BIG
BROTHER
WATCH

Police Access to Digital Evidence

The powers of the Police to examine digital devices and how forces are training staff

A Big Brother Watch Report

November 2017

Contents

Executive Summary

Police Access to Digital Evidence reveals that **93%** of UK police forces are extracting data from digital devices including mobile phones, laptops, tablets and computers which are seized as evidence from suspects, victims and witnesses.

As mobile phones and other connected devices are now ubiquitous, it should come as no surprise that such technologies can play a significant role in committing or assisting a crime. The data held on digital devices can give a detailed insight into people's lives, communications, contacts, friends, family and acquaintances. Extracting and interrogating evidence such as location data, photos, messages or internet searches can therefore be beneficial in assisting the police with criminal investigations.

Nevertheless, whilst the investigation of crime is important, ensuring that the law is comprehensive and up to date is equally important.

Based on Freedom of Information requests and research we have conducted, we are concerned that the seizure of devices and extraction of digital evidence is being undertaken using laws that were established in a pre-digital age. Rather than updating the existing laws to adequately address the complexities of new technology and data, the Government have merely amended them, creating a patchy and far from technically detailed framework.

But it is not just the laws which are complex and unclear. The details about how the police acquire, interrogate and retain data is also opaque. The majority of UK police forces failed to respond to our FOI request asking for detail on how many devices have been seized, how many have been interrogated and how many officers have been trained.

32 police forces cited that the data was not held centrally or was not easy to retrieve. Such responses are simply not acceptable and undermine the key principle of transparency which the Police's own 'Good Practice' guidance recommends.

Rethinking how our data can be used in all aspects of life, including law enforcement, is necessary if we are all to live in a just and fair connected society. If law enforcement is to continue to police in line with the Peelian principle of consent then up-to-date laws, training practices and actively working towards establishing systems for transparency are essential.

In light of this Big Brother Watch make **three recommendations**:

1. **Review of legislation**. The legislative process for extraction and interrogation of data from seized devices, in relation to a criminal act, needs urgent re-examination to ensure it is clear, concise and fit for modern policing.
2. **Police must be transparent regarding digital evidence gathering.** Police forces must adhere to good practice guidance on transparency. Records of the number of seized devices, the number of devices subject to data extraction and details regarding how long data is held for must be kept and made available for audit.
3. **Training in digital evidence gathering for all officers.** Improvements need to be made to the training of police officers in the handling, interrogation and retention of data extracted from devices. Any front-line officer whose role may involve the handling of digital evidence should be able to prove a high level of competence and understanding of the technical process and data protection.

Key Findings

- **93%** of UK police forces extract data from digital devices[1]

- **11 forces** recovered 149,203[2] devices as evidence.
    - Computer/Laptops**: 12,593**
    - Mobile Phones/Tablets: **50,468**
    - External Hard Drives/USB's: **14,575**
    - Other connected digital devices: **8507**

- **9 forces** subjected 156,595[3] devices to data extraction as part of an investigation.
    - Computer/Laptops: **36,994**
    - Mobile Phones/Tablets: **95,143**
    - External Hard Drives/USB's: **3899**
    - Other connected digital devices: **5298**

- **32 forces (71%)** refused to provide data in response to the FOI:
    - **22 forces (49%)** stated the information is not held in an "easily retrievable format".
    - **10 forces (22%)** stated that a "manual search" would be necessary to provide us with the relevant data.

[1] 42 forces confirmed; 1 refused, 2 didn't respond

[2] A number of forces didn't provide a breakdown per device type

[3] A number of forces didn't provide a breakdown per device type

Data tables

Devices recovered as evidence (2013-2016)

Force	Total
West Yorkshire Police	28,808
Norfolk Constabulary	27,870
Suffolk Constabulary	19,747
Merseyside Police	17,302
Northamptonshire Police	14,284

Number of devices they extracted data from (2013-2016)

Force	Total
Police Scotland	52,560
Metropolitan Police	46,400
Cheshire Constabulary	15,281
Kent Police	15,084
Norfolk Constabulary	7,464

Budget for digital forensics training (2013-2016)

Force	Total
Metropolitan Police	£520,000[4]
North Wales Police	£137,621
Northamptonshire Police	£73,085
City of London Police	£63,175.42
Norfolk/Suffolk Constabulary	£20,000[5]

[4] Approximately £130,000 per year

[5] Combined budget

Issue 1: The law and police good practice

The law used by the police to seize and interrogate digital devices for evidence is the Police and Criminal Evidence Act 1984 (PACE).

The two relevant clauses of PACE are:

Section 9(1) states that:

"A constable may obtain access to excluded material or special procedure material for the purposes of a criminal investigation by making an application under Schedule 1 below and in accordance with that Schedule."

Whilst Section 19(4) says:

"The constable may require any information which is stored in any electronic form and is accessible from the premises to be produced in a form in which it can be taken away and in which it is visible and legible or from which it can readily be produced in a visible and legible form if he has reasonable grounds […]"

When PACE became law in 1984 digital and connected devices, that are ever-present today, simply did not exist and property was generally non-digital. Paper documents, photographs and tape recordings will have provided some clues to an individual's personal life, but were not able to reveal a treasure trove of data relating to, not just the suspect, but their wider social network.

Today the seizure of mobile phones, laptops, computers and tablets, can expose sensitive data of innocent people who are not under suspicion. In contrast to 1984, digital evidence today contains vast quantities of data and poses challenges in regard to the complexities of a connected society.

The concept of property and evidence therefore requires a more appropriate and specific definition, to take the challenges of a digital world into account. However legislation has, so far, not caught up with these needs. Instead, PACE has merely been amended by the Government in the early 2000's by inserting the terms *"stored in an electronic form"* and that data must be *"produced in a visible and legible form"*.[6]

These amendments, we would argue, do little to acknowledge the numerous and significant complexities of modern connected devices or the vast quantities of sensitive personal data held on them.

It could be argued that data protection could be the key to creating protection for innocent people's data. The new Data Protection Bill, currently making its way through Parliament, will ensure that the police adhere to six data protection principles. In particular, the attainment of data by the police must be *"adequate, relevant and not excessive"*[7] and *"personal data be kept no longer than is necessary"*.[8]

[6] Amended by the *Criminal Justice and Police Act 2001*
[7] Clause 35, Data Protection Bill
[8] Clause 32(e), Data Protection Bill

However, when it comes to the *"prevention, detection, investigation or prosecution of criminal offences"*, the Bill allows exemptions from data protection laws in these circumstances.[9]This makes sense when it comes to addressing criminal's data, but arguably creates a grey area for the sensitive data of people who have communicated via digital means with the individual whose device was seized. Their data is also subject to be accessed, interrogated and retained unknowingly and unnecessarily.

With PACE failing to acknowledge the complexities of modern technology and data protection laws potentially allowing innocent people to fall between the cracks, it is clear that consideration needs to be given to ensure that modern policing methods are subject to specifically drafted laws. Existing square laws shouldn't be forced into modern policing round holes. Without such specific legislation there is always the chance that officers may find themselves engaging in digital evidence gathering which is far from necessary or proportionate.

The police themselves know that this is a problem and have taken measures to try and constrain potential problems associated with accessing digital evidence.

Back in 2012 the Association of Chief Police Officers (ACPO)[10] issued the *Good Practice Guide for Digital Evidence*[11] to ensure that police officers had some sort of steer to what good practice should look like.

Although the guide is now five years old it does provide a coherent approach to informing officers on how, when and why digital data should be extracted and tries to outline the complexity of the law in a meaningful way.

The emphasis on proportionality is central to the *Good Practice Guide's* policies on digital evidence. Section 4.3.1 makes clear that a device should only be seized if it is likely to hold evidence and the police have reasonable grounds to do so. Additionally, officers are warned that *"digital devices and media should not be seized just because they are there"*[12].

On the face of it, this should ensure that only strictly necessary evidence is acquired, but worryingly this doesn't appear to be the case.

According to Her Majesty's Inspectorate of Constabulary (HMIC)'s 2016 *PEEL: police effectiveness* report large numbers of devices are being seized and held, often for long periods of time, before they are examined.[13] The figures published show that:

- over 16,000 devices were awaiting examination;
- nearly 4,000 of them were considered 'high priority' devices
- 3,298 devices had been waiting for over 3 months to be investigated.

[9] Clause 42, Clause 43, Clause 46, and Clause 66, Data Protection Bill

[10] ACPO was replaced by the National Police Chiefs' Council (NPCC) in 2015.

[11] Association of Chief Police Officers, 'Good Practice Guide for Digital Evidence' (March 2012) http://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf

[12] Ibid s4.3.2

[13] HMIC: PEEL: Police effectiveness 2016 - A national overview (2016), p.56 figure 12. https://www.justiceinspectorates.gov.uk/hmicfrs/wp-content/uploads/peel-police-effectiveness-2016.pdf

HMIC's report also revealed that 40% of UK police forces need to take steps to reduce unacceptable backlogs of retrieving and examining evidence from digital devices and that *"[d]igital forensic capability and capacity is not keeping up with demand."*

We understand that the police may only have the intention to seize devices and extract data relevant to the case, but the figures raise concern that devices may be seized *"just because they are there."*[14]

Without explanation from the police as to why the figures are so large we fear, like HMIC, that digital policing is in a mess. If officers are being asked to undertake a new approach to policing, without strong laws and clear up-to-date guidance, then errors, backlogs and confusion are inevitable.

These issues must be addressed urgently. The police deserve better legislative guidance to enable them to investigate crime quickly, fairly and accurately. The public deserve to know what devices and data are seized and investigated. There is also a need for clear and coherent processes to be put in place which are accessible and understandable to the public, enabling them to question and challenge decisions if necessary.

Recommendation 1

Review of legislation. The legislative process for extraction and interrogation of data from seized devices, in relation to a criminal act, needs urgent re-examination to ensure it is clear, concise and fit for modern policing.

Issue 2: Transparency

Transparency is crucial when it comes to establishing trust between law enforcement and the wider public.

ACPO's *Good Practice Guide for Digital Evidence* demands that information about how evidence has been recovered needs to be recorded to show each process through which evidence was obtained, so it can be inspected by third parties.

Principle 3 of the guide says:

"An audit trail or other record of all processes applied to digital evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result".

However, more than half of the UK's 45 police forces were unable to even tell us:

(a) how many devices they had seized, or
(b) the number of devices they had extracted data from

The explanations we were given stated that the information wasn't centrally stored or it was not held in an easily retrievable format. This is extremely worrying and a clear breach of ACPO guidance.

[14] Ibid

This is particularly troubling when you consider that the data being accessed, interrogated and held doesn't only address the investigated criminal act, but involves communications, events and contacts of people unconnected to the crime.

Publicly available data in this area is essential and will help shed some light on a process many are currently left in the dark about. Otherwise, it is impossible to know how often these powers are used and therefore impossible to conclude whether the police are using them correctly in a fair and proportionate manner.

Digital evidence, as part of modern policing, is here to stay. The forces who failed to provide us with data must improve their internal processes, build and maintain appropriate systems and ensure they are transparent and accountable.

Recommendation 2

Police must be transparent regarding digital evidence gathering. Police forces must adhere to good practice guidance on transparency. Records of the number of seized devices, the number of devices subject to data extraction and details regarding how long data is held for must be kept and made available for audit.

Issue 3: Training and third parties

Digital policing is the future. The training of police officers on how to undertake digital evidence gathering should be a standard process for all new recruits and existing officers.

If the police are going to utilise extraction technology, it is imperative this process is not in the hands of the untrained and the inexperienced. Many officers working in the police today were trained before digital evidence became a high priority and find handling new technologies challenging. For example, a report revealed an anonymous officer admitted to feeling *"frustrated with their lack of ability to deal with digital investigations"*[15] – this cannot continue.

The emphasis on dealing with challenges to digital policing through training was clearly referenced in HMIC's assessment. It acknowledged that police forces were being *"overwhelmed"*[16] by digital evidence and that this was due to some forces being unable to get the basics of digital crime-fighting right.

Furthermore, the assessment stressed the importance of getting forces up to speed since *"[d]igital forensics is one of the fastest-growing areas of business."*[17] The report stated that *"[f]orces urgently need to recruit and train a workforce that is fit for a digital future."*[18]

We agree with this assessment and emphasise the importance of a police force to be as well-equipped as possible when it comes to dealing with digital evidence.

[15] HMIC 'Real Lives, Real Crimes' December 2015 https://www.justiceinspectorates.gov.uk/hmicfrs/wp-content/uploads/real-lives-real-crimes-a-study-of-digital-crime-and-policing.pdf

[16] HMIC State of Policing: The Annual Assessment of Policing in England and Wales 2016 http://www.justiceinspectorates.gov.uk/hmicfrs/wp-content/uploads/state-of-policing-2016.pdf

[17] P.57

[18] Ibid

We asked all police forces to provide us with figures relating to the number of staff trained for digital forensics and the budget that they dedicate for this training.

Yet again the majority of forces failed to provide us with any data on this. However, what we can glean from the 14 responses we received shows a patchy picture of training and inconsistencies in training budgets.

The data shows that, between 2013 and 2016 seven forces were spending anywhere between £20,000 and £520,000 on training officers to carry out data extraction and forensic analysis. Whilst disparity in budgets due to the size of each force is expected, this must not be used as cover for allowing smaller forces to get left behind.

In terms of the number of officers trained since 2013, not enough data has been made available to produce a nationwide picture – but individual figures sent to us do portray a push towards increased training.

Norfolk and Suffolk Constabularies have nearly doubled the number of officers trained in data extraction from 59 officers in 2015 to 109 officers in 2016.

Similarly, West Mercia Constabulary trained more officers in data extraction in 2016 than they did in the previous three years combined. They now have 68 officers trained in this area of modern policing.

Derbyshire Constabulary deserve full recognition for training all frontline staff in forensic examination of devices and/or the data contained on them. This is a significant achievement and one we champion. Comments made by Chief Constable Peter Goodman of Derbyshire constabulary in November 2017, at the Association of Police and Crime Commissioners (APCC) and National Police Chiefs' Council (NPCC) joint summit, showed that the force understand the enormity of digital crime. Chief Constable Goodman was quoted as saying that digital crime was now the *"biggest single crime category"* faced by police. It is clear that this realisation of the extent of the problem has led the force to ensure that staff are well equipped to handle digital evidence.

However, this approach is in marked contrast to City of London Police who told us they have only trained 8 officers in the process of digital forensic examination between 2013 and 2016 and that only a total of 16 officers are trained to carry out digital data extraction or digital forensic examination. This is of particular concern as this force are focussed on investigating fraud and economic crime; two forms of crime which are not only rising year on year, but are predominantly taking place online and therefore involve digital evidence. That so few officers within the force are trained in digital extraction is a genuine surprise and one we are keen to understand.

Obviously if 93% of forces are engaged in digital extraction but so few officers are being trained, logic would imply that third party services are being used.

To get a measure of this we asked forces if they had used a third party organisation or service to carry out digital forensics. Six police forces confirmed to us that they used third party services between 2013 and 2016 to carry out digital forensics.

The Metropolitan Police told us that they have spent £8,698,000 over the past four years on engaging third-party services to carry out digital forensics. 10 different services[19] were used on at least 15,600 separate occasions. It is important to note that the Metropolitan Police often has to handle digital evidence sent to them from other forces on top of their own load.[20]

Nevertheless, outsourcing law enforcement makes the police less accountable to the public and makes scrutiny of procedures more opaque. Furthermore, adding yet another organisation into the mix of policing creates complexity for citizens if they need to raise a query or make a complaint; blurring the process of accountability.

This is clearly a complex area and a one size fits all solution is not necessarily the answer. What is evident is that training and funding are patchy, causing the police to be overwhelmed. Outsourcing might seem logical, but it will only take one giant data breach, hack or cyberattack for this practice to be put under scrutiny.

As we have stressed throughout the report, digital evidence is a key part of policing in a connected society. We feel that all police officers should be trained to handle devices and data. Outsourcing a fundamental part of law enforcement to private third parties therefore seems far from appropriate.

Recommendation 3
Training in digital evidence gathering for all officers. Improvements need to be made to the training of police officers in the handling, interrogation and retention of data extracted from devices. Any frontline officer whose role may involve the handling of digital evidence should be able to prove a high level of competence and understanding of the technical process and data protection.

Conclusion

Nowadays, there are very few crimes where digital evidence is not an essential part of the investigation. This report, however, highlights a worrying lack of transparency, regulatory guidance and accountability of the police.

Digital devices need to be analysed and the data they hold may be extremely useful evidence. This is common sense, but the current system of operation is lacking specific, technical and data protection laws, hindering the police's ability to guarantee proportionality and the public's understanding of what digital evidence gathering entails.

Many of us will be apathetic: 'I'm not a criminal and don't intend on committing any crimes, so why should I care?' – but these powers represent a further slow-creep of surveillance powers, which were initially introduced at the borders to fight terrorism, but are now being used for everyday arrests. It is not just criminals whose personal data will be accessed; their friends, family, colleagues and acquaintances will be caught in the net too.

[19] CCL Forensics, FTS, FMS, Sector Forensics, MD5, Zentek, IntaForensics, LGC, Control Risks, QCC Information Security
[20] MPS – Digital, Cyber and Communications Forensics Unit – Information for Prospective Bidders (June 2015), p. 15.

More needs to be done to research the effectiveness of modern investigative approaches. More must be spent on the ongoing training of officers to ensure that the ‘skills gap’ is kept to a minimum, and that officers are prepared to deal with new evolving technologies.

New guidance and legislation is increasingly required to bring the law into the 21st century. Legislation should limit the extraction of data to only which is strictly necessary for the investigation and should give digital devices extra protections. The indiscriminate extraction of masses of digital data must come to an end, for the benefit of the public and the efficiency of the police.

Complex laws, poor training and the constant advances of technology are a ripe concoction for confusion, for the public and the police. For everyone’s sake the situation needs to change.

A modern technological world should be matched with an equally modern police force, guided by modern legislation.

Appendix 1: Regional police force breakdown

	Is data being extracted from devices seized?
Avon and Somerset Constabulary	Yes
Bedfordshire Police	Yes
Cambridgeshire Constabulary	Yes
Cheshire Constabulary	Yes
City of London Police	Yes
Cleveland Police	Yes
Cumbria Constabulary	Yes
Derbyshire Constabulary	Yes
Devon and Cornwall Police	Yes
Dorset Police	Yes
Durham Police	Yes
Dyfed Powys Police	Yes
Essex Police	Refused[21]
Gloucestershire Constabulary	Yes
Greater Manchester Police	Yes
Gwent Constabulary	Yes
Hampshire Constabulary	Yes
Hertfordshire Constabulary	Yes
Humberside Police	Yes
Kent Police	Yes
Lancashire Constabulary	Yes
Leicestershire Constabulary	Yes
Lincolnshire Police	Yes

[21] Refused based on Section 23(5) – Information supplied by, or concerning, certain security bodies; Section 24(2) National security; Section 30(3) Investigations and proceedings conducted by public authorities; Section 31 (3) Law enforcement.

Merseyside Police	Yes
Metropolitan Police	Yes
Norfolk Constabulary	Yes
North Wales Police	Yes
North Yorkshire Police	Yes
Northamptonshire Police	Yes
Northumbria Police	Yes
Nottinghamshire Police	Yes
Police Service of Northern Ireland	Yes
Police Scotland	Yes
South Wales Police	Yes
South Yorkshire Police	Yes
Staffordshire Police	Yes
Suffolk Constabulary	Yes
Surrey Police	Yes
Sussex Police	No response
Thames Valley Police	Yes
Warwickshire Police	Yes
West Mercia Constabulary	Yes
West Midlands Police	Yes
West Yorkshire Police	No response
Wiltshire Constabulary	Yes

Devices seized as evidence

	Device	2013	2014	2015	2016
Avon and Somerset Constabulary	Refused –cost and time				
Bedfordshire Police	Refused – cost and time				
Cambridgeshire Constabulary	Data not recorded				
Cheshire Constabulary	Refused – cost and time				
City of London Police	Computers	20	73	203	55
	Laptops	67	207	104	109
	Mobile Phones	908	1039	1123	1005
	Tablets	25	27	35	32
	External Hard Drives and USB's	46	203	135	115
	Other connected devices	-	-	-	-
	Total	**1066**	**1549**	**1600**	**1316**
Cleveland Police	Refused – cost and time				
Cumbria Constabulary	Refused – cost and time				
Derbyshire Constabulary	Computers/Laptops	593	573	496	635
	Mobile Phones/Tablets	630	619	746	680
	External Hard Drives and USB's	122	25	113	141
	Other connected devices	89	21	65	56
	Total	**1434**	**1238**	**1420**	**1512**
Devon and Cornwall Police	Refused – cost and time				
Dorset Police	Refused – cost and time				

Durham Police[22]	Computers	-	-	-	37
	Laptops	-	-	-	66
	Mobile Phones	-	-	-	179
	Tablets	-	-	-	43
	External Hard Drives and USB's	-	-	-	209
	Other connected devices	-	-	-	unknown
	Total	**-**	**-**	**-**	**534**
Dyfed Powys Police	Computers/Laptops/other devices that amount to a hard drive	407	557	544	280
	Laptops	-	-	-	-
	Mobile Phones/Tablets	1216	1490	1505	1179
	Tablets	-	-	-	-
	External Hard Drives and USB's	362	257	427	361
	Other connected devices	-	-	-	-
	Total	**1985**	**2304**	**2476**	**1883**
Essex Police	Refused – cost and time				
Gloucestershire Constabulary	No response				
Greater Manchester Police	Refused – cost and time				
Gwent Constabulary	Computers	8	16	173	221
	Laptops	13	46	281	347
	Mobile Phones	-	-	-	-
	Tablets	2	37	202	195
	External Hard Drives and	3	41	319	430

[22] The numbers reflect the period between September and December 2016

	USB’s				
	Other connected devices	37	155	769	1164
	Total	**63**	**295**	**1744**	**2357**
Hampshire Constabulary	Refused – cost and time				
Hertfordshire Constabulary	Refused – cost and time				
Humberside Police	Refused – cost and time				
Kent Police	Refused – cost and time				
Lancashire Constabulary	Refused – cost and time				
Leicestershire Constabulary	Refused – cost and time				
Lincolnshire Police	Computers	-			
	Laptops	-			
	Mobile Phones	-			
	Tablets	-			
	External Hard Drives and USB’s	--			
	Other connected devices	-			
	Total	**9350**			
Merseyside Police	Computers	-	-	-	-
	Laptops	-	-	-	-
	Mobile Phones	-	-	-	-
	Tablets	-	-	-	-
	External Hard Drives and USB’s	-	-	-	-
	Other connected devices	-	-	-	-

	Total	**1602**[23]	**5231**	**5300**	**5169**
Metropolitan Police	Refused – cost and time				
Norfolk Constabulary	Computers	183	192	170	210
	Laptops	575	797	694	721
	Mobile Phones	4146	4781	4142	4251
	Tablets	140	265	359	358
	External Hard Drives and USB’s	1025	1631	1621	1609
	Other connected devices	-	-	-	-
	Total	**6069**	**7666**	**6986**	**7149**
North Wales Police	Refused – cost and time				
North Yorkshire Police	Refused – cost and time				
Northamptonshire Police	Computers	5	126	175	93
	Laptops	4	162	264	171
	Mobile Phones	58	1495	1893	1665
	Tablets	3	78	199	194
	External Hard Drives and USB’s	20	357	639	532
	Other connected devices	3	1800	2283	2065
	Total	**93**	**4018**	**5453**	**4720**
Northumbria Police	Refused – cost and time				
Nottinghamshire Police	Refused – cost and time				
Police Service of Northern Ireland	Refused – cost and time				
Police Scotland	Refused – cost and time				

[23] Half year figures only, as records not kept until July 2013

South Wales Police	Refused – cost and time				
South Yorkshire Police	Refused – cost and time				
Staffordshire Police	Refused – cost and time				
Suffolk Constabulary	Computers	97	145	121	113
	Laptops	345	419	391	329
	Mobile Phones	3176	3360	3183	3045
	Tablets	143	255	290	284
	External Hard Drives and USB's	533	951	1343	1214
	Other connected devices	-	-	-	-
	Total	**4304**	**5130**	**5328**	**4985**
Surrey Police	No response				
Sussex Police	No response				
Thames Valley Police	Refused – cost and time				
Warwickshire Police	Refused – cost and time				
West Mercia Constabulary	Refused – cost and time				
West Midlands Police	Refused – cost and time				
West Yorkshire Police	Refused – cost and time				
Wiltshire Constabulary	Refused – cost and time				

Number of devices data has been extracted from

	Device	**2013**	**2014**	**2015**	**2016**
Avon and Somerset Constabulary	Refused – cost and time				
Bedfordshire Police	Refused – cost and time				

Cambridgeshire Constabulary	Computers	130	187	214	-
	Laptops	-	-	-	-
	Mobile Phones	977	972	1012	-
	Tablets	-	-	-	-
	External Hard Drives and USB's	-	-	-	-
	Other connected devices	-	-	-	-
	Total	**1107**	**1159**	**1226**	-
Cheshire Constabulary	Refused – cost and time				
City of London Police	Refused – cost and time				
Cleveland Police	Refused – cost and time				
Cumbria Constabulary	Refused – cost and time				
Derbyshire Constabulary	Computers/Laptops	593	573	496	635
	Mobile Phones/Tablets	630	619	746	680
	External Hard Drives and USB's	122	25	113	141
	Other connected devices	89	21	65	56
	Total	**1434**	**1238**	**1420**	**1512**
Devon and Cornwall Police	Refused – cost and time				
Dorset Police	Refused – cost and time				
Durham Police	Refused – cost and time				
Dyfed Powys Police	No information held				
Essex Police	Refused – cost and time				
Gloucestershire Constabulary	No response				
Greater Manchester Police	Refused – cost and time				

Gwent Constabulary	Details before 2017 not kept				
Hampshire Constabulary	Refused – cost and time				
Hertfordshire Constabulary	Refused – cost and time				
Humberside Police	Refused – cost and time				
Kent Police	Computers	360	323	249	244
	Laptops	633	669	572	492
	Mobile Phones	1077	1069	1033	595
	Tablets	165	284	315	212
	External Hard Drives and USB's	680	571	548	320
	Other connected devices	1587	1276	1079	731
	Total	**4502**	**4192**	**3796**	**2594**
Lancashire Constabulary	Refused – cost and time				
Leicestershire Constabulary	Refused – cost and time				
Lincolnshire Police	Refused – cost and time				
Merseyside Police	Refused – cost and time				
Metropolitan Police	Computers	-	-	6400	-
	Laptops	-	-	-	-
	Mobile Phones	-	-	40000	-
	Tablets	-	-	-	-
	External Hard Drives and USB's	-	-	-	-
	Other connected devices	-	-	-	-
	Total	-	-	**46400**	-
Norfolk	Computers/Laptops	-	-	2067	2806

Constabulary	Laptops	-	-	-	-
	Mobile Phones/Tablets	-	-	1098	1493
	Tablets	-	-	-	-
	External Hard Drives and USB’s	-	-	-	-
	Other connected devices	-	-	-	-
	Total	**-**	**-**	**3165**	**4299**
North Wales Police	Refused – cost and time				
North Yorkshire Police	Refused – cost and time				
Northamptonshire Police	Refused – cost and time				
Northumbria Police	Refused – cost and time				
Nottinghamshire Police	Refused – cost and time				
Police Service of Northern Ireland	Refused – cost and time				
Police Scotland	Computers/laptops/external hard drives/USBs	-	6,524	5,011	5,052
	Mobile Phones/Tablets/Satellite Navigation	-	10,411	11,295	14,267
	Other connected devices	-	-	-	-
	Total	**-**	**16,935**	**16,306**	**19,319**
South Wales Police	Refused – cost and time				
South Yorkshire Police	Refused – cost and time				
Staffordshire Police	Refused – cost and time				
Suffolk Constabulary	Computers	-	-	2067	2806
	Laptops	-	-	-	-

	Mobile Phones	-	-	1098	1493
	Tablets	-	-	-	-
	External Hard Drives and USB’s	-	-	-	-
	Other connected devices	-	-	-	-
	Total			**3,165**	**4,299**
Surrey Police	No response				
Sussex Police	No response				
Thames Valley Police	Refused – cost and time				
Warwickshire Police	Refused – cost and time				
West Mercia Constabulary	Refused – cost and time				
West Midlands Police	Computers/laptops/external hard drives/storage media	-	-	-	1569
	Mobile Phones/Tablets/memory cards	-	-	-	2445
	Other connected devices	-	-	-	-
	Total				**4014**
West Yorkshire Police	Refused – cost and time				
Wiltshire Constabulary	Computers/laptops	290	299	243	363
	Mobile Phones/tablets	1132	1186	705	725
	External Hard Drives and USB’s	389	277	389	324
	Other connected devices	72	64	115	143
	Total	**1,883**	**1,826**	**1,452**	**1,555**

Number of officers/other police staff trained in data extraction and/or digital forensic examination

	Officers trained in	2013	2014	2015	2016
Avon and Somerset Constabulary	Refused – cost and time				
Bedfordshire Police	Refused – cost and time				
Cambridgeshire Constabulary	Refused – cost and time				
Cheshire Constabulary	Refused – cost and time				
City of London Police	Officers trained in data extraction	8			
	Officers trained in digital forensic examination	8			
Cleveland Police	Refused – cost and time				
Cumbria Constabulary	Refused – cost and time				
Derbyshire Constabulary	Officers trained in data extraction	260			
	Officers trained in digital forensic examination	2350			
Devon and Cornwall Police	Refused – cost and time				
Dorset Police	Refused – cost and time				
Durham Police	Officers trained in data extraction	108			
	Officers trained in digital forensic examination	8			
Dyfed Powys Police	Officers trained in data extraction	1	1	2	4
	Officers trained in digital forensic examination				
Essex Police	Refused – cost and time				
Gloucestershire Constabulary	No response				

Greater Manchester Police	Refused – cost and time				
Gwent Constabulary	Officers trained in data extraction	7	7	6	42
	Officers trained in digital forensic examination				
Hampshire Constabulary	Refused – cost exceeds the appropriate level				
Hertfordshire Constabulary	Refused – cost and time				
Humberside Police	Refused – cost and time				
Kent Police	Officers trained in data extraction	42	40	35	84
	Officers trained in digital forensic examination				
Lancashire Constabulary	Refused – cost and time				
Leicestershire Constabulary	Refused – cost and time				
Lincolnshire Police	Refused – cost and time				
Merseyside Police	Refused – cost and time				
Metropolitan Police	Officers trained in data extraction	1500			
	Officers trained in forensic examination	Approx. 50			
Norfolk Constabulary	Officers trained in data extraction	-	-	59	109
	Officers trained in forensic examination	-	-	9	9
North Wales Police	Refused – cost and time				
North Yorkshire Police	Refused – cost and time				
Northamptonshire Police	Refused – cost and time				

Northumbria Police	Refused – cost and time				
Nottinghamshire Police	Refused – cost and time				
Police Service of Northern Ireland	Refused – cost and time				
Police Scotland	Officers trained in data extraction	23	27	35	39
	Officers trained in forensic examination	23	27	35	39
South Wales Police	Refused – cost and time				
South Yorkshire Police	Refused – cost and time				
Staffordshire Police	Refused – cost and time				
Suffolk Constabulary	Officers trained in data extraction	See Norfolk			
	Officers trained in forensic examination				
Surrey Police	No response				
Sussex Police	No response				
Thames Valley Police	Refused – cost and time				
Warwickshire Police	Officers trained in data extraction	6	5	10	23
	Officers trained in forensic examination	-	-	-	-
West Mercia Constabulary	Officers trained in data extraction	11	16	15	68
	Officers trained in forensic examination	-	-	-	-
West Midlands Police	Officers trained in data extraction	30			
	Officers trained in forensic examination				

West Yorkshire Police	Refused – cost and time	
Wiltshire Constabulary	Officers trained in data extraction	119
	Officers trained in forensic examination	

Total training budget

	2013	2014	2015	2016
Avon and Somerset Constabulary	Refused – cost and time			
Bedfordshire Police	Refused – cost and time			
Cambridgeshire Constabulary	Refused – cost and time			
Cheshire Constabulary	Refused – cost and time			
City of London Police[24]	£16,431.38	£15,408.76	£12,015.00	£19,320
Cleveland Police	Refused – cost and time			
Cumbria Constabulary	Refused – cost and time			
Derbyshire Constabulary	Information not held			
Devon and Cornwall Police	Refused – cost and time			
Dorset Police	Refused – cost and time			
Durham Police	£4,377	£6,600	£21,062	£16,933
Dyfed Powys Police	No information held			
Essex Police	Refused – cost and time			
Gloucestershire Constabulary	No response			
Greater Manchester Police	Refused – cost and time			
Gwent Constabulary	Refused – cost and time			
Hampshire Constabulary	Refused – cost exceeds the ‘appropriate level’			

[24] Numbers are for the financial years 2012/2013, 2013/2014, 2014/2015 and 2015/2016

Hertfordshire Constabulary	Refused – cost and time			
Humberside Police	Refused – cost and time			
Kent Police	Refused – cost and time			
Lancashire Constabulary	Refused – cost and time			
Leicestershire Constabulary	Refused – cost and time			
Lincolnshire Police	Refused – cost and time			
Merseyside Police	Refused – cost and time			
Metropolitan Police	Approx. £130,000	Approx. £130,000	Approx. £130,000	Approx. £130,000
Norfolk Constabulary	-	-	Approx. £10,000	Approx. £10,000
North Wales Police[25]	£23,793	£46,770	£67,058	£47,060
North Yorkshire Police	Refused – cost and time			
Northamptonshire Police[26]	-	£17,612.00	£55,473.00	£39,523.00
Northumbria Police	Refused – cost and time			
Nottinghamshire Police	Refused – cost and time			
Police Service of Northern Ireland	Refused – cost and time			
Police Scotland	Refused – cost and time			
South Wales Police	Refused – cost and time			
South Yorkshire Police	Refused – cost and time			
Staffordshire Police	Refused – cost and time			
Suffolk Constabulary	See Norfolk Constabulary			
Surrey Police	No response			
Sussex Police	No response			

[25] Numbers are for the financial years 2013/2014, 2014/2015, 2015/2016, 2016/2017.

[26] Numbers are for the financial years 2014/2015, 2015/2016, 2016/2017.

Thames Valley Police	Refused – cost and time
Warwickshire Police	Refused – cost and time
West Mercia Constabulary	Refused – cost and time
West Midlands Police	Not stated
West Yorkshire Police	Refused – cost and time
Wiltshire Constabulary	Refused – cost and time

Appendix 2: Methodology

Beginning on the 31st May, we sent a Freedom of Information request to all UK police forces.

We asked each force for details on how many digital devices were seized, how many had data extracted from them and how many were subject to further forensic examination. We also requested information on how many officers had been trained to do this and comparative figures for other forms of specialist training. Finally we requested budgetary information for digital forensic training and for other types of specialist training.

We received responses from 42 police forces, equivalent to 93%. For the purposes of this report only responses received by 22nd September 2017 have been included.

On the 26th July a follow-up Freedom of Information request was sent to all 45 police forces.
Simply this requested whether their police force had extracted data from any device seized as evidence.

We received responses from 42 police forces, equivalent to 93%. For the purposes of this report only responses received by 22nd September 2017 have been included.

Appendix 3: Freedom of Information Requests

FOI 1

Dear Sir or Madam,

I am writing under the Freedom of Information Act 2000 to request information about your force's capacity to deal with digital evidence, specifically I am asking the following:

1. How many of the following have been recovered as evidence by your force each year in the period 2013-2016:
    a. Computers.
    b. Laptops.
    c. Mobile Phones.
    d. Tablets.
    e. External hard drives and USBs.
    f. Other connected and digital devices.

2. How many of the devices referred to in question 1 have been subject to data extraction as part of an investigation for each year in the period 2013-2016?

3. How many officers/other police staff have received training to carry out data extraction from the devices referred to in question 1 for each year in the period 2013-2016?

4. How many devices and/or data obtained from a device have been subject to further digital forensic examination for each year in the period 2013-2016?

5. How many officers/other police staff have received training to carry out this forensic examination on digital devices for each year in the period 2013-2016?

6. Please provide a breakdown of the number of officers/police staff who have received specialist training in fields other than digital evidence for each year in the period 2013-2016.

7. Please provide the total number of officers/police staff who have, at any time, received training to carry out data extraction and/or digital forensic examination

8. Please provide the total training budget available for all forms of specialist training. Please provide a breakdown of how this budget is allocated per field, for each year in the period 2013-2016.

9. Please provide the amount of money that has been spent on training officers/police staff to undertake and conduct digital forensic examination for each year in the period 2013-2016.

10. Has your force ever used a third-party organisation/service to carry out digital forensics? If so:

a. Which third-party organisation/service did you use?
b. On how many separate occasions have you used them during the period 2013-2016?
c. How much was spent by your force on these services during the period 2013-2016?

I understand under the Freedom of Information Act that I am entitled to a response within twenty working days. I would be grateful if you could confirm this request in writing as soon as possible.

FOI 2

Dear Sir or Madam,

I am writing under the Freedom of Information Act 2000 to request information about your force's treatment of digital devices. This is a short follow-up request to one sent by my colleague Ben Snaith in May. Specifically I am asking the following as a yes/no question:

1. Since 2013, have your force extracted data from digital devices that have been seized as evidence?

I understand under the Freedom of Information Act that I am entitled to a response within twenty working days. I would be grateful if you could confirm this request in writing as soon as possible.

About Big Brother Watch

Big Brother Watch work to ensure that those who fail to respect our privacy, undermine our online security, or fail to protect our personal data, are held to account.

We campaign on behalf of the individual to ensure your privacy and civil liberties are maintained in the digital age by government, public authorities and businesses.

Founded in 2009, Big Brother Watch produces unique research exposing the misuse of powers, informative factsheets explaining complex laws, and briefings for parliament, the press and the public.

If you are a journalist and would like to contact Big Brother Watch please call +44 (0) 7505 448925 (24hrs).

Postal address:
Big Brother Watch
55 Tufton Street
London SW1P 3QL

Website:
www.bigbrotherwatch.org.uk

Email: info@bigbrotherwatch.org.uk