting fundamental rights and the integrity of our justice system.

OUR CALL FOR CHANGE:

Big Brother Watch is calling on the National Police Chiefs' Council to urgently reform this failed digital evidence policy:

- **Victims' consent to access their personal records should be freely given, specific and limited to the information relevant to the crime – not blanket. Victims of crime should never have to sign away their privacy rights in the pursuit of justice.**

- **The police's digital evidence technology should be brought up to date so police can collect targeted pieces of evidence from smart phones, rather than entire digital copies.**

- **Police should not be using artificial intelligence to conduct fishing expeditions through victims' phones.**

This call has been signed by Amnesty International, Big Brother Watch, the Centre for Women's Justice, End Violence Against Women, JUSTICE, Liberty, Privacy International, Southall Black Sisters and The Survivors Trust.

In addition, it has been signed by the Victims Commissioner for England and Wales, Dame Vera Baird, and Jess Phillips MP and Caroline Lucas MP.

Furthermore, 35,000 people have now signed Big Brother Watch's petition calling on the police and the Crown Prosecution Service to stop forcing sexual assault survivors to hand in their phones in investigations.[1]

Our voices must be heard.

1 https://you.38degrees.org.uk/petitions/stop-forcing-sexual-assault-survivors-to-hand-in-their-phones-in-investigations

POLICE TAKING VICTIMS' MOBILE PHONES AND DIGITAL INFORMATION

Digital evidence from mobile phones, computers and other digital devices is unsurprisingly involved in an increasing number of criminal investigations. Our 2017 investigation into police use of digital evidence found that 93% of police forces were extracting data from digital devices including mobile phones, laptops, tablets and computers.[2]

Alarmingly, we now know that police are not only taking digital devices from suspects, but are also demanding them from victims of crime. Victims are being subjected to suspicionless, far-reaching digital interrogations when they report crimes to police. Currently, this practice is being applied almost exclusively to victims of rape and serious sexual offences – but it is set to be applied to victims of potentially any crime

Our new Freedom of Information campaign has confirmed this practice. 100% of UK police forces that responded to our FOI requests confirmed that they take digital information from complainants of sexual offences' mobile phones and other devices. 37 UK police forces – 82% of the total – responded to our FOI requests.[3]

The Crown Prosecution Service pressures police to collect masses of digital information on victims, regardless of its relevance to the investigation. According to national police representatives, Police and Crime Commissioners and an independent review of the investigation and prosecution of rape, the Crown Prosecution Service consistently rejects case files which do not provide the requested extensive digital – and other – information.[4] Police officials have reported that unless this action is taken, the Crown Prosecution Service *"will not consider a charge"*.[5] Even the police themselves have questioned *"the need for so much information"*.[6]

These digital interrogations significantly increased in December 2017 following the high-

---

2 Big Brother Watch, 'Police Access to Digital Evidence', November 2017 (https://bigbrotherwatch.org.uk/wp-content/uploads/2017/11/Police-Access-to-Digital-Evidence-1.pdf)

3 Avon and Somerset Constabulary, Bedfordshire Police, Cambridgeshire Constabulary, Cheshire Constabulary, Cleveland Police, Derbyshire Constabulary, Devon and Cornwall Police, Dorset Police, Durham Police, Dyfed Powys Police, Essex Police, Gloucestershire Constabulary, Greater Manchester Police, Gwent Constabulary, Hampshire Constabulary, Hertfordshire Constabulary, Kent Police, Lancashire Constabulary, Lincolnshire Police, Merseyside Police, Metropolitan Police, Norfolk Constabulary, North Wales Police, Northumbria Police, Nottinghamshire Police, Police Service of Northern Ireland, Police Scotland, South Wales Police, South Yorkshire Police, Staffordshire Police, Suffolk Constabulary, Surrey Police, Thames Valley Police, Warwickshire Police, West Mercia Constabulary, West Midlands Police, Wiltshire Constabulary. (https://bigbrotherwatch.org.uk/all-campaigns/freedom-of-information-requests/)

4 PCC Dame Vera Baird QC, 'Written evidence from Office of the Police and Crime Commissioner for Northumbria', (http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/justice-committee/disclosure-of-evidence-in-criminal-cases/written/80665.pdf); APCC calls for inquiry to look at all sides of disclosure – APCC, 14 February 2018: (http://www.apccs.police.uk/latest_news/apcc-calls-inquiry-look-sides-disclosure/); Rt Hon Dame Elish Angiolini QC, 'Report of the Independent Review into the Investigation and Prosecution of Rape in London - 'Angiolini Review', 2015, para 518 (https://www.cps.gov.uk/sites/default/files/documents/publications/dame_elish_angiolini_rape_review_2015.pdf)

5 Dame Vera Baird QC, PCC for Northumbria, 'Letter to Justice Committee', 14 February 2018

6 Rt Hon Dame Elish Angiolini QC, 'Report of the Independent Review into the Investigation and Prosecution of Rape in London', 2015, para 518 (https://www.cps.gov.uk/sites/default/files/documents/publications/dame_elish_angiolini_rape_review_2015.pdf)

profile collapse of several rape prosecutions due to disclosure errors in relation to digital evidence.[7] However, this form of speculative and excessive data gathering from victims does not address disclosure failings; in contrast, it creates additional unnecessary work for an already strained criminal justice system.

In April 2019, in response to widespread criticism, the National Police Chiefs' Council introduced new 'Digital Processing Notices' for use by police across England and Wales, intended to obtain victims' consent for the extraction and analysis of their personal digital information from mobile phones and devices.[8]

However, far from improving the system and protecting victims from intrusive digital investigations, these new police 'Digital Processing Notices' entrench and reinforce the unspecified, unlimited and coercive demands for disproportionate volumes of personal data from victims, enabling completely excessive downloads.

Police mobile phone extractions

Currently, the police can access, extract and analyse a victim's mobile phone or other digital device and all of the information on it without any restrictions, safeguards or oversight. Police are using crude and intrusive technology to extract huge amounts of personal digital information, and even deleted information.

Our research shows that these digital searches are disproportionate by default, extending far beyond the collection of specified pieces of evidence.

The new police 'Digital Processing Notice' which is given to victims states that their mobile phone or other digital device will be subjected to one of three types of digital 'extraction', either *"at the police station"* or *"a digital forensics laboratory"*:[9]

- **Level 1 'logical' extraction:** *"This may provide almost all of the data you could see if you were to turn on the device and browse through it. It will not normally extract data that has been deleted from the device."*
- **Level 2 'logical' or 'physical' extraction:** *"either a "logical"*

7 House of Commons Justice Committee, 'Disclosure of evidence in criminal cases', Eleventh Report of Session 2017-19, 17 July 2018 (https://publications.parliament.uk/pa/cm201719/cmselect/cmjust/859/859.pdf)

8 NPCC 'Digital Processing Notice', published 29 April 2019 (https://www.npcc.police.uk/documents/NPCC%20FINAL%20CONSENT%20v1.2.pdf)

9 NPCC 'Digital device extraction – information for complainants and witnesses', published 29 April 2019 (https://www.npcc.police.uk/documents/NPCC%20FINAL%20CONSENT%20v1.2.pdf)

extraction using selected tools in a laboratory environment or a "physical" extraction, which recovers a copy of the data held on the memory chip of the device. "Physical" downloads can extract deleted data, although capabilities vary depending on the nature of the device and the operating system."

– **Level 3:** *"These are usually expert or bespoke methods to tackle complex issues or damaged devices".*[10]

> *"...even though we may only consider a limited number of messages relevant to the investigation, the tool may obtain all messages"*[14]

Police explicitly tell victims that they will extract more information than they need or even want as part of the investigation. In the 'Digital Processing Notice' provided to victims, they state:

"The data that can be extracted may vary by handset and the extraction software used. (E) Some technology will not be able to obtain material using parameters such as a specific time period, ***meaning even though we may only consider a limited number of messages relevant to the investigation, the tool may obtain all messages."***[11] On the Digital Processing Notice, there is space for the investigating officer to identify the data they seek from the phone – but rather than seeking specific evidence, the form invites investigators to request entire categories of data:

"In order to investigate the crime you are involved in, ***the police intend to extract the following data categories from the device*** *e.g. call data, messages, email, contacts, applications (apps), internet browsing history etc.:"* [12]

This is thought to be in part due to the fact that the police's digital extraction technology is designed to extract bulk data rather than specified evidence – although on a technical level, it is entirely possible to extract specified pieces of evidence.

10 NPCC 'Digital device extraction – information for complainants and witnesses', published 29 April 2019 (https://www.npcc.police.uk/documents/NPCC%20FINAL%20CONSENT%20v1.2.pdf)

11 NPCC 'Digital device extraction – information for complainants and witnesses', published 29 April 2019 (https://www.npcc.police.uk/documents/NPCC%20FINAL%20CONSENT%20v1.2.pdf), emphasis added

12 NPCC 'Digital Processing Notice', published 29 April 2019 (https://www.npcc.police.uk/documents/NPCC%20FINAL%20CONSENT%20v1.2.pdf)

The police say that regardless of what data is listed as being necessary for the investigation *"Each of these [extraction] levels may extract data in addition to that listed above by the investigating officer"*.[13] This provides the police with a blank cheque to take unlimited amounts of personal digital information from victims' mobile phones and devices.

Evidently, all of the extraction methods set out in the police's 'Digital Processing Notice' are designed to take vast amounts of personal data – often, ***all*** of the data available on their phone – rather than specified and limited pieces of evidence.

Some phones can contain over 200,000 messages and over 100,000 photos. The personal data on some phones would produce "millions of A4 sheets" if printed out in their entirety[17, 20]

Private, personal and sensitive messages, photos and videos

The information taken from a phone can include texts, encrypted WhatsApp messages or other messaging apps, call logs, contacts, emails, photos, videos, internet browsing history, notes, maps and GPS, location information, and more. Some phones can contain over 200,000 messages and over 100,000 photos.[14] The Crown Prosecution Service also often requires police investigators to request victims' online passwords and information, including social media account logins and personal 'cloud' storage services.[15]

This information can run to many thousands of pages. An average individual's mobile phone can contain the equivalent of 35,000 A4 pages of data.[16] Assistant Commissioner and National Police Chiefs' Council Criminal Justice Lead Nick Ephgrave even described how some phones produce *"millions of A4 sheets"* if printed out in their entirety.[17]

---

13 NPCC 'Digital Processing Notice', published 29 April 2019 (https://www.npcc.police.uk/documents/NPCC%20FINAL%20CONSENT%20v1.2.pdf)

14 NPCC and CPS evidence to the Justice Committee Inquiry into Disclosure in Criminal Cases (http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/justice-committee/disclosure-of-evidence-in-criminal-cases/written/80778.pdf)

15 Rt Hon Dame Elish Angiolini QC, 'Report of the Independent Review into the Investigation and Prosecution of Rape in London', 2015 (https://www.cps.gov.uk/sites/default/files/documents/publications/dame_elish_angiolini_rape_review_2015.pdf); Dame Vera Baird QC, PCC for Northumbria, 'Letter to Justice Committee', 14 February 2018

16 Office of the Police and Crime Commissioner Northumbria, Written evidence to the Justice Committee, 24 April 2018 (data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/justice-committee/disclosure-of-evidence-in-criminal-cases/written/80665.pdf)

17 https://www.theguardian.com/society/2019/apr/29/new-police-disclosure-consent-forms-could-free-rape-suspects

Much of this information is incredibly personal, including private conversations with friends, family members and partners; personal and potentially sensitive photographs and videos; personal notes; financial information; and even legally sensitive work-related information such as in emails. Most people's phones and communications contain sensitive information classed as 'special category data' under data protection law: information about an individual's race, ethnic origin, politics, religious or philosophical beliefs, health, sex life or sexual orientation, and as such data extraction from phones requires robust safeguards.[18]

Mobile phone extraction tools

The police are deploying a wide range of commercially-bought technologies to extract data from personal devices.

In 2018, Privacy International reported that over half of UK police forces were using mobile phone extraction technology within their own forces, with the rest either trialling or intending to trial the technology, or contracting out to the private sector.[19]

Mobile device extraction software from mobile forensics company MSAB is being used by at least 11 UK police forces.[20] MSAB software allows the police to *"overcome security and encryption challenges on locked devices".*[21] It also allows police to *"recover[ing] data beyond the mobile device"* and access *"online social media data and app-based information"* for apps such as WhatsApp, iCloud, Facebook, Google, Twitter, Instagram, Snapchat and others.[22] MSAB has previously publicly claimed: *"If you've got access to a sim card, you've got access to the whole of a person's life".*[23]

Cellebrite, used by at least 7 UK police forces,[24] claims that its software can *"extract, preserve and analyse public- and private-domain, social media data, instant messaging, file storage, web pages and other cloud-based content"* as well as *"detailed location information"* and even *"a subject's history of text searches, visited pages, voice-search recordings and translations from Google web history".*[25]

---

18 General Data Protection Regulation (GDPR), Article 9(2) supplemented by the Data Protection Act 2018, Schedule 1

19 HMICFRS, PEEL: Police effectiveness 2017', March 2018 (https://www.justiceinspectorates.gov.uk/hmicfrs/wp-content/uploads/peel-police-effectiveness-2017.pdf)

20 Privacy International, 'Digital Stop and Search', March 2018 (https://privacyinternational.org/sites/default/files/2018-03/Digital%20Stop%20and%20Search%20Report.pdf)

21 https://www.msab.com/products/xry/

22 https://www.msab.com/products/xry/xry-cloud/

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

24 Privacy International, 'Digital Stop and Search', March 2018 (https://privacyinternational.org/sites/default/files/2018-03/Digital%20Stop%20and%20Search%20Report.pdf)

25 https://www.cellebrite.com/en/products/ufed-cloud-analyzer/

Radio Tactics[26] software is used by 10 UK police forces.[27] Radio Tactics claims that its digital device extraction tool, ACESO, *"can obtain information that would otherwise be unavailable. This data can lead to additional cause for arrest and the identification of associates and other people of interest"*.[28] Radio Tactics also states that its software *"enables non-experts to capture evidence and intelligence from digital mobile devices, SIM and memory cards"*.[29]

If you've got access to a SIM card, you've got access to the whole of a person's life.[26]

These mobile phone extraction technology companies boast of the specifications of their tools and systems and the possibility of downloading and accessing specific data from a device. However this contradicts the police's claim in their 'Digital Processing Notice' policy that technology they use requires them to download excessive information far beyond what is relevant to a case.

It is clear that it is not simply technological limitations that are responsible for driving the police's disproportionate data collection – far more sophisticated and targeted technologies exist. The "collect it all" approach appears to be purposefully aimed at those who attract suspicion – which makes the disproportionate application of this approach to victims of sexual offences all the more concerning.

Digital searches are far more permissive than equivalent physical searches

The intrusiveness of a search and download of a smart phone often eclipses that of a physical property, such is the personal nature of the information held on our phones. The data contained on a mobile phone or similar digital device in 2019 exceeds much of the informational contents of a pre-digital age house, such as letters, personal notes and notebooks, photographs, files, financial information, and work or employment

26 https://radio-tactics.com/

27 Privacy International, 'Digital Stop and Search', March 2018 (https://privacyinternational.org/sites/default/files/2018-03/Digital%20Stop%20and%20Search%20Report.pdf)

28 https://radio-tactics.com/products/aceso-kiosk/

29 https://radio-tactics.com/products/aceso-kiosk/

information. It extends to information that has never before been recorded so regularly and voluminously, including private conversations with friends, family and distant contacts on social networks, work communications, and messages on dating apps. It even extends to information that has never before been recorded at all, such as the thought processes, mental explorations and formation of opinions that are reflected in our internet browsing data.

However, for police to carry out a consensual search of even a suspect's physical property and take away documents there are several criteria police must meet.

The Police and Criminal Evidence Act (PACE) 1984 safeguards individuals from intrusive or excessive police searches of physical property. Under PACE 1984 Code B, which relates to the search of a premises with consent, police must obtain the written consent of the individual for the search.[30] The individual concerned:

"must be clearly informed they are not obliged to consent, that ***any consent given can be withdrawn at any time*** *including before the search starts or while it is underway".* [Emphasis added][31]

The police officer in charge must ensure that consent is not being given *"under duress".*[32] The requirements continue:

"Before seeking consent the officer in charge of the search shall state the purpose of the proposed search and its extent. This information ***must be as specific as possible, particularly regarding the articles or persons being sought and the parts of the premises to be searched."*** (Emphasis added)[33]

When a search has been carried out, police have to provide *"a written notice: specifying what has been seized".*[34]

It is clear that police's unrestricted and disproportionate approach to taking vast swathes of victims' personal information in so-called consensual digital searches goes far beyond the comparable legislative regime regulating consensual physical property searches.

30 Police and Criminal Evidence Act 1985, Code B, paragraph 5.1

31 Police and Criminal Evidence Act 1985, Code B, paragraph 5.2

32 Police and Criminal Evidence Act 1985, Code B, paragraph 5.3

33 Police and Criminal Evidence Act 1985, Code B, paragraph 5.2

34 Police and Criminal Evidence Act 1985, Code B, paragraph 7.12

Suspects have more protection than victims in digital investigations

The lack of safeguards for victims in the context of digital searches is in stark contrast to the legal protections for suspects' mobile phones and digital devices.

The police have general powers of seizure and specific powers of seizure of *"computerized information"* under Section 19 and 20 of the Police and Criminal Evidence Act 1984. However, in practice suspects' devices are not taken or requested by default as victims' devices often are.[35] Relevant police policy also contains many safeguards and restrictive guidance to protect suspects. The Association of Chief Police Officers (ACPO) *ACPO Good Practice Guide for Digital Evidence* provides some relevant guidance for police officers (although it was published in March 2012, over 6 years ago, and ACPO has since been replaced by the National Police Chiefs' Council).[36] The ACPO Guide is centered entirely on criminal investigations of suspects and considers only the extraction of digital evidence "seized" as part of police investigations. The Guide states that complete copies of all the information on a device should only be made *"wherever practical, proportionate and relevant"*.[37] It makes clear that devices should only be seized if they are *"likely to hold evidence"*, and that *"digital devices and media should not be seized just because they are there"*.[38] It also states that police *"must have reasonable grounds to remove property and there must be justifiable reasons for doing so"*.[39]

The *Attorney General's Supplementary Guidelines on Digitally Stored Material* published in 2013 is similarly aimed specifically at safeguarding police investigations of suspects. It also states that investigators should seize as little material from suspects as possible during an investigation.[40]

The Law Commission has even proposed to update current requirements in relation to

35 Rape Crisis England and Wales written evidence to the Justice Committee Inquiry on Disclosure of evidence in criminal cases, March 2018 (http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/justice-committee/disclosure-of-evidence-in-criminal-cases/written/80748.html)

36 ACPO, 'ACPO Good Practice Guide for Digital Evidence' March 2012 (http://library.college.police.uk/docs/acpo/digital-evidence-2012.pdf)

37 Para 2.2.4, ACPO, 'ACPO Good Practice Guide for Digital Evidence' March 2012 (http://library.college.police.uk/docs/acpo/digital-evidence-2012.pdf)

38 Paragraph 4.3, ACPO, 'ACPO Good Practice Guide for Digital Evidence' March 2012 (http://library.college.police.uk/docs/acpo/digital-evidence-2012.pdf)

39 Para 4.3.2, ACPO, 'ACPO Good Practice Guide for Digital Evidence' March 2012 (http://library.college.police.uk/docs/acpo/digital-evidence-2012.pdf)

40 Attorney General's Office, 'Attorney General's Guidelines on Disclosure' December 2013 (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/262994/AG_Disclosure_Guidelines_-_December_2013.pdf); Justice, Written evidence to the Justice Committee inquiry into disclosure of evidence in criminal cases, June 2018 (http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/justice-committee/disclosure-of-evidence-in-criminal-cases/written/84429.pdf)

search warrants, including *"introducing safeguards whenever electronic devices are seized under a search warrant so that devices are examined and returned swiftly."*[41] There is no indication that this will extend to victims of crime.

Rape Crisis England and Wales has said that:

"*There are still huge concerns that someone who reports rape to the police is routinely asked to surrender all of their personal digital data and sign away their right to privacy while a suspected rapist doesn't endure the same level of scrutiny."*[42]

It is right that there are safeguards and protections in place to prevent police from overly-intrusive investigations and digital searches of suspects' devices. However, it is a gross oversight that victims of crime are afforded no protections at all.

Disproportionate treatment of victims of sexual offences

The National Police Chiefs' Council and the Crown Prosecution Service have stated very clearly that their new national policy around mobile phones and digital evidence applies to victims of all crimes.

However, in practice, this approach has thus far been used almost exclusively against victims of rape and serious sexual offences. The (then) APCC Victims' Lead Vera Baird and (then) Victims' Commissioner for England and Wales Baroness Newlove reported that if the same individual reports a physical assault, with no sexual element, even if they are the only witness and even if the defendant denies the allegation, they will not be asked for such personal documentation, or for their mobile phone.[43] This disparity occurs despite the police and Crown Prosecution Service being under exactly the same obligations in all criminal cases.

The Victims' Commissioner for London called the criminal justice system's approach to using material from victims' phones to discredit their claim *"victim blaming"*, and warned that it feeds into the *"dangerous myths and stereotypes surrounding rape"*.[44] Rape Crisis England and Wales has made clear that *"the sensation of sex crime survivors is often that*

41 Law Commission, 'Public should be given more search warrant protections – Law Commission', 5 June 2018 (https://www.lawcom.gov.uk/public-should-be-given-more-search-warrant-protections-law-commission/)

42 https://www.endviolenceagainstwomen.org.uk/disclosure-crisis-reveals-rape-investigations-are-still-all-about-victim-credibility/

43 http://www.northumbria-pcc.gov.uk/article-dame-vera-baird-baroness-newlove-disclosure-must-put-victims-first/

44 https://www.independent.co.uk/voices/rape-trial-evidence-disclosure-cps-cases-victims-commissioner-justice-select-committee-a8482946.html

they are being put on trial".[45]

The Director of the Centre for Women's Justice, Harriet Wistrich, has also said that the National Police Chiefs' Council and Crown Prosecution Service 'Digital Processing Notice':

"...will primarily be used for cases of reported rape, sexual assault and domestic abuse, rather than for other criminal offences. Thus those impacted are very predominantly women and the policy is therefore discriminatory."[46] It is important to acknowledge that this policy has been introduced into a criminal justice system that has a well-documented history of treating victims of sexual offences with disbelief and focusing on attempts to discredit them. There are clear and concerted efforts to remedy this – but the use of excessive digital searches effectively as character references for victims is clearly a retrograde step.

Unfortunately, there is a widespread belief in the UK, encouraged by media headlines, that there are a vast number of false allegations of sexual violence. This is a myth. The latest available figures from the Crown Prosecution Service show that 0.62% of rape allegations were prosecuted as false allegations.[47] Government figures estimate that over 80% of serious sexual assaults are never reported at all.[48]

False allegations are a serious matter. If there is clear and objective evidence that someone is lying to the police it must be followed up and investigated. However, this does not mean that every victim who reports a sexual offence to the police should be treated like a suspect and have their digital private life investigated by default.

Treating victims like suspects deters them from coming forward and bringing criminals to justice.

Excessive digital investigations cause huge delays to the criminal justice system

The extraction and analysis of so much digital information – including large amounts of completely irrelevant data – unsurprisingly causes huge delays to investigations, prosecutions, and the criminal justice system as a whole.

---

45 https://www.theguardian.com/law/2018/may/15/police-mishandling-digital-evidence-forensic-experts-warn

46 https://www.dailymail.co.uk/news/article-6970319/How-shameful-victims-violated-says-womens-justice-campaigner.html

47 Crown Prosecution Service, 'Charging Perverting the Course of Justice and Wasting Police Time in Cases Involviung Allegedly False Rape and Domestic Violence Allegations', March 2013 (https://www.cps.gov.uk/sites/default/files/documents/legal_guidance/perverting-course-of-justice-march-2013.pdf#page=6)

48 https://www.theguardian.com/uk-news/2018/feb/08/sexual-assault-women-crime-survey-england-wales-ons-police-figures

Police tell victims via 'Digital device extraction' information sheets provided with the 'Digital Processing Notice' that taking their phone or device and extracting digital information *"can take some time"* and as a result, *"we need to keep your phone and any other devices for several months"*. In addition, the forms also warn that police *"may request it from you at a later stage"*.[49]

Our Freedom of Information investigation has found that current practices are swamping police in digital devices and evidence, with average delays of up to 6 months for digital devices to be examined. The Metropolitan Police, the UK's largest police force, reported 9 month delays for "*complex phone examinations*".[50]

Police force	Average wait time for digital devices to be examined[1]
Bedfordshire Constabulary	29 days (4 weeks)
Devon and Cornwall Police	25 weeks (over 5 months)
Dorset Police	18 weeks (over 4 months)
Durham Police	6 weeks
Essex Police	175 days (25 weeks, over 5 months)
Hampshire Constabulary	68 days (over 2 months)
Hertfordshire Constabulary	3 weeks
Kent Police	4 days – 144 days (over 4 months)[2]
Merseyside Police	12 weeks (3 months)[3]
Metropolitan Police	3 – 9 months[4]
South Yorkshire Police	4 – 12 weeks (up to 3 months)
West Midlands	20 – 139 days (over 4 months)[5]

Note: 26 police forces responded to this FOI request, of which only 12 police forces recorded any data on wait times. Interpretation of device 'examination' varied between forces – it appears that most forces interpreted this as a technical examination/data extraction, rather than including the time taken for a police investigator to sift through and report on all of the data. See our website campaign page 'Victims Not Suspects' for the Freedom of Information responses.

It is estimated that excessive data collection causes overall delays of up to 18 months to the life cycle of a criminal case, with estimates in some parts of the country reaching

49 NPCC Digital device extraction – information for complainants and witnesses, published 29 April 2019 (https://www.npcc.police.uk/documents/NPCC%20FINAL%20CONSENT%20v1.2.pdf)

50 https://bigbrotherwatch.org.uk/all-campaigns/freedom-of-information-requests/

1 12 forces (out of 45) responded with waiting times. A further 14 forces responded saying they didn't record waiting times or held no information (https://bigbrotherwatch.org.uk/all-campaigns/freedom-of-information-requests/)

2 Kent Police reported that where there was a 'Service Level Agreement' that a mobile phone examination should take 28 days, the average turnaround is 66 days, and for 75 day 'Service Level Agreement', the average wait time is 144 days.

3 Merseyside Police reported they had a 'Service Level Agreement' that mobile phones will be examined within 12 weeks

4 Metropolitan Police reported 3 month wait for 'Standard' examinations, and 9 months for 'complex phone examinations'

5 West Midlands reported that it took 20 days for a priority examination, with 'Reporting' in 'Priority' cases taking 93 days, and 139 days in 'Standard' cases.

2 years.[51] End Violence Against Women Coalition reports that cases *"which may have already taken a 12-24 months to come to trial can take significantly longer if there is a lot of digital evidence to analyse."* [52]

The National Police Chiefs' Council and the Crown Prosecution Service recognise that being *"denied access to a telephone could cause serious financial and social hardship or risk to personal safety"*.[53] Rape Crisis also has said that throughout this time a victim will experience:

"considerable anxiety, fear and stress in relation to the process, as well as a direct impact of the sexual violence they have experienced. Many child, young person or adult victim/survivors will question their continued engagement with the system due to the overly long time frames." [54]

It is estimated that excessive data collection causes overall delays of up to 2 years to the life cycle of a criminal case[54]

Once a victim's device(s) are taken by the police for examination, they will not be returned to them until the end of criminal proceedings or when the case is closed.

Victims' consent to access their personal records should be freely given, specific and limited to the information relevant to the crime – not blanket. Victims of crime should never have to sign away their privacy rights in the pursuit of justice.

Our call for change: The police's digital evidence technology should be brought up to date so police can collect targeted pieces of evidence from smart phones, rather than entire digital copies.

---

51 https://www.theguardian.com/commentisfree/2018/mar/21/rape-complainant-loss-privacy-intrusive-investigations

52 End Violence Against Women Coalition written evidence to the Justice Committee Inquiry on Disclosure in criminal cases, March 2018 (https://www.endviolenceagainstwomen.org.uk/wp-content/uploads/EVAW-Coalition-Submission-to-Justice-Committee-Disclosure-Inquiry-March-2018-1.pdf)

53 NPCC and CPS evidence to the Justice Committee Inquiry into Disclosure in Criminal Cases (http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/justice-committee/disclosure-of-evidence-in-criminal-cases/written/80778.pdf)

54 Rape Crisis England and Wales written evidence to the Justice Committee Inquiry on Disclosure of evidence in criminal cases, March 2018 (http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/justice-committee/disclosure-of-evidence-in-criminal-cases/written/80748.html)

The police's digital evidence technology should be brought up to date so police can collect targeted pieces of evidence from smart phones, rather than entire digital copies.

VICTIMS, ‘CONSENT’ AND THE LAW

Historically, police seized complainants' mobile phones and digital devices under laws intended for use against suspects of criminal offences.[55]

Over the years, police forces began to use vague, broadly worded and coercive 'consent' statements to obtain obtain huge amounts of victims' personal digital information and attempt to comply with data protection laws. Until recently, police forces in England and Wales designed their own digital and personal information 'consent' forms.

Using the Freedom of Information Act, Big Brother Watch obtained 20 of these forms from 45 forces – each revealing a disproportionate approach to personal data collection from victims.

Astonishingly, 11 police forces that responded to our FOI requests from December 2018 said that they were still seizing complainants' mobile phones and digital devices under the Police and Criminal Evidence Act 1984.[56]

Police 'Digital Processing Notices'

In January 2019, the National Police Chiefs' Council instructed all police forces to stop seizing victims' mobile phones and digital evidence under the Police and Criminal Evidence Act 1984. The National Police Chiefs' Council stated that the only proper basis for collecting victims' mobile phones and information was via their "*informed and ongoing consent*", and that this should be obtained by a new national 'consent' form, created alongside the Crown Prosecution Service[57] - the new Digital Processing Notice introduced in April 2019.

The NPCC Lead for Criminal Justice, Assistant Commissioner Nick Ephgrave, said that they introduced the new national forms *"to help police seek informed consent proportionately and consistently"*.[58]

However, these new forms appear to be plainly incompatible with legal requirements in relation to data protection and consent under the General Data Protection Regulation and Data Protection Act 2018, as well as the right to privacy under the Human Rights Act 1998.

The Digital Processing Notice, whilst professing to function as a lawful consent form:

- **Does not expressly ask for victims' "consent" but for victims to confirm**

55 Police and Criminal Evidence (PACE) Act 1984, Section 19 and 20

56 https://bigbrotherwatch.org.uk/all-campaigns/freedom-of-information-requests/

57 National Police Chiefs' Council, 'Consent for Digital Downloads during the course of an investigation', 16 January 2019 (https://www.north-wales.police.uk/media/655973/2018-1166-victims-consent.pdf)

58 https://news.npcc.police.uk/releases/progress-update-in-meeting-the-disclosure-challenge

they "understand" why the police want to take their phones;

- **Tells victims police will extract excessive personal information regardless of its relevance, ranging from entire categories of data to a forensic copy of all data on their phones;**
- **Tells victims that if they do not give blanket consent to a disproportionate digital search, their case may not be investigated or prosecuted;**
- **Threatens victims with prosecution** if evidence of suspected criminal offences is found.

These forms clearly require non-specific, blanket consent to unlimited amounts of data and are framed in a coercive manner. Lawful consent, on the other hand, must be informed, specific, limited and freely given.

We raised our concerns about these new forms in a meeting with the Crown Prosecution Service and National Police Chiefs' Council on 17 January 2019. We were informed that limited police technology was partly to blame, but also that the police and Crown Prosecution Service needed to review mobile phone information *"because some complainants lie"*.

An unlawful approach to consent

The police and Crown Prosecution Service say they are using victims' consent as the legal basis for the extraction, analysis and disclosure of the information from their mobile phones and digital devices. Consent to the extraction, analysis and disclosure ('processing') of personal data is a legal basis set out in data protection law, under the General Data Protection Regulation and the Data Protection Act 2018.[59]

We believe that obtaining victims' consent is the right legal basis to collect their personal information, if obtained lawfully under a clear legal framework. Consent offers an individual, who is seeking to assist the criminal justice system, the ability to provide relevant evidence whilst protecting their privacy and data rights. It is the victim's decision to report a crime and provide evidence, including in the form of digital information, to the police. Therefore, consent is essential in the process of proportionate evidence gathering.

However, the police and Crown Prosecution Service's 'Digital Processing Notice' does not allow lawful consent. Under data protection law, a person's consent must be freely given,

59 General Data Protection Regulation, Recital 32 (Conditions for consent) and Article 7, supplemented by the Data Protection Act 2018

specific, informed and unambiguous, and withdrawable.[60] However, currently consent is coerced, blanket, ambiguous and cannot be withdrawn once given.

Consent must be freely given

In this context, 'freely given' means that the victim cannot be coerced or pressured into consenting to the collection and processing of their personal information. They must be able to refuse to give consent without undue detriment to them, and must be able to withdraw consent easily at any time. If the victim has no real choice, consent is not freely given.[61]

However, the police currently coerce victims into giving consent to these excessive digital downloads. The police form itself states that their case may not be investigated or prosecuted if they refuse to consent to the excessive digital downloads:

"If you do not provide consent for the police to access data from your device for the police to investigate, or for the prosecution to disclose material then it may not be possible for the investigation or prosecution to continue."[62]

The threat is that if the individual does not consent to these excessive digital downloads, the investigation or prosecution cannot continue. There are numerous accounts from victims' whose cases have been dropped as a result of this refusal. Victims are also warned that even if the case does continue, "*defence representatives will be told of your refusal*".[63]

The police's forms note the influence of the Crown Prosecution Service in this process, who, the forms state, *"will advise the investigating officer about what data should be examined before a case is charged"*.[64] The (then) Association of Police and Crime Commissioners Victims' Lead Vera Baird reported that the pressure to obtain so much excessive and unnecessary information, and refusal to prosecute without it, comes from the Crown Prosecution Service (CPS):

"When the police resist CPS requests to review and retrieve non-relevant material which is

60 General Data Protection Regulation, Recital 32 (Conditions for consent) and Article 7

61 Information Commissioners Office, 'What is valid consent?' (https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/what-is-valid-consent/)

62 NPCC, 'Digital Processing Notice' published 29 April 2019 (https://www.npcc.police.uk/documents/NPCC%20FINAL%20CONSENT%20v1.2.pdf)

63 NPCC 'Digital device extraction – information for complainants and witnesses', published 29 April 2019 (https://www.npcc.police.uk/documents/NPCC%20FINAL%20CONSENT%20v1.2.pdf)

64 NPCC 'Digital device extraction – information for complainants and witnesses', published 29 April 2019 (https://www.npcc.police.uk/documents/NPCC%20FINAL%20CONSENT%20v1.2.pdf)

not the subject of any reasonable inquiry, the response of the CPS is sometimes that the case will not be progressed should the material not be reviewed and potentially disclosed.

"Some officers believe that this CPS practice is due to nervousness at 'missing something', worsened by the recent high profile disclosure failings. However, such a broad-brush approach to every case is unsuitable, and each case should be considered on its own." [65]

The Association of Police and Crime Commissioners has also previously stated that

"...evidence on the ground suggests that even when officers are confident that they have pursued all reasonable lines of inquiry, they are often being told by CPS to pursue all other available sources." [66]

A 2015 review of the investigation and prosecution of rape cases in London noted that the Crown Prosecution Service "*consistently reject [case] files due to the absence of key information such as social media*".[67]

Consent must be specific

In this context, 'specific' means that police or the Crown Prosecution Service must only be able to access, collect and analyse information that has been clearly defined and limited before lawful, informed consent can be given - for example, a set of messages between two individuals within a proportionately specified time period. The Data Protection Act 2018 also requires that information processed by law enforcement must be relevant and not excessive.[68]

However, the police and Crown Prosecution Service forms request blanket access to entire data categories as a minimum, despite admitting only a small amount of it is relevant to their investigation.[69] This is unacceptable.

Rape Crisis England and Wales has reported an incident of alleged rape where the police's response was:

---

65 PCC Dame Vera Baird QC, 'Written evidence from Office of the Police and Crime Commissioner for Northumbria', (http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/justice-committee/disclosure-of-evidence-in-criminal-cases/written/80665.pdf)

66 APCC calls for inquiry to look at all sides of disclosure – APCC, 14 February 2018: (http://www.apccs.police.uk/latest_news/apcc-calls-inquiry-look-sides-disclosure/)

67 Rt Hon Dame Elish Angiolini QC, 'Report of the Independent Review into the Investigation and Prosecution of Rape in London', 2015, para 518 (https://www.cps.gov.uk/sites/default/files/documents/publications/dame_elish_angiolini_rape_review_2015.pdf)

68 Section 37, Data Protection Act 2018.

69 NPCC 'Digital Processing Notice', published 29 April 2019 (https://www.npcc.police.uk/documents/NPCC%20FINAL%20CONSENT%20v1.2.pdf)

"*...to search the survivor's phone for information that related to 3 years prior to the rape. This time frame did not appear to be based on any guidelines and appeared arbitrary.*"[70]

Rape Crisis has also said that for many of those who access its services:

"*...the fact that their phone, tablet or laptop will be downloaded without the clarity around which specific data is being sought can feel like they themselves are being treated as a suspect.*"[71]

Previously, the Director of Public Prosecutions Max Hill QC has said that "*seeking to examine the mobile telephones of complainants and witnesses is not something that should be pursued as a matter of course in every case*"; that investigations must not be *"a purely speculative enquiry";* and that they must *"avoid unnecessary intrusion into a complainants' personal life."* [72] While these comments are welcome, this contradicts the effect of these blanket digital consent statements and as such is not the reality faced by victims.

Consent must be informed and unambiguous

The requirement that consent must be 'informed and unambiguous' means that the complainant must be fully aware of the process they are consenting to, the specific information they are consenting to, and their rights, including the right to withdraw their consent.[73]

However, the forms do not provide clear and unambiguous information on what data will be downloaded from victims' devices, instead referring to entire data categories: *"call data, messages, email"*.[74] The fact that police provide a catch-all caveat, stating that *"Each of these [extraction] levels may extract data in addition to that listed above by the investigating officer"*,[75] means that this is ultimately a blank cheque for police and prosecutors to download excessive personal information.

---

70 Rape Crisis England and Wales written evidence to the Justice Committee Inquiry on Disclosure of evidence in criminal cases, March 2018 (http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/justice-committee/disclosure-of-evidence-in-criminal-cases/written/80748.html)

71 Rape Crisis England and Wales written evidence to the Justice Committee Inquiry on Disclosure of evidence in criminal cases, March 2018 (http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/justice-committee/disclosure-of-evidence-in-criminal-cases/written/80748.html)

72 https://www.independent.co.uk/news/uk/crime/rape-victims-trial-sexual-offences-phone-data-records-seized-cps-prosecutions-max-hill-a8632411.html

73 General Data Protection Regulation, Recital 32 (Conditions for consent) and Article 7

74 NPCC 'Digital Processing Notice', published 29 April 2019 (https://www.npcc.police.uk/documents/NPCC%20FINAL%20CONSENT%20v1.2.pdf)

75 NPCC 'Digital Processing Notice', published 29 April 2019 (https://www.npcc.police.uk/documents/NPCC%20FINAL%20CONSENT%20v1.2.pdf)

The police 'Digital Processing Notice' does not even use the language of consent. Instead, victims are merely asked to sign to indicate that they "*understand*" the "*process*". Therefore, victims cannot be deemed to give informed, unambiguous consent to this process, and the police forms do not even allow for lawful consent to be given.[76]

'Special category data' requires additional safeguards

Under data protection law, there are further requirements in relation to processing 'special category data': information which is more sensitive and so needs more protection.

Special category data includes sensitive information about an individual's race, ethnic origin, politics, religious or philosophical beliefs, health, sex life or sexual orientation.[77] It is extremely likely that some if not all of this information is contained on individuals' mobile phones and digital devices, either within messages, apps, or wider social media information accessible through these devices. The requirements for processing special category data include obtaining an individual's explicit consent and that there must be additional safeguards.[78]

However, under the current process there is neither an individual's explicit consent, nor are there additional safeguards or protective rules governing access and retention of the extracted data.

The Information Commissioner has reported significant concern over the number of serious breaches resulting from the police's collection and retention of excessive data from victims of crime.

In one chilling example, Kent Police gave the entire contents of a victim's phone to the alleged perpetrator's solicitor, which was then handed to the defendant. The victim had given her phone to police because it contained a single video supporting her testimony, but officers downloaded files including text messages and photographs.[79]

---

76 NPCC 'Digital Processing Notice', published 29 April 2019 (https://www.npcc.police.uk/documents/NPCC%20FINAL%20CONSENT%20v1.2.pdf)

77 General Data Protection Regulation (GDPR), Article 9(2) supplemented by the Data Protection Act 2018, Schedule 1

78 General Data Protection Regulation (GDPR), Article 9(2) supplemented by the Data Protection Act 2018, Schedule 1

79 Information Commissioner's Office, Written evidence to the Justice Committee, March 2018 (http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/justice-committee/disclosure-of-evidence-in-criminal-cases/written/80671.pdf); https://www.bbc.co.uk/news/uk-england-kent-36101713

Police threaten to prosecute victims for other criminal offences and share their data with unknown government agencies, even internationally

Incredibly, the police forms threaten victims that if they find evidence on the victim's phone that they or others they know have committed criminal offences, they will be investigated:

"If information is identified from your device that suggests the commission of a separate criminal offence, other than the offence(s) under investigation, the relevant data may be retained and investigated by the police. This data may be shared with other parties including, for example other police forces or a court in any criminal proceedings." [80]

The police also state that they may retain any information found on police intelligence databases, and that it may even be shared amongst other government agencies, including governments abroad:

"If your device contains information that may assist in the prevention or detection of crime, or protecting the vulnerable, then the ***police may process and retain this information on our intelligence management system*** *and/or share that information with relevant parties/agencies, including other police forces or government agencies,* ***including those outside of the UK.***" [81] [Emphasis added]

There is no further explanation of this process, or of any safeguards or redress that the victim can access. As such, victims are being asked to 'consent' to incredibly broad, vague and completely unforeseeable uses of their digital information.

Many people will be concerned at this threat to investigate, not least in light of the fact that the police have given themselves the power to extract any or all information they want from victims' phones. People are likely to be deterred from reporting crimes due to a fear that they may be investigated for even minor offences, or that they may incriminate their friends or family by handing over their communications to the police. Moreover, in a system where police have reported rape victims to immigration enforcement,[82] this is an incredibly real threat which will undoubtedly put some of the most vulnerable people off reporting.

80 NPCC 'Digital device extraction – information for complainants and witnesses', published 29 April 2019 (https://www.npcc.police.uk/documents/NPCC%20FINAL%20CONSENT%20v1.2.pdf)

81 NPCC 'Digital device extraction – information for complainants and witnesses', published 29 April 2019 (https://www.npcc.police.uk/documents/NPCC%20FINAL%20CONSENT%20v1.2.pdf)

82 https://www.theguardian.com/lifeandstyle/2017/nov/28/victim-arrested-on-immigration-charges-after-going-to-police

Infringement of victims' right to privacy

There is no doubt that victims' Article 8 right to a private life under the Human Rights Act 1998 is engaged by the excessive collection of victims' digital information by the police and the Crown Prosecution Service.

Even the police and Crown Prosecution Service have recognised that this process *"is an intrusion into the complainant's privacy"*.[83]

These digital interrogations cannot be considered necessary or proportionate. As the current police process does not meet required data protection standards, there is no legal basis for this infringement. There are no safeguards against indiscriminate and disproportionate extraction, analysis and disclosure of victims' personal and sensitive information from their mobile phones: the police policy explicitly provides for unnecessary, disproportinate data downloads.

The police cannot rely on a victim's consent as a waiver of their right to privacy - the 'consent' obtained is not lawful, as considered above.[84]

We believe that the current policy and 'Digital Processing Notices' are highly likely to constitute an infringement of victims' right to a private life under the Human Rights Act 1998.

Our call for change:

Victims' consent to access their personal records should be freely given, specific and limited to the information relevant to the crime – not blanket. Victims of crime should never have to sign away their privacy rights in the pursuit of justice.

83 NPCC and CPS evidence to the Justice Committee Inquiry into Disclosure in Criminal Cases (http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/justice-committee/disclosure-of-evidence-in-criminal-cases/written/80778.pdf)

84 *DH v Czech Republic* (2008) 47 EHRR 3 at §202

Victims' consent to access their personal records should be freely given, specific and limited to the information relevant to the crime – not blanket. Victims of crime should never have to sign away their privacy rights in the pursuit of justice.

POLICE USE OF ARTIFICIAL INTELLIGENCE TO ANALYSE VICTIMS' INFORMATION

Police in England and Wales are using artificial intelligence to analyse the excessive digital information they are taking from victims of crime.

The digital technology company Cellebrite confirmed in 2018 that it was working with a dozen UK police forces, including the Metropolitan Police. It refused to name other forces due to apparent commercial non-disclosure agreements with the respective forces.[85] Staffordshire Police has also confirmed that it was working on AI to analyse digital evidence.[86]

In addition, two police forces trialled artificial intelligence for the *"search and analysis of mobile phone downloads"* and *"identifying the relevance of material"* in 2018. These were Surrey Police and *"one in the East Midlands"* according to the Director of Public Prosecutions in 2018.[87]

The Metropolitan Police has confirmed that it has been exploring Cellebrite's 'Analytics Enterprise' artificial intelligence tool to analyse digital evidence.[88] Cellebrite claims that its 'Analytics Enterprise' tool:

"...is a force multiplier that uses Artificial Intelligence (AI), and machine learning algorithms, to automatically surfaces (sic) *formative leads and actionable insights from every bit and byte of digital data during the early hours of an investigation."*[89]

There are a long list of chilling and intrusive actions that Cellebrite claims its Analytics tools can achieve:

"Cellebrite Analytics automatically merges large quantities of disparate mobile, cloud, computer and telco data sources so users can simultaneously identify patterns, reveal connections and uncover leads with greater speed and accuracy".[90]

"Automatically aggregate and merge multiple identifiers across different sources to see a suspect's complete digital persona and their map of connections".[91]

---

85 https://www.theguardian.com/uk-news/2018/may/27/police-trial-ai-software-to-help-process-mobile-phone-evidence

86 https://www.theguardian.com/uk-news/2018/may/27/police-trial-ai-software-to-help-process-mobile-phone-evidence

87 Director of Public Prosecutions written evidence to the Justice Committee, February 2018 (http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/justice-committee/disclosure-of-evidence-in-criminal-cases/written/86396.pdf)

88 https://www.theguardian.com/uk-news/2018/may/27/police-trial-ai-software-to-help-process-mobile-phone-evidence

89 https://cf-media.cellebrite.com/wp-content/uploads/2019/05/DataSheet_Analytics_A4_web-v3.pdf

90 https://www.cellebrite.com/en/analytics/

91 https://cf-media.cellebrite.com/wp-content/uploads/2019/05/DataSheet_Analytics_A4_web-v3.pdf

"Surface insights from seemingly unrelated events, locations and relationships"[92]

"Automatically detect and categorize image frames such as weapons, drugs and documents using advanced facial recognition and image categorization".[93]

"...detect and match objects within images and video such as weapons, money, nudity and more".[94]

"...visualise social networks and feed in data from multiple phones to highlight, via geo-tagging data, when people were in the same place at the same time".[95]

This intrusive, experimental technology claims to be able to carry out incredibly intrusive analysis using masses of people's personal data. It is described as a tool aimed at targeting 'suspects'. This is the kind of investigation that victims of crime, particularly victims of serious sexual offences, risk being subjected to.

Our Freedom of Information investigation

Following these concerning reports, we sent freedom of information requests to all police forces asking them whether they were using artificial intelligence to analyse victims' mobile phones and digital information. Despite the widely publicised details and reports that several forces were trialling this technology, not a single force disclosed using it in relation to victims.

This lack of transparency around the use of advanced and intrusive technology in the criminal justice system is unacceptable, particularly the deliberate use of commercial non-disclosure agreements.

The law on artificial intelligence and automated decision making

The use of an automated processing system to analyse the contents of a victim's mobile phone or digital device, and potentially make decisions on the relevance of digital evidence to a police investigation, would engage the right not to be subject to a decision based solely on automated processing, under data protection law.[96] Police would be required to have a lawful basis to carry out such profiling or automated decision making, and they would

92 https://www.cellebrite.com/en/analytics/

93 https://cf-media.cellebrite.com/wp-content/uploads/2019/05/DataSheet_Analytics_A4_web-v3.pdf

94 https://www.cellebrite.com/en/products/analytics-enterprise/

95 https://www.theguardian.com/uk-news/2018/may/27/police-trial-ai-software-to-help-process-mobile-phone-evidence

96 Data Protection Act 2018, Section 49 and Section 50, and Article 22, General Data Protection Regulation

have to notify individuals both about this process and their rights to have the decision(s) reconsidered or a new decision taken.[97]

It is unclear whether victims are specifically informed of the use of such technologies or given the opportunity to explicitly consent to their use. We are not aware of any individual being notified that their mobile device or digital information has been subject to analysis by artificial intelligence.

In addition, the ethical issues of sifting through victims' digital lives with artificial intelligence are profound and have not been fully considered by any components of the criminal justice system.

Moreover, the very basis of such technological analysis is flawed. The role of artificial intelligence has become a consideration *because* of the excessive collection of huge volumes of data from victims. Innovative technology is not appropriate for, and cannot remedy, a situation built on a breach of rights. The solution is lawful and proportionate collection of evidence – not experimental artificial intelligence to brush the unlawful and disproportionate collection of personal information under the carpet.

The chilling prospect of artificial intelligence-led investigations into serious crimes

These proposals create the possibility that when a victim reports sexual violence to the police, they will have their phone taken and their personal information analysed by a machine carrying out a fishing expedition without human oversight. This is a deeply disturbing concept.

Neither the police nor the Crown Prosecution Service should be outsourcing such extremely sensitive tasks to an experimental computer system that automates data processing, obstructs accountability and transparency, and could allow for even more disproportionate intrusions of privacy.

Our call for change:

Police should not be using artificial intelligence to conduct fishing expeditions through victims' phones.

97 Data Protection Act 2018, Section 49 and Section 50

Police should not be using artificial intelligence to conduct fishing expeditions through victims' phones.

PUBLIC RESPONSE

The police and Crown Prosecution Service's approach to victims of rape and serious sexual offences' mobile phones and digital information has been heavily criticised by senior police figures, and victims and rights organisations.

The former Chair of the National Police Chief's Council, Sara Thornton, cautioned against intrusive police investigation of victims:

> *"We cannot allow people to be put off reporting to us because they fear intrusion into their lives and private information that's not relevant to the crime being shared in court."*[98]

The former Association of Police and Crime Commissioners (APCC) Victims' Lead Vera Baird, now Victims Commissioner for England and Wales, warned that these investigations would result in *"many complainants withdraw[ing] their complaint"* and also that *"people may be put off complaining of sexual assaults"*.[99] She concluded:

> *"We need to ensure that complainants are not discouraged from coming forward to report sexual offences by inappropriate 'fishing' into personal records, access to which is demanded in no other kind of case."* [100]

The Victims' Commissioner for London, Claire Waxman, expressed similar fears that women would not report rape to police because they fear that irrelevant material from their phones would be taken and potentially used against them to discredit their account.[101]

Rape Crisis England and Wales reported that for many of those who access their services *"the fact that their phone, tablet or laptop will be downloaded without the clarity around which specific data is being sought can feel like they themselves are being treated as a suspect."* [102]

Big Brother Watch made a formal complaint to the Information Commissioner in November

98 NPCC Chief Sara Thornton, Police Chief's blog, 11 February 2018 (https://news.npcc.police.uk/releases/police-chiefs-blog-cc-sara-thornton-on-disclosure)

99 Dame Vera Baird QC, PCC for Northumbria, 'Letter to Justice Committee', 14 February 2018

100 Dame Vera Baird QC, PCC for Northumbria, 'Letter to Justice Committee', 14 February 2018

101 https://www.independent.co.uk/voices/rape-trial-evidence-disclosure-cps-cases-victims-commissioner-justice-select-committee-a8482946.html

102 Rape Crisis England and Wales written evidence to the Justice Committee Inquiry on Disclosure of evidence in criminal cases, March 2018 (http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/justice-committee/disclosure-of-evidence-in-criminal-cases/written/80748.html)

2018, calling for a high priority investigation into the intrusive digital investigations of victims, the unchecked use of invasive mobile phone extraction tools, and the police and Crown Prosecution Service's use of blanket 'consent' forms.[103] The Information Commissioner's Office announced in December 2018 that it would conduct a high priority investigation into the issue.[104]

National coverage and criticism

The release of the new police 'Digital Processing Notices' in April 2019 generated a widespread national outcry.

Almost 35,000 people signed Big Brother Watch's petition calling on the police and the Crown Prosecution Service to stop demanding sexual assault survivors' mobile phones. 15,000 signatories also sent emails in protest to the NPCC and Minister for Policing.[105]

Many MPs and other high profile figures spoke out against the policy.

The Shadow Attorney General, Shami Chakrabarti, said that:

> *"Any suggestion that rape victims must automatically hand over their phones in exchange for the support of the authorities is as unlawful as it is wrong. Women, who are the overwhelming majority of rape victims, are already discriminated against in judicial system. A trawl through their social media only reinforces the idea they are in the dock. This is the effect of the purported 'consent form'."* [106]

103 Big Brother Watch, Letter to the Information Commissioner, 9 November 2018 (https://bigbrotherwatch.org.uk/wp-content/uploads/2018/11/Letter-to-the-ICO-redact.pdf)

104 Information Commissioner, Letter to Big Brother Watch, 4 December 2018 (https://bigbrotherwatch.org.uk/wp-content/uploads/2018/12/Letter-from-the-ICO-re-priority-investigation-4-December-2018-redacted.pdf)

105 https://you.38degrees.org.uk/petitions/stop-forcing-sexual-assault-survivors-to-hand-in-their-phones-in-investigations

106 https://labour.org.uk/press/shami-chakrabarti-responds-rape-victims-asked-hand-phones-police/

The Labour Party leader Jeremy Corbyn said that:

> *"with rape and sexual assaults already under-reported, this disturbing move risks letting more rapists get away with it".*[107]

In response to the widespread and sustained criticism of the new forms the Minister for Policing, Nick Hurd, said that the police 'consent' forms *"attempt to distil best practice to ensure that there is consistency and clarity for complainants".*[108] He said that *"police have acknowledged that the use of personal data in criminal investigations is a source of anxiety"* and that:

"They will continue to work to ensure that their approach to this issue strikes the necessary, if difficult, balance between the requirement for reasonable lines of inquiry and the victim's right to privacy." [109]

An urgent debate was held in Parliament, in which MPs lined up to castigate the police and Crown Prosecution's treatment of victims of crime, particularly victims of rape and sexual offences.

Anna Soubry MP warned that the police policy was a "*blanket request to rape victims, or indeed any other victim, to hand over phones and other digital devices*" and that:

> *"it is going to deter victims of rape in particular from coming forward".*[110]

Chair of the Joint Committee on Human Rights, Harriet Harman MP, gave the harrowing account of a woman who had contacted her about her own experience:

---

107 https://www.theguardian.com/society/2019/apr/29/police-face-legal-action-over-requests-for-victims-digital-records

108 Hansard, Urgent debate 'Rape Victims: Disclosure of Evidence', Volume 659, 29 April 2019 (https://hansard.parliament.uk/commons/2019-04-29/debates/5BF3D4EA-A2DC-47D8-98FF-E1070FB4E3BE/RapeVictimsDisclosureOfEvidence)

109 Hansard, Urgent debate 'Rape Victims: Disclosure of Evidence', Volume 659, 29 April 2019 (https://hansard.parliament.uk/commons/2019-04-29/debates/5BF3D4EA-A2DC-47D8-98FF-E1070FB4E3BE/RapeVictimsDisclosureOfEvidence)

110 Hansard, Urgent debate 'Rape Victims: Disclosure of Evidence', Volume 659, 29 April 2019 (https://hansard.parliament.uk/commons/2019-04-29/debates/5BF3D4EA-A2DC-47D8-98FF-E1070FB4E3BE/RapeVictimsDisclosureOfEvidence)

> *"She said:* ***'Six months ago, I was seriously sexually assaulted by a complete stranger. Two months after the assault, the police demanded full access to my phone, including my Facebook and Instagram passwords, my photos, stretching back to 2011, notes, texts, emails and the full history of 128 WhatsApp groups and individuals' conversations stretching back over five years. I had no prior or subsequent contact with my attacker. I lie awake at night worrying about the details of private conversations with friends, boyfriends, business contacts, family that are now in the hands of the police. It is a gross intrusion into my privacy and theirs. I feel completely as if I am the one on trial.'"***[111]

Harriet Harman MP said that *"there is a real problem out there that has been exposed"* and called on the Minister for Policing *"to take action on it"*.[112]

Chair of the Home Affairs Select Committee, Yvette Cooper MP, said that it was *"pretty obvious that the form will deter people from coming forward and pursuing cases"* and that

> *"in the interests of justice for women who are victims of awful crimes, the Minister should pull this document back and get the police and the Crown Prosecution Service to rewrite it."* [113]

Sir Edward Davey MP said that it was *"vital that we ensure that nothing is done to prevent people from coming forward"* and that the policy *"should be reviewed"*.[114]

Stuart C. McDonald MP said that *"Investigations in pursuit of information must be evidence-led and targeted"* and that there must be a *"proportionate and sensible way to support justice and protect privacy at the same time"*, but that the police's policy *"gets that balance totally wrong"*.[115]

---

111 Hansard, Urgent debate 'Rape Victims: Disclosure of Evidence', Volume 659, 29 April 2019 (https://hansard.parliament.uk/commons/2019-04-29/debates/5BF3D4EA-A2DC-47D8-98FF-E1070FB4E3BE/RapeVictimsDisclosureOfEvidence)

112 Hansard, Urgent debate 'Rape Victims: Disclosure of Evidence', Volume 659, 29 April 2019 (https://hansard.parliament.uk/commons/2019-04-29/debates/5BF3D4EA-A2DC-47D8-98FF-E1070FB4E3BE/RapeVictimsDisclosureOfEvidence)

113 Hansard, Urgent debate 'Rape Victims: Disclosure of Evidence', Volume 659, 29 April 2019 (https://hansard.parliament.uk/commons/2019-04-29/debates/5BF3D4EA-A2DC-47D8-98FF-E1070FB4E3BE/RapeVictimsDisclosureOfEvidence)

114 Hansard, Urgent debate 'Rape Victims: Disclosure of Evidence', Volume 659, 29 April 2019 (https://hansard.parliament.uk/commons/2019-04-29/debates/5BF3D4EA-A2DC-47D8-98FF-E1070FB4E3BE/RapeVictimsDisclosureOfEvidence)

115 Hansard, Urgent debate 'Rape Victims: Disclosure of Evidence', Volume 659, 29 April 2019 (https://

Following this widespread criticism of the police's policy, and many victims coming forward to share harrowing accounts of their own experiences, the Association of Police and Crime Commissioners (ACPP), took the extremely unusual step of calling on the National Police Chiefs' Council and Crown Prosecution Service to urgently reform the new 'consent' form.

The APCC's deputy victims lead, Julia Mulligan, who recently revealed that she was raped when she was 15, said:

> *"As someone with lived experience, I can tell you that it is hard enough having to live through a sexual attack or rape without having to expose oneself to this 'in return' for an investigation. And to be told you have no chance of justice without doing so is truly awful."* [116]

The APCC's Criminal Justice Lead, David Lloyd, said that:

> *"We have no doubt that this form, as it currently stands, should be withdrawn, or it is likely to result in a loss of confidence in the police, the CPS and the criminal justice system more broadly."*[117]

Big Brother Watch shares these concerns.

hansard.parliament.uk/commons/2019-04-29/debates/5BF3D4EA-A2DC-47D8-98FF-E1070FB4E3BE/RapeVictimsDisclosureOfEvidence)

116 https://www.theguardian.com/society/2019/may/04/police-commissioners-criticise-rape-victim-data-request-form

117 https://www.theguardian.com/society/2019/may/04/police-commissioners-criticise-rape-victim-data-request-form

VICTIMS' EXPERIENCES

Anonymous

A woman who reported being violently sexually assaulted had her case dropped because she refused to hand over the entire contents of her mobile phone.

"A few years ago I was violently sexually assaulted by a "friend" on a night out. It was a sustained and sadistic attack that in no way began with consent. I made the incredibly difficult decision to report it to the police because I needed to take power back.

"Even though some time had elapsed between the assault and my reporting of it, there was evidence that the police acknowledged as compelling. Despite this, my case was dropped not because of an unlikely prospect of conviction, but because I refused to hand over my mobile phone to be downloaded in its entirety.

"I consider that request to be a gross violation of my human rights. What is on my phone is private and irrelevant to the crime that was committed."

"The way I have been treated by the Crown Prosecution Service has affected me deeply. In the years of dealing with intrusive requests from the police, such as asking for my counselling or medical records, I have been a shadow of my former self. They would tell me I had to supply this information or they wouldn't pursue my case. I was diagnosed with PTSD, not from the assault but from how I was treated by the authorities after reporting it. Over the course of the investigation, when a new request for deeply personal information would come in, I had panic attacks that resulted in 999 calls.

"Unable to think properly or function for months at a time, I felt betrayed by the people who should have been there to help."

"Imagine your most private thoughts and feelings from counselling held in your phone being seen by anyone, let alone your rapist."

"And imagine having no guarantee about how in the future this data may be used or stored. The decision to have my case dropped was a no-brainer for self-preservation, but I now feel that the requirement to surrender one's data is the same as being raped with impunity.

"The optimism I had at the beginning of this process of "taking power back" has been replaced with a feeling of absolute helplessness. Why would other victims of rape or sexual assault come forward to make complaints knowing all their past emails, messages and photographs, however irrelevant to the case, would be subjected to similar scrutiny under this policy?

"The outpouring of support from the public has given me some grounds for hope. I will not stop fighting until this policy is changed to ensure no victim ever has to choose between privacy and justice as I did." [118]

Olivia*

Olivia* reported being drugged and then attacked by a group of strangers. Despite being willing to hand over relevant information, police asked for 7 years worth of phone data, and her case was then dropped after she refused.

"The data on my phone stretches back seven years and the police want to download it and keep it on file for a century. My phone documents many of the most personal moments in my life and the thought of strangers combing through it, to try to use it against me, makes me feel like I'm being violated once again." [119]

"This isn't about trying to stop the police from putting together the facts of the case. This isn't about objecting to the police downloading information from the time that it happened. This is about objecting to the police downloading seven years of information that pre-dates the event and therefore has zero relevance." [120]

"I kept trying to ask them if the data that they took could be restricted just to the period of time of relevance to what actually happened, and they said no."

"They told me that if I didn't consent that they may just drop the case and may not proceed with it. They have now dropped the case citing one of the reasons being that I have not handed over seven years of my personal life which is of complete and utter irrelevance to that one night.

"I am willing to hand over the information that is relevant to what happened - I'm not willing to hand over seven years worth of information that is totally and utterly irrelevant." [121]

118 https://www.theguardian.com/commentisfree/2019/apr/29/sexual-assault-case-dropped-refused-police-phone-rape

119 https://www.telegraph.co.uk/news/2019/04/28/rape-victims-told-hand-mobile-phones-see-attackers-walk-free/

120 https://www.theguardian.com/society/2019/apr/29/police-face-legal-action-over-requests-for-victims-digital-records

121 https://www.lbc.co.uk/radio/presenters/eddie-mair/rape-victim-says-complaint-dropped-phone-data/

Jane*

Police demanded Jane's mobile phone and personal records after she was raped by a stranger eight years ago, even after identifying the attacker using DNA evidence. She told police she had no contact with the man other than when she was raped, but she was told that unless she gave over her mobile phone, the Crown Prosecution Service might refuse to charge.

"I literally had no idea who the suspect was and it was DNA that linked him to me.

"They asked me at one point whether I had the same mobile phone that I had at the time and I said no. Otherwise they said they would have asked for my phone and wanted my messages.

"I'm sure this is a pretty standard experience. As a victim, you are the one under suspicion. You are the one who has to prove your good character." [122]

Anonymous

A woman who reported pre-mobile phone era historic abuse had her case dropped when she would not consent to handing over her current phone.[123]

Anonymous

In a further case, the Crown Prosecution Service demanded access to the phone and 40,000 digital files on it of a 12 year old victim of rape - despite the perpetrator admitting to rape. The victim's case was delayed for months while the Crown Prosecution Service insisted on an extensive digital review of his personal mobile phone data.[124]

122 https://www.independent.co.uk/news/uk/crime/rape-victims-phones-medical-records-met-police-cps-a8949636.html

123 https://www.theguardian.com/society/2018/oct/17/data-gathering-may-deny-victims-access-to-justice

124 https://www.theguardian.com/law/2019/mar/25/cps-under-fire-for-delay-in-charging-man-accused-of-raping-boy-12

The disclosure of irrelevant data downloads to the defence further exacerbates the harm caused:

Zara*

An individual's mobile phone records, showing that Zara had called unknown numbers following the rape, were used against her to suggest that the rape was consensual. She stated that the calls were to specialist support helplines, but it was implied that the time between the rape happened and when the calls were made showed that she wasn't that deeply affected by it as she was able to make calls.[125]

Helen*

During Helen's* cross-examination, the defence went through her text messages and implied that she wasn't struggling enough and therefore the offence didn't take place. The attacker was subsequently found not guilty.[126]

Names have been changed to protect the identities of victims

125 https://www.independent.co.uk/voices/rape-trial-evidence-disclosure-cps-cases-victims-commissioner-justice-select-committee-a8482946.html

126 https://www.independent.co.uk/voices/rape-trial-evidence-disclosure-cps-cases-victims-commissioner-justice-select-committee-a8482946.html

Contribution:

Harriet Wistrich, Director of the Centre for Women's Justice.

If you report a crime to the police, such as your car being stolen, a burglary or an assault in the street, you would expect to be treated like a victim. Not told to hand over your mobile phone so officers can trawl through the data it contains, dating back several years.

But this is what victims of rape and sexual assault will be required to do as a matter of routine, under the National Police Chiefs' Council's new policy.

Most worrying, this change in the way rape cases are handled is deterring some victims from reporting being attacked. Many will choose not to proceed with investigations if they realise that their past lives will be subject to intensive scrutiny.

Of course, the disclosure of any evidence that might weaken a case against a defendant is a proper and necessary part of any criminal investigation. Indeed, the police and the Crown Prosecution Service have rightly been criticised for such failures which in some cases have led to miscarriages of justice and wrongful convictions in relation to a variety of criminal offences.

Reasonable lines of inquiry must always be permissible, but declaring open season on mining years' worth of material – be it photos, messages and a woman's online browsing history, as the new National Police Chiefs' Council policy suggests – is going too far.

It's only a matter of time before other victims come forward to share similar accounts.

This move comes at a time when the number of rape prosecutions has fallen – and when only about 2 per cent of reported rapes result in a criminal conviction.

Treating victims as you'd expect suspects of crime to be treated simply adds insult to injury.[127]

127 This account was originally published on the Daily Mail Online, 30 April 2019 (https://www.dailymail.co.uk/news/article-6970319/How-shameful-victims-violated-says-womens-justice-campaigner.html)

CONCLUSION

The police and Crown Prosecution Service's digital investigations of victims are unnecessary, likely unlawful, and an obstruction of justice.

35,000 people have signed our petition calling on the police and Crown Prosecution Service to stop demanding survivors of sexual violence's mobile phones.[128] Their voices must be heard.

A cross-party group of MPs, victims' rights organisations, human rights organisations, and senior police figures are calling on the National Police Chiefs' Council and the Crown Prosecution Service to urgently revise the current policy to protect victims from these digital strip searches.

Government must step in to ensure the National Police Chiefs' Council and the Crown Prosecution Service take immediate action.

128 https://you.38degrees.org.uk/petitions/stop-forcing-sexual-assault-survivors-to-hand-in-their-phones-in-investigations

OUR CALL FOR CHANGE:

- **Victims' consent to access their personal records should be freely given, specific and limited to the information relevant to the crime – not blanket. Victims of crime should never have to sign away their privacy rights in the pursuit of justice.**
- **The police's digital evidence technology should be brought up to date so police can collect targeted pieces of evidence from smart phones, rather than entire digital copies.**
- **Police should not be using artificial intelligence to conduct fishing expeditions through victims' phones.[129]**

129 This call has been signed by Amnesty International, Big Brother Watch, the Centre for Women's Justice, End Violence Against Women, JUSTICE, Liberty, Privacy International, Southall Black Sisters, The Survivors Trust, Vera Baird QC (Victims' Commissioner for England and Wales), Caroline Lucas MP and Jess Phillips MP

BIG BROTHER WATCH

DEFENDING CIVIL LIBERTIES, PROTECTING PRIVACY

bigbrotherwatch.org.uk - @bbw1984