LEGAL AND POLICY FRAMEWORK FOR DIGITAL FORENSICS: A RESOURCE FOR PRACTITIONERS

A Policy and Practice Briefing from the Digital Forensics and Social Media project funded by the Dawes Trust

Authored by:
Dr Janice Goldstraw-White

September 2022

UCL
perpetuity research
Birkbeck UNIVERSITY OF LONDON
ICPR Institute for Crime & Justice Policy Research

Copyright

Acknowledgements

This paper forms part of a larger project on Digital Forensics and Social Media (DFSM) made possible by the generous support of the Dawes Trust, to whom we are extremely grateful.

I would particularly like to thank my colleagues on the project team, Professor Martin Gill, Professor Jessica Jacobson, Professor Ben Bradford, Tiggey May, Dr Kari Davies, and Owen Wilkie for their support and feedback. In addition, I would like to extend my gratitude to those who made comments on earlier versions of this paper, whose feedback and insights were invaluable. In particular, I would like to thank Sara Fotheringham, David Johnson, Danni Driscoll, Temitayo Afolabi, Laura Tams, Eleanor Farrow, Tamzin Jeffs and Lee White.

The views expressed in this paper are solely those of the author.

Background

Compared to traditional forms of evidence, the use of digital evidence in courts of law is a relatively new phenomenon. As such, it presents a number of challenges to existing legal procedures that were developed and framed for more traditional evidence types.[1] These key challenges relate not only to identifying and accessing potential evidential data (which, compared to more traditional evidence may stretch over many jurisdictions)[2], but also in analysing and presenting these data in useable and acceptable formats in court.[3] The volume of these data, the range of formats and the number of different devices data are stored or accessed on, add further complications. One recent estimate suggested that, if printed out, the average iPhone will produce five million pages.[4] It is of course essential that the legal framework governing the use of digital evidence in criminal cases keeps pace with digital developments and is generally fit-for-purpose.

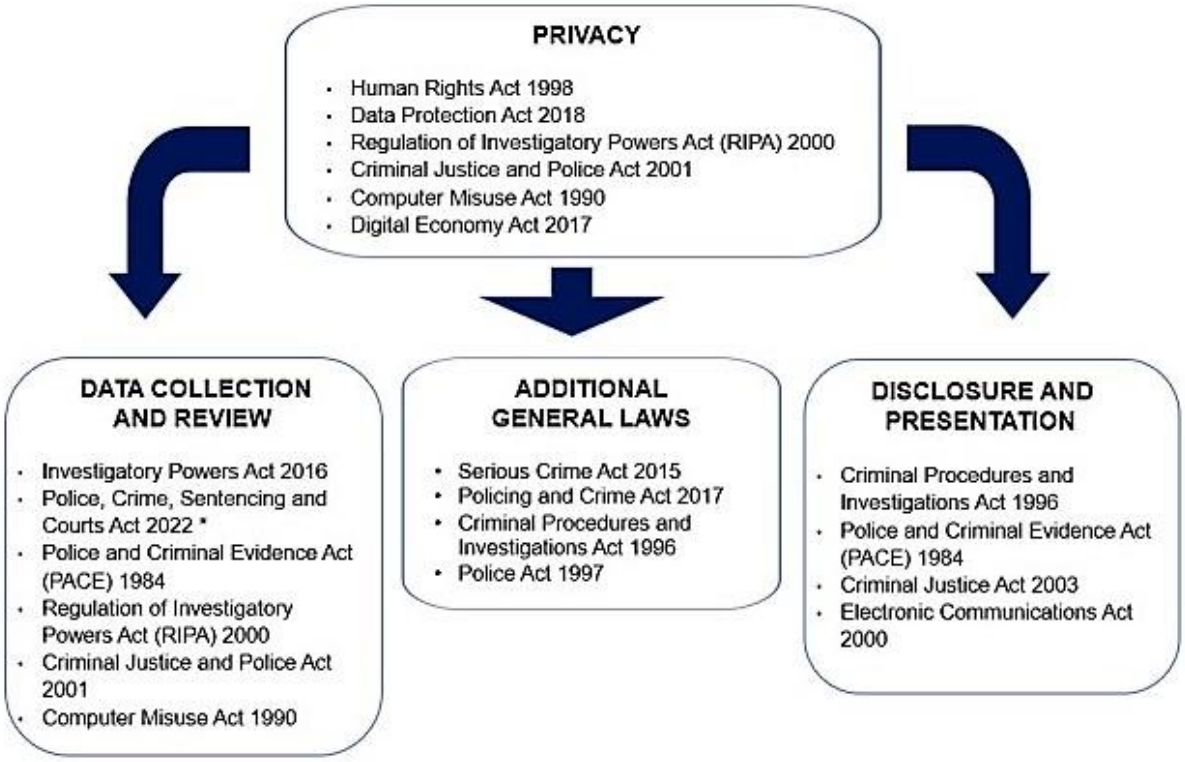
There are currently at least 15 Acts of Parliament that need to be considered if social media data are used as evidence in court for cases involving murder or serious assault (see Figure 1). It is split over two main themes – first, the collection and review of potential evidence, and second, the subsequent disclosure and presentation of this. Privacy was regarded as a theme that runs throughout all these processes. Whereas many of these laws (in whole or part), are specific to using digital evidence to investigate crime, other laws are more generic in nature and need to be interpreted for this type of evidence. The Police, Crime, Sentencing and Courts Act was given Royal Assent in April 2022 and in Sections 37 to 44 includes details for the extraction of information from electronic devices. At the time of publication of this paper, this part of the act has not been brought into force.

The overall legal framework applies to all investigatory processes from initially identifying, accessing, seizing, and extracting social media data, through to preserving, storing, transferring, examining, and analysing it, before formal presentation of the evidence in a court of law.[5] In addition to these procedures, there are other general laws that protect individuals (for example those relating to privacy[6] and general human rights) that must be taken into consideration by investigators.

Many of these laws have been in existence for a number of years when the use of traditional evidence types was the norm, therefore, they have had to be updated for evidence presented in a digital format. A review of these laws suggests that they have been updated in the last few decades in two main stages. Firstly, during the 1980s to ensure that any data from computers submitted as evidence is covered, and secondly, from the 1990s to include the admissibility of data derived from the Internet. For the latter stage, when these laws were updated, generic wording for the types of data have been used, such as ‘digital’ and ‘electronic’ which are broad enough to encompass data that are extracted from social media. As such, no Acts of Parliament have been changed specifically for the inclusion of social media data.

Under these statues there is a supporting layer of legislation detailed as statutory instruments, orders, as well as government policy and associated guidance. In addition, professions working with digital evidence may have their own professional standards and guidance. The Attorney General[7] and CPS[8] have both produced guidelines and manuals on disclosure procedures.

Figure 1 – Handling digital evidence and the relevant acts of parliament



* Digital evidence section of Act not brought into force yet

The Forensic Science Regulator (FSR) is responsible for the quality of digital forensic services in the UK criminal justice system, and The FSR's Codes of Practice and Conduct[9] govern both those involved in analysing data and acting as expert witnesses.[10] All forensic laboratories working for the criminal justice system need to be accredited to ISO/IEC 17025,[11] which specifies the general requirements for competence, impartiality and consistent operation of these establishments. This standard was last updated in 2017 and does not specifically mention digital or social media data.

For the police, ACPO (now superseded by NPCC) has produced a good practice guide for digital evidence,[12] the latest version of which was issued in March 2012. This guidance details four main short principles (relating to preserving the original data; competency; keeping an audit trail of processes applied to digital evidence; and management of the process) to be followed by practitioners. Whereas these principles are still applicable, it is argued that given the pace of change in both technology and the field of digital forensics, the principles need reviewing and possibly updating because they are vague, missing emerging themes in digital evidence and have stagnated.[13]

How to use this guide

This document contains a number of resources which practitioners may find useful when working with digital evidence.

The Acts of Parliament detailed in Figure 1 have been mapped over the five themes of the digital evidence project, these being – data extraction; data review; disclosure; presentation; and privacy, to produce a digital evidence legal framework (see Appendix A). In Appendices B(i) to B(v) this is further broken down over the themes detailing the relevant part of the acts relating to digital evidence.

A list of prominent and useful cases are detailed in Appendix C.

Policies, procedures and guidance relating to the use of digital evidence are mapped similarly to the main five themes and can be seen in Appendix D. In Appendices E(i) to E(v) these are further broken down over the main themes detailing the relevant parts of documents relating to digital evidence.

Academic and more general literature articles are mapped similarly to the main five themes and can be seen in Appendix F. In Appendices G(i) to G(v) either a summary or abstract of these articles is detailed over the relevant themes.

More general information and references beyond the five themes used for the project can be found in Appendix H, and include areas such as policing digital evidence, process models, and judges understanding of digital evidence.

Appendix A

Legal Framework For Digital Forensics

Data Extraction	Data Review	Disclosure	Presentation	Privacy
• Investigatory Powers Act 2016 • Police, Crime, Sentencing and Courts Act 2022 (only part in force) • Police Act 1997 • Police and Criminal Evidence Act (PACE) 1984 • Policing and Crime Act 2017 • Regulation of Investigatory Powers Act (RIPA) 2000 • Data Protection Act 2018 • Criminal Procedures and Investigations Act 1996 • Criminal Justice and Police Act 2001 • Human Rights Act 1998 • Computer Misuse Act 1990 • Serious Crime Act 2015	• Computer Misuse Act 1990 • Regulation of Investigatory Powers Act (RIPA) 2000 • Police and Criminal Evidence Act (PACE) 1984 • Data Protection Act 2018 • Electronic Communications Act 2000 • Criminal Justice and Police Act 2001 • Investigatory Powers Act 2016	• Criminal Procedures and Investigations Act 1996 • Data Protection Act 2018	• Police and Criminal Evidence Act (PACE) 1984 • Criminal Justice Act 2003 • Electronic Communications Act 2000 • Criminal Procedures and Investigations Act 1996 • Data Protection Act 2018	• Regulation of Investigatory Powers Act (RIPA) 2000 • Data Protection Act 2018 • Criminal Procedures and Investigations Act 1996 • Criminal Justice and Police Act 2001 • Human Rights Act 1998 • Electronic Communications Act 2000 • Computer Misuse Act 1990 • Digital Economy Act 2017

Appendix B(i)

Legal Framework – Data Extraction

ACT	NARRATIVE
Investigatory Powers Act 2016	This Act brings together all of the powers already available to law enforcement and the security and intelligence agencies to obtain communications and data about communications. The Act provides an updated framework for the use of investigatory powers to obtain communications and communications data. These powers cover the interception of communications, the retention and acquisition of communications data, and equipment interference for obtaining communications and other data. It is not lawful to exercise such powers other than as provided for by the Act. It provides consistent statutory safeguards and clarifies which powers different public authorities can use and for what purposes. It sets out the statutory tests that must be met before a power may be used and the authorisation regime for each investigative tool, including a new requirement for Judicial Commissioners to approve the issuing of warrants for the most sensitive and intrusive powers.
Police, Crime, Sentencing and Courts Act 2022 (currently not in force)	Sections 37 to 44 detail requirements to be followed when an authorised person requires to extract information from an electronic device. This can be for the prevention, detection, investigation or prosecution of crime; helping to locate a missing person; or protecting a child or at-risk adult from neglect or harm. It provides that an authorised person may extract information stored on an electronic device providing that: 1. the device has been provided voluntarily by a user of the device 2. the user has given their agreement for information stored on the device to be extracted 3. an authorised person must reasonably believe that information stored on an electronic device is relevant to a reasonable line of enquiry. That Act makes it clear that 'crime' means conduct which amounts to a criminal offence in a part of the UK or conduct which, had it taken place in a part of the UK, would have amounted to an offence there. This allows the power to be exercised further to the receipt of mutual legal assistance requests from overseas (provided the conduct in question would have constituted an offence in the UK, had it taken place here). The Act specifies that the authorised person is satisfied that the extraction is proportionate and that there are no other ways of obtaining the required information. They must demonstrate that the issues and alternatives for obtaining the information have been considered before undertaking the extraction activity. thinks there is a risk of obtaining information in excess of that which is required for the purposes of subsection (2) or section 41(2). In such a case, in order to be satisfied, the authorised person must be satisfied that there are no other ways of obtaining the required information which avoid that risk or, if there are, that it is not reasonably

	practicable to rely on them. This means that, for example, a police constable should not use this power to extract video evidence from a witness's digital device if there is a risk of extracting other information and it is possible and practical to obtain the same video evidence another way which doesn't carry that risk. There may be instances where the information required exists elsewhere, such as in CCTV, but it is not reasonably practicable to obtain it, as doing so would take an excessive amount of time. The authorised person must show due regard for confidential information in the course of exercising these powers and the potential amount of confidential information likely to be held on the device. Where cases involved devices owned by individuals have died or are used by individuals without capacity the authorised persons will need to make a separate assessment for this.
Police Act 1997	This Act makes provision for entry and interference with property and wireless telegraphy, during the course of the prevention or detection of serious crime. Social media data can be acquired via equipment interference such as bugging or hacking devices. Police can do this via physical equipment under this Act.
Police and Criminal Evidence Act (PACE) 1984	The Police and Criminal Evidence Act 1984 (PACE) sets out a legislative framework for the powers of police officers in England and Wales to combat crime and provides codes of practice for the exercise of those powers. This legislation does not apply in Scotland unless officers from England, Wales and Northern Ireland are using their cross-border policing powers and procedures. In relation to social media evidence: **Powers to search** Section 1 details the procedure by which special procedure material and excluded material can be obtained. A circuit judge can order that such material be produced to a constable for him to take away or that such material be made available for the constable to access within seven days of the order. For information held on a computer, an order can be made that the material is produced in a visible and legible form in which it can be taken away. Or an order can be made giving a constable access to the material in a visible and legible form within seven days of the order. **Obtaining a search warrant** Section 8 details that a justice of the peace can issue a search warrant, if it is believed an indictable offence has been committed and evidence of that offence is on the premises. This warrant may, as per S16 of PACE, also authorise persons who can accompany the officers conducting the search – for example, a computer expert. **Powers of seizure** Section 19 details the power by which an officer can seize items and the circumstances in which they can be seized. Schedule 20 details extensions to those powers listed in Schedule 19 for computerised information. This includes details the power for requiring information held on a computer to be produced in a form in which it can be taken away and in which it is visible and legible. **Access and Copying** Section 21 details the power in relation to having items seized accessed and copied to other relevant parties. **Retention**

	Section 22 details the circumstances in which seized property can be retained.
Policing and Crime Act 2017	Section 20 of the Act covers Investigations by IPCC: powers of seizure and retention. The Act amends Section 19 of the Police Reform Act 2002 by adding Section 19ZE that provides the IPCC with the power to seize items which may have evidential value relating to the IPCC's investigations. Sub-section (3) enables the designated person to request digital information.
Regulation of Investigatory Powers Act (RIPA) 2000	RIPA makes provision for the acquisition and disclosure of data relating to the interception of private communications (e.g., phone calls, emails, text messages and social media posts); carrying out covert surveillance by public bodies including the use of bugs and video surveillance; the use of covert human intelligence sources; and the acquisition of the means by which electronic data protected by encryption or passwords may be decrypted or accessed; The scope extends beyond the police to other law enforcement bodies (such as the Serious Fraud Office or the Serious Organised Crime Agency), the security and intelligence services (MI5, MI6 and GCHQ), as well other public bodies, including local government. Chapter 1 details provisions for the lawful interception of communications and communications data and the requirement of warrants. The Act updated the law on "telephone tapping" to clearly cover Internet communications and to ensure that tapping "private" networks was lawful. Chapter 2 covers directed and intrusive surveillance and also sets up a formal system for the serving of notices on telecommunication companies and ISPs to obtain "communications data", superseding the old ad hoc system based on s29(3) of the Data Protection Act 1998. Part 1 of the Act covers communications and communications data. Communications data in the Act is categorised into three groups: • Traffic data – including information about where the communications were made and received • Service use information – such as the type of communication, time sent, duration etc. • Subscriber information – including billing data such as name, address and bank details *Note: Certain clauses of Part 1 of the Act were never brought into force. These and a small number of the operative provisions of this Part of the Act have now been subsumed into the Investigatory Powers Act 2016* *Part 2 details a system for authorising "surveillance" to ensure that the right to a "private life" under Article 8 of the European Convention on Human Rights is not breached. Part 2 power has now been incorporated into the Investigatory Powers Act 2016* Part 3 covers the provisions for the investigation of electronic data protected by encryption etc. Section 49 introduced powers enabling members of the law enforcement to give notices that require the disclosure of protected or encrypted information that would facilitate the obtaining or discovery of the "key" (any key, code, password, algorithm or other data that allows access to the electronic data or facilitates the putting of the data in an intelligible form).

	The grounds for a Section 49 notice are recorded in Section 49(2): (a) that the key is in the possession of the person on whom the notice is served; (b) that disclosure is necessary for the purpose of securing the effective exercise or proper performance by any public authority of any statutory power or statutory duty; (c) the disclosure requirement is proportionate to what is sought to be achieved; and (d) an intelligible version of the relevant protected information cannot be obtained by other reasonable means The areas covered by the notice listed in Section 49(2)(b) relate to (i) national security; (ii) preventing or detecting crime; (iii) economic well-being of the United Kingdom; or (iv) securing performance by any public authority of a statutory power or duty. Section 53 creates an offence of failing to comply with the terms of a notice served under Section 49. Part 4 established the Intelligence Services Commissioner, Surveillance and Interception Commissioners, Investigatory Powers Commissioner for Northern Ireland, and an Investigatory Powers Tribunal to hear complaints about unwarranted interception and related issues. Part 5 covers other miscellaneous and supplementary issues.
Data Protection Act 2018	The Data Protection Act 2018 controls how an individual's personal information is used by organisations, businesses or the government. Everyone responsible for using personal data must follow strict procedures that follow data protection principles. The four main areas provided for in the Act are general data processing; law enforcement data processing; data processing by the intelligence services; and regulatory oversight and enforcement. The other parts contain provisions of general application, including interpretation and our functions and powers. Part 3 of the DPA 2018 sets out a separate data protection regime for authorities with law enforcement functions when they are processing for law enforcement purposes. It also applies to their processors. Section 29 details that consent of the data subject is not required when processing personal data to prevent or detect crime, apprehend or prosecute offenders, the assessment and collection of taxes and duties and to discharge a statutory function.
Criminal Procedures and Investigations Act 1996	Part 2 of the Criminal Procedure and Investigations Act 1996 makes provision for the publication of a Code of Practice which sets out how police officers are to record, retain and reveal to the prosecutor material obtained in a criminal investigation.
Criminal Justice and Police Act 2001	The main powers of seizure for the police are provided by Section 19 of PACE 1984. Additional powers are detailed in Part 2 of the Criminal Justice and Police Act 2001, Sections 50 and 51. These allow officers limited powers to seize property from premises or persons so they can sift or examine it elsewhere. These powers should only be used when essential and implications for the owners be considered. Copies, images or data should be considered as an alternative to removing originals. Materials seized under Sections 50-51 should be kept separate from any materials seized under other powers.

	Section 50 (re: search and seizure – bulk items) describes the power by which an item can be seized, if it is believed it may be something or it may contain an item or items for which there is a lawful authorisation to search. Section 50(1) where a person is lawfully on premises carrying out a search and it is not practicable to determine at the time if an item found is something that he is entitled to seize, or if the contents of an item are things that he is entitled to seize, the item can be taken away for this to be determined. There must be reasonable grounds for believing the item may be something for which there was authorisation to search. **Section 50(2)** where a person is lawfully on premises and an item for which there is a power to seize is found, but it is contained within an item for which there would ordinarily be no power to seize and it is not practicable to separate them at the time, both items can be seized. **Section 51** gives additional powers of seizure from the person where there is an existing power to search that person. It is necessary because, for example, individuals might have on them handheld computers or computer disks which might contain items of electronic data which the police would wish to seize. Part 2 of Schedule 1 details a list of powers of seizure conferred by various legislation to which section 51 applies. Any item found, which is seized with no power to do so, must be returned as soon as reasonably practicable. Items of legal privilege should also be returned as soon as practicable, if there is no power to retain them.
Human Rights Act 1998	Part II, Protocol 1 Article 1 of the Act provides that every natural or legal person is entitled to the peaceful enjoyment of his possessions. No one shall be deprived of his possessions except in the public interest and subject to the conditions provided for by law and by the general principles of international law. The preceding provisions shall not, however, in any way impair the right of a State to enforce such laws as it deems necessary to control the use of property in accordance with the general interest or to secure the payment of taxes or other contributions or penalties.
Computer Misuse Act 1990	The Act deals specifically with the crime of accessing or modifying data stored on a computer system without being authorised to do so. Section 1 deals with unauthorised access to computer material. It is an offence to cause a computer to perform any function with intent to gain unauthorised access to any program or data held in any computer i.e., hacking. It is necessary to prove that access secured is unauthorised and the suspect knows this is the case. Section 2 deals with unauthorised access with intent to commit other offence. An offence is committed as per Section 1, but the Section 1 offence is committed with the intention of committing an offence or facilitating the commission of an offence. Section 3 explores unauthorised acts which have the intent to impair operation. An offence is committed if any person does an unauthorised act with the intention of impairing the operation of any computer.

Serious Crime Act 2015	Investigators can also acquire data via equipment interference software that allows remote access to the device. The Serious Crime Act 2015 grants certain exemptions from the Computer Misuse Act 1990.

Appendix B(ii)

Legal Framework – Data Review

ACT	NARRATIVE
Computer Misuse Act 1990	The Act deals specifically with the crime of accessing or modifying data stored on a computer system without being authorised to do so. Section 1 deals with unauthorised access to computer material. It is an offence to cause a computer to perform any function with intent to gain unauthorised access to any program or data held in any computer i.e. hacking. It is necessary to prove that access secured is unauthorised and the suspect knows this is the case. Section 2 deals with unauthorised Access with Intent to Commit Other Offence. An offence is committed as per Section 1, but the Section 1 offence is committed with the intention of committing an offence or facilitating the commission of an offence. Section 3 explores unauthorised Acts with Intent to Impair Operation. An offence is committed if any person does an unauthorised act with the intention of impairing the operation of any computer.
Regulation of Investigatory Powers Act (RIPA) 2000	RIPA makes provision for the acquisition and disclosure of data relating to the interception of private communications (e.g. phone calls, emails, text messages and social media posts); carrying out covert surveillance by public bodies including the use of bugs and video surveillance; the use of covert human intelligence sources; and the acquisition of the means by which electronic data protected by encryption or passwords may be decrypted or accessed; The scope extends beyond the police to other law enforcement bodies (such as the Serious Fraud Office or the Serious Organised Crime Agency), the security and intelligence services (MI5, MI6 and GCHQ), as well other public bodies, including local government. Part 3 covers the provisions for the investigation of electronic data protected by encryption etc. Section 49 introduced powers enabling members of the law enforcement to give notices that require the disclosure of protected or encrypted information that would facilitate the obtaining or discovery of the "key" (any key, code, password, algorithm or other data that allows access to the electronic data or facilitates the putting of the data in an intelligible form). The grounds for a Section 49 notice are recorded in Section 49(2): (a) that the key is in the possession of the person on whom the notice is served; (b) that disclosure is necessary for the purpose of securing the effective exercise or proper performance by any public authority of any statutory power or statutory duty; (c) the disclosure requirement is proportionate to what is sought to be achieved; and (d) an intelligible version of the relevant protected information cannot be obtained by other reasonable means The areas covered by the notice listed in Section 49(2)(b) relate to (i) national security; (ii) preventing or detecting crime; (iii) economic well-being of the United Kingdom; or (iv) securing performance by any public authority of a statutory power or duty.

	Section 53 creates an offence of failing to comply with the terms of a notice served under Section 49. Part 5 covers other miscellaneous and supplementary issues.
Police and Criminal Evidence Act (PACE) 1984	The Police and Criminal Evidence Act 1984 (PACE) sets out a legislative framework for the powers of police officers in England and Wales to combat crime and provides codes of practice for the exercise of those powers. This legislation does not apply in Scotland unless officers from England, Wales and Northern Ireland are using their cross-border policing powers and procedures. In relation to social media evidence: **Access and Copying** Section 21 details the power in relation to having items seized accessed and copied to other relevant parties. **Retention** Section 22 details the circumstances in which seized property can be retained.
Data Protection Act 2018	The Data Protection Act 2018 controls how an individual's personal information is used by organisations, businesses or the government. Everyone responsible for using personal data must follow strict procedures that follow data protection principles. The four main areas provided for in the Act are general data processing; law enforcement data processing; data processing by the intelligence services; and regulatory oversight and enforcement. The other parts contain provisions of general application, including interpretation and our functions and powers. Part 3 of the DPA 2018 sets out a separate data protection regime for authorities with law enforcement functions when they are processing for law enforcement purposes. It also applies to their processors. Section 29 details that consent of the data subject is not required when processing personal data to prevent or detect crime, apprehend or prosecute offenders, the assessment and collection of taxes and duties and to discharge a statutory function.
Electronic Communications Act 2000	Section 8 of the Act provides a power to modify legislation to remove restrictions arising from other legislation which prevent the use of electronic communications or storage in place of paper. The Act increases confidence in electronic transactions by providing legal admissibility for digital signatures. This includes amending the Public Records Act 1958 to enable the Public Record Office to authenticate copies in electronic form of public records so as to make them admissible evidence in legal proceedings when they are viewed on the Public Record Office website.
Criminal Justice and Police Act 2001	Part 2 of the Act, Sections 50 and 51 allow officers limited powers to seize property from premises or persons so they can sift or examine it elsewhere. Materials seized under section 50-51 should be kept separate from any materials seized under other powers.
Investigatory Powers Act 2016	This Act provides an updated framework for the use of investigatory powers to obtain communications and communications data. These powers cover the interception of communications, the retention and acquisition of communications data, and equipment interference for

	obtaining communications and other data. It is not lawful to exercise such powers other than as provided for by the Act. It provides consistent statutory safeguards and clarifies which powers different public authorities can use and for what purposes. It sets out the statutory tests that must be met before a power may be used and the authorisation regime for each investigative tool, including a new requirement for Judicial Commissioners to approve the issuing of warrants for the most sensitive and intrusive powers.

Appendix B(iii)

Legal Framework – Disclosure

ACT	NARRATIVE
Criminal Procedures and Investigations Act 1996	The statutory framework for criminal investigations and disclosure is contained in the Criminal Procedure and Investigations Act 1996 (the CPIA) and the CPIA Code of Practice. The CPIA aims to ensure that criminal investigations are conducted in a fair, objective and thorough manner, and requires prosecutors to disclose to the defence material which has not previously been disclosed to the accused and which might reasonably be considered capable of undermining the case for the prosecution against the accused or of assisting the case for the accused. The CPIA requires a timely dialogue between the prosecution, defence and the court to enable the prosecution properly to identify such material.
Data Protection Act 2018	The Data Protection Act 2018 controls how an individual's personal information is used by organisations, businesses or the government. Everyone responsible for using personal data must follow strict procedures that follow data protection principles. The four main areas provided for in the Act are general data processing; law enforcement data processing; data processing by the intelligence services; and regulatory oversight and enforcement. The other parts contain provisions of general application, including interpretation and our functions and powers. Part 3 of the DPA 2018 sets out a separate data protection regime for authorities with law enforcement functions when they are processing for law enforcement purposes. It also applies to their processors. Section 29 details that consent of the data subject is not required when processing personal data to prevent or detect crime, apprehend or prosecute offenders, the assessment and collection of taxes and duties and to discharge a statutory function.

Appendix B(iv)

Legal Framework – Presentation

ACT	NARRATIVE
Police and Criminal Evidence Act (PACE) 1984	Section 78 of PACE is the principal device by which a judge can exclude evidence. Section 78 permits the Judge to "refuse to allow evidence on which the prosecution proposes to rely… if it appears to the Court that, having regard to all the circumstances, including the circumstances in which the evidence was obtained, the admission of the evidence would have such an adverse effect on the fairness of the proceedings that the Court ought not to admit it." Section 78(1) states "In any proceedings the court may refuse to allow evidence to be given on which the prosecution proposes to rely if it appears to the court that, having regard to all the circumstances, including the circumstances in which the evidence was obtained, the admission of the evidence would have such an adverse effect on the fairness of the proceedings that the court ought not to admit it."
Criminal Justice Act 2003	Hearsay is not explicitly defined in the Act but the opening words of s114(1) taken together with section 115(3) effectively define it as a representation of fact or opinion made by a person, otherwise than in oral evidence in the proceedings in question, when tendered as evidence of any matter stated therein. Section 114 permits the admission of hearsay evidence if it is the opinion of a non-expert. Written notice must be given under the Criminal Procedure Rules 2015 to the other party and to the court when making an application to admit hearsay evidence in the following cases: • in the interests of justice (under section 114 (1) (d) CJA 2003); • where a witness is unavailable (section 116 CJA 2003); • where the evidence is in a statement prepared for the purposes of criminal proceedings (section 117(1)(c) CJA); • where the evidence is multiple hearsay (section 121 CJA 2003).
Electronic Communications Act 2000	Section 8 of the Act provides a power to modify legislation to remove restrictions arising from other legislation which prevent the use of electronic communications or storage in place of paper. The Act increases confidence in electronic transactions by providing legal admissibility for digital signatures. This includes amending the Public Records Act 1958 to enable the Public Record Office to authenticate copies in electronic form of public records so as to make them admissible evidence in legal proceedings when they are viewed on the Public Record Office website.
Criminal Procedures and Investigations Act 1996	This code of practice is issued under Part II of the Criminal Procedure and Investigations Act 1996 ('the Act'). It sets out the manner in which police officers are to record, retain and reveal to the prosecutor material obtained in a criminal investigation and which may be relevant to the investigation, and related matters. The Code of Practice was published in 2015 in accordance with section 25(4) of the Criminal Procedure and Investigations Act 1996 (see Disclosure for further definitions and details).

Data Protection Act 2018	The Data Protection Act 2018 controls how an individual's personal information is used by organisations, businesses or the government. Everyone responsible for using personal data must follow strict procedures that follow data protection principles. The four main areas provided for in the Act are general data processing; law enforcement data processing; data processing by the intelligence services; and regulatory oversight and enforcement. The other parts contain provisions of general application, including interpretation and our functions and powers.

Appendix B(v)

Legal Framework – Privacy

ACT	NARRATIVE
Regulation of Investigatory Powers Act (RIPA) 2000	RIPA makes provision for the acquisition and disclosure of data relating to the interception of private communications (e.g., phone calls, emails, text messages and social media posts); carrying out covert surveillance by public bodies including the use of bugs and video surveillance; the use of covert human intelligence sources; and the acquisition of the means by which electronic data protected by encryption or passwords may be decrypted or accessed; The scope extends beyond the police to other law enforcement bodies (such as the Serious Fraud Office or the Serious Organised Crime Agency), the security and intelligence services (MI5, MI6 and GCHQ), as well other public bodies, including local government. Chapter 1 details provisions for the lawful interception of communications and communications data and the requirement of warrants. The Act updated the law on "telephone tapping" to clearly cover Internet communications and to ensure that tapping "private" networks was lawful. Chapter 2 covers directed and intrusive surveillance and also sets up a formal system for the serving of notices on telecommunication companies and ISPs to obtain "communications data", superseding the old ad hoc system based on s29(3) of the Data Protection Act 1998. Part 1 of the Act covers communications and communications data. Communications data in the Act is categorised into three groups: • Traffic data – including information about where the communications were made and received • Service use information – such as the type of communication, time sent, duration etc. • Subscriber information – including billing data such as name, address and bank details *NOTE: Certain clauses of Part 1 of the Act were never brought into force. These and a small number of the operative provisions of this Part of the Act have now been subsumed into the Investigatory Powers Act 2016* *Part 2 details a system for authorising "surveillance" to ensure that the right to a "private life" under Article 8 of the European Convention on Human Rights is not breached. Part 2 power has now been incorporated into the Investigatory Powers Act 2016* Part 3 covers the provisions for the investigation of electronic data protected by encryption etc. Section 49 introduced powers enabling members of the law enforcement to give notices that require the disclosure of protected or encrypted information that would facilitate the obtaining or discovery of the "key" (any key, code, password, algorithm or other data that allows access to the electronic data or facilitates the putting of the data in an intelligible form). The grounds for a Section 49 notice are recorded in Section 49(2):

	(a) that the key is in the possession of the person on whom the notice is served; (b) that disclosure is necessary for the purpose of securing the effective exercise or proper performance by any public authority of any statutory power or statutory duty; (c) the disclosure requirement is proportionate to what is sought to be achieved; and (d) an intelligible version of the relevant protected information cannot be obtained by other reasonable means The areas covered by the notice listed in Section 49(2)(b) relate to (i) national security; (ii) preventing or detecting crime; (iii) economic well-being of the United Kingdom; or (iv) securing performance by any public authority of a statutory power or duty. Section 53 creates an offence of failing to comply with the terms of a notice served under Section 49. Part 4 established the Intelligence Services Commissioner, Surveillance and Interception Commissioners, Investigatory Powers Commissioner for Northern Ireland, and an Investigatory Powers Tribunal to hear complaints about unwarranted interception and related issues. Part 5 covers other miscellaneous and supplementary issues.
Data Protection Act 2018	The Data Protection Act 2018 controls how an individual's personal information is used by organisations, businesses or the government. Everyone responsible for using personal data must follow strict procedures that follow data protection principles. The four main areas provided for in the Act are general data processing; law enforcement data processing; data processing by the intelligence services; and regulatory oversight and enforcement. The other parts contain provisions of general application, including interpretation and our functions and powers. Part 3 of the DPA 2018 sets out a separate data protection regime for authorities with law enforcement functions when they are processing for law enforcement purposes. It also applies to their processors. Section 29 details that consent of the data subject is not required when processing personal data to prevent or detect crime, apprehend or prosecute offenders, the assessment and collection of taxes and duties and to discharge a statutory function.
Criminal Procedures and Investigations Act 1996	Part 2 of the Criminal Procedure and Investigations Act 1996 makes provision for the publication of a Code of Practice which sets out how police officers are to record, retain and reveal to the prosecutor material obtained in a criminal investigation.
Criminal Justice and Police Act 2001	The main powers of seizure the police have are provided by Section 19 of PACE 1984. Additional powers are detailed in Part 2 of the Criminal Justice and Police Act, Sections 50 and 51. These allow officers limited powers to seize property from premises or persons so they can sift or examine it elsewhere. These powers should only be used when essential and implications for the owners be considered. Copies, images or data should be considered as an alternative to removing originals. Materials seized under section 50-51 should be kept separate from any materials seized under other powers.
Human Rights Act 1998	Article 8 of the Act protects a person's privacy, family life, home and our communications. Individuals have the right to uninterrupted and uncensored communication with others – a right that's particularly

	relevant when challenging phone tapping and the reading of private communications.
Electronic Communications Act 2000	Section 8 of the Act provides a power to modify legislation to remove restrictions arising from other legislation which prevent the use of electronic communications or storage in place of paper. The Act increases confidence in electronic transactions by providing legal admissibility for digital signatures. This includes amending the Public Records Act 1958 to enable the Public Record Office to authenticate copies in electronic form of public records so as to make them admissible evidence in legal proceedings when they are viewed on the Public Record Office website.
Computer Misuse Act 1990	The Act deals specifically with the crime of accessing or modifying data stored on a computer system without being authorised to do so. Section 1 deals with unauthorised access to computer material, which is pertinent to privacy issues. It is an offence to cause a computer to perform any function with intent to gain unauthorised access to any program or data held in any computer i.e. hacking. It is necessary to prove that access secured is unauthorised and the suspect knows this is the case.
Digital Economy Act 2017	Part 5 of the Act gives government powers to share personal information across organisational boundaries to improve public services. It states what data can be shared and for which purposes. It also includes safeguards to make sure that the privacy of citizens' data is protected.

Appendix C

Relevant Legal Cases for Digital Evidence

Digital Extraction

- Aston Investments Limited v OJSC Russian Aluminium (Rusal), [2006] EWHC 2545 (Comm). (changes to data affecting digital evidence)
- Freemont (Denbigh) Ltd v Knight Frank LLP 3 [2014] EWHC 3347 (Ch) (tampering and falsifying evidence)
- Court of Appeal in R v E [2018] EWCA 2426 (Crim) (reasonable lines of enquiry)
- R v Carl Bater-James and Sultan Mohammed [2020] EWCA Crim 790 (access, review and disclosure of digital evidence)

Digital Review

- Bilta (UK) Limited (in Liquidation) v Nazir [2010] EWHC 3227 (CH) (hard drive access)
- Khodorkovskiy and Lebedev v Russia EU 11082/06 13772/05 – [2013] ECHR 747 (25 July 2013). (volatile nature of data)
- L C Services Limited v Andrew Brown [2003] EWHC 3024 (QB) (deleting evidence before found)
- O'Shea v The Queen [2010] EWCA Crim 2879 (disguising IP addresses)

Disclosure

- R v E [2018] EWCA Crim 2426 (disclosure of digital evidence and the weight attached to it by the judge)
- R v Allan [2017] (late disclosure of mobile phone evidence by police in a rape trial)
- R v Richards, Gold, Whiston-Dew, Anwyl, Demetriou, Gold, Page and Franklin [2015] (correct disclosure procedures for bulk data)

Presentation

- ZXC v Bloomberg LP [2019] EWHC 970 (QB) (right to privacy for those being investigated)
- Big Brother Watch v. Secretary of State [2018] ECHR 722 (secret surveillance, including the bulk interception of external communications)

Privacy

- R v Singh [2006] EWCA Crim 660 (hearsay and applied assertions)
- R v Palmer [2016] EWCA Crim 2237 (use of social media text message as adduced evidence)
- Bucknor [2010] EWCA Crim 1152 (authentication of weak evidence)
- R v Twist and Others [2011] EWCA Crim 1143 (hearsay and "implied assertion")
- Mayers [2008] EWCA Crim 2989; Fox [2009] EWCA Crim 1280; Ford [2010] EWCA Crim 2250 (anonymous hearsay evidence)

Appendix D

Policy, Procedure and Guidance Framework for Digital Evidence

Data Extraction	Data Review	Disclosure	Presentation	Privacy
• ACPO Good Practice Guide for Digital Evidence 2012 • ACPO Good Practice and Advice Guide for Managers of e-Crime Investigations • Criminal Procedure and Investigations Act Code of Practice 2015 • CPS A guide to "reasonable lines of enquiry" and communications evidence 2018 • ENFSI Scenes of Crime Examination Best Practice Manual 2012 • ENISA Basic Guide for first responders 2014 • FSR Codes of Practice and Conduct for Forensic Science Providers and Practitioners in the Criminal Justice System 2017 • FSS Scenes of Crime Handbook 2004	• Al-Khateeb and Cobley (2015) • ACPO Good Practice Guide for Digital Evidence 2012 • AFSP Standards for the formulation of evaluative forensic science expert opinion 2009 • Common Digital Evidence Storage Format Working Group. (2006) • CPS A guide to "reasonable lines of enquiry" and communications evidence 2018 • ENISA Basic Guide for first responders 2014 • FSR Codes of Practice and Conduct for Forensic Science Providers and Practitioners in the Criminal Justice System 2017 • FSR Guidance: Expert Report Guidance 2019 • Home Office Digital Imaging Procedure 2007	• ACPO Good Practice Guide for Digital Evidence 2012 • Attorney General's Guidelines on disclosure for investigators, prosecutors and defence practitioners 2020 • Criminal Procedure and Investigations Act Code of Practice 2015 • Criminal Procedure Rules and Guide 2015 • CPS Disclosure Manual 2018 • CPS Disclosure - Guidelines on Communications Evidence 2018 • CPS CPS guidance social media offences. 2018 • CPS Guidance for Experts on Disclosure, Unused Material and Case Management 2019	• ACPO Good Practice Guide for Digital Evidence 2012 • AFSP Standards for the formulation of evaluative forensic science expert opinion 2009 • Criminal Procedure Rules and Guide 2015 • Law Commission, Expert Evidence in Criminal Proceedings in England and Wales, 2011 • MoJ Criminal Practice Directions 2015 (and amendments) • Sommer (2017) Digital Evidence Handbook (Kindle edition)	• ACPO Good Practice Guide for Digital Evidence 2012 • Criminal Procedure and Investigations Act Code of Practice 2015 • EC The Privacy and Electronic Communications (EC Directive) Regulations 2003 • HO Interception of communications: code of practice 2016 • House of Commons/House of Lords Joint Committee on Human Rights (2019) (moved from below) • Sommer (2017) Digital Evidence Handbook (Kindle edition)

• Home Office Digital Imaging Procedure 2007 • Home Office Rules for Mutual Legal Assistance (MLA) in Criminal Matters 2013 • Home Office Acquisition and Disclosure of Communications Data Code of Practice 2015 • Home Office Interception of communications: code of practice 2016 • Home Officer Covert surveillance and covert human intelligence sources codes of practice 2018 • Information Commissioner's Officer 2020 • National Forensic Science Technology Center (NFSTC) • Sommer (2017) Digital Evidence Handbook (Kindle edition) 2017	• HM Government 2011 • ISO/IEC 17020 General Criteria for the Operation of Various Types of Bodies Performing Inspection • ISO/IEC 17025 General requirements for the competence of testing and calibration laboratories • Law Commission 2011 • National Forensic Science Technology Center (NFSTC) • PACE Code B 2013 • Sommer (2017) Digital Evidence Handbook (Kindle edition)	• FSR Guidance: Expert Report Guidance 2019 • Home Office Acquisition and Disclosure of Communications Data Code of Practice 2015 • Judiciary of England and Wales, Judicial Protocol on the Disclosure of Unused Material in Criminal Cases Dec 2015 • Law Commission, Expert Evidence in Criminal Proceedings in England and Wales, 2011 • Sommer (2017) Digital Evidence Handbook (Kindle edition)		

Appendix E(i)

Policies, Procedures and Guidance – Data Extraction

DOCUMENT	NARRATIVE
ACPO Good Practice Guide for Digital Evidence 2012	Section 3 details procedures for planning a digital investigation, including where digital evidence can be found, including in-transit data. Section 4 outlines how to capture and retrieve this data. Including proportionality issues relating to seizure; planning and attending the crime scene; and capturing online evidence.
ACPO Good Practice and Advice Guide for Managers of e-Crime Investigations	An updated version of the ACPO Good Practice and Advice Guide for Managers of e-Crime Investigation.
Criminal Procedure and Investigations Act Code of Practice 2015	The Code of Practice issued under section 23(1), CPIA (in its March 2015 edition) identifies at part 3 general responsibilities relevant to this disclosure duty. In particular, paras.3.4-5 state: "… In conducting an investigation, the investigator should pursue all reasonable lines of inquiry, whether these point towards or away from the suspect. What is reasonable in each case will depend on the particular circumstances.
CPS A guide to "reasonable lines of enquiry" and communications evidence 2018	Mobile devices are not standard and the ability of digital forensic services to access data varies between manufacturers, models, operating systems and even versions of the same model may also change over time. It is not possible to obtain and examine every artefact or item of digital evidence from a device for analysis in every situation – there are constraints to the extent and depth of an examination in the circumstances of each case. It is critical that the investigator and prosecutor are aware of the opportunities presented by a device and the limitations and boundaries of an examination; including the implications of utilising one examination methodology over another if further work is required in the future. This document sets out guidance as to the approach that ought to be adopted by prosecutors, in accordance with their duties under the Criminal Procedure and Investigations Act 1996 ('CPIA'), and the relevant Codes issued under and in pursuance to that Act. In particular, it seeks to address the issues that arise in the context of allegations where the accused and the complainant are known to each other, and where the smart phone or similar digital devices of the complainant or others may contain communication that may be relevant to the case and would fall to be disclosed. This guidance should be read in conjunction with the Disclosure – Guidance on Communication Evidence (published 26 January 2018). Although capabilities vary across England and Wales, there are essentially 3 levels of data extraction and examination of mobile devices offered by the digital forensic services, namely: i) Level 1 – Configured Logical Extraction - Digital Forensics Kiosks,

	ii) Level 2 – Logical & Physical Extraction - Digital Forensics Hubs or Laboratories or Forensic Service Providers, and iii) Level 3 – Specialist Extractions & Examinations - Central Digital Forensics Laboratories or Forensic Service Providers.
ENFSI Scenes of Crime Examination Best Practice Manual 2012	The purpose of this document is threefold: a) To provide a framework of standards, principles and approaches for the detection, recording and recovery of forensic evidence at the crime scene in compliance with the requirement of ISO 17020, as interpreted for crime scene examination. b) To provide a systematic approach for crime scene investigators to establish and maintain working practices in the field of crime scene examination that will deliver reliable records of the crime scene in overview and detail, maximise the quality of the recovery and collecting procedures, and produce robust evidence. c) To encourage more consistent methodology and hence the production of more comparable results, so as to facilitate interchange of data between crime scene investigators and their partners in law enforcement. The manual addresses the entire forensic process at the scene of crime as it is covered by the standard ISO/IEC 17020, from the arrival of the first officer at the crime scene to the point where the report from the crime scene is written. It encompasses the systems, procedures, personnel, equipment and accommodation requirements for the whole spectrum of the process. The process has various stages of action including the following: • Undertaking initial actions at the scene • Developing a scene examination strategy • Undertaking scene examination • Interpreting scene findings and order further examination • Reporting findings
ENISA Basic Guide for first responders 2014	European Union Agency for Network and Information Security document sets out basic guidance for first responders at digital evidence crime scenes, including: • Preparation before arriving at the crime scene • Suggested first responders toolkit and laptop specification • Tools and commands (including Window and Linux) • Arriving at the scene • Seizure of evidence • Memory forensics • Evidence examination
FSR Codes of Practice and Conduct for Forensic Science Providers and Practitioners in the Criminal Justice System 2017	The Forensic Science Regulator (the Regulator) sets out for all practitioners, whether instructed by the prosecution or defence, the values and ideals the profession stands for. This Code of Conduct provides a clear statement to customers and the public of what they have a right to expect. Needs to be read in conjunction with ISO/IEC 17020 and ISO/IEC 17025. The Code currently covers all forensic units that extract and review of crime scene data.
FSS Scenes of Crime Handbook 2004	The overall aim of this handbook is to encourage police forces and international law enforcement agencies to make the most effective and efficient use of forensic science. It has been produced for use as a reference for situations where samples and exhibits are to be collected

	and submitted to any forensic laboratory and deals with all aspects of sampling, packaging and the prevention of contamination.
Home Office Digital Imaging Procedure 2007	To be read in conjunction with other ACPO Guidance. These procedures cover the areas of preparation; capture, protection and storage; and use of social media evidence. Notes to be read in conjunction with the flowchart in the document.
Home Office Interception of communications: code of practice 2016	The code of practice relates to the powers and duties conferred or imposed under Chapter I of Part I of the Regulation of Investigatory Powers Act 2000 ("RIPA"), amended in 2014 by the Data Retention and Investigatory Powers Act 2014 ("DRIPA"). It provides guidance on the procedures that must be followed before interception of communications can take place under those provisions. This code of practice is primarily intended for use by those public authorities listed in section 6(2) of RIPA. It will also allow postal and telecommunication operators and other interested bodies to acquaint themselves with the procedures to be followed by those public authorities.
Home Office Rules for Mutual Legal Assistance (MLA) in Criminal Matters 2013	Mutual Legal Assistance (MLA) is a method of cooperation between States for obtaining assistance in the investigation or prosecution of criminal offences. MLA is generally used for obtaining material that cannot be obtained on a law enforcement (police to police) to basis, particularly enquiries that require coercive means. Requests are made by a formal international Letter of Request (ILOR or LOR). These guidelines are to ensure that requests for MLA received by the UK can be acceded to and executed quickly and efficiently. The guidelines include: • Guidance to authorities who wish to make a formal request for MLA to the UK ('requesting authorities'); • Guidance to authorities on what can be requested without making a formal request for MLA to the UK; These guidelines contain advice on how to make an MLA request, service of process, transfer of proceedings, and restraint and confiscation of property.
Home Office Acquisition and Disclosure of Communications Data Code of Practice 2015	This code of practice relates to the powers and duties conferred or imposed under Chapter II of Part I of the Regulation of Investigatory Powers Act 2000 ('RIPA'). It provides guidance on the procedures to be followed when acquisition of communications data takes place under those provisions.
Home Office Covert surveillance and covert human intelligence sources codes of practice 2018	Guidance on the use of covert surveillance or human intelligence sources by public authorities under part 2 of the Regulation of Investigatory Powers Act (RIPA) 2000. The codes of practice also provide guidance on entry or interference with property or wireless telegraphy by public authorities under section 5 of the Intelligence Services Act 1994 or part 3 of the Police Act 1997.
Information Commissioner's Office Mobile phone data extraction by police forces in England and Wales 2020	This report explains how current mobile phone extraction practices and rules risk negatively affecting public confidence in our criminal justice system. It covers the relevant legislative framework including PACE 1984; CPIA 1996; and privacy laws as covered by the Data Protection Act 2018. The Commissioner concluded that there is concern about the ways that police forces routinely access and extract the contents of mobile phones, with excessive amounts of personal data often being

	extracted, stored, and made available to others, without an appropriate basis in existing data protection law. Practices vary across the country. It is suggested there has been some erosion of public confidence relating to this, especially in terms of privacy. The report makes recommendations that, if implemented effectively, should contribute to restoring this confidence.
National Forensic Science Technology Center (NFSTC)	A useful guide for the extraction and analysis of social media data. Dividing major forensic categories into three, where evidence can be found 1. Internet-based 2. stand-alone computers 3. devices, and mobile devices the guide assists first responders in the difference evidence-gathering processes, tools and concerns. The guide also look at data analysis – where this is performed, the kind of results expected, and the limitations to this.
Sommer (2017) Digital Evidence Handbook (Kindle)	Independent Handbook (Kindle only).

Appendix E(ii)

Policies, Procedures and Guidance – Data Review

DOCUMENT	NARRATIVE
Al-Khateeb, H. M., Cobley, P. (2015) 'How you can Preserve Digital Evidence and why it is Important', A Practical Guide To Coping With Cyberstalking, National Centre for Cyberstalking Research, UK: Andrews UK Limited, pp.50-62.	A practical guide to preserving digital evidence. Includes guidance on storage, deleted material, copying, moving and renaming digital evidence files.
ACPO Good Practice Guide for Digital Evidence 2012	Section 5 details procedures for analysing and interpreting social media data evidence. Also makes reference to: ACPO The NPIA Forensics21 HTCU Computer Examination Process, 2012 (latest version).
Association of Forensic Science Providers. (2009). Standards for the formulation of evaluative forensic science expert opinion. Science and Justice, 49, 161–164.	See Willis, S. (2010). Standards for the formulation of evaluative forensic science expert opinion Association of Forensic Science Providers. Science & Justice, 1(50), 49 re: letter to editor about article. See also Presentation.
Common Digital Evidence Storage Format Working Group. (2006). Standardizing digital evidence storage. Communications of the ACM, 49(2), 67-68.	A publication by the Common Digital Evidence Storage Format Working Group (CDESGW) an American group looking at the lack of a generally accepted format for storing all forms of digital evidence. This has hampered the development of digital forensics as a scientific discipline, and may result in compromised or lost evidence, and significant judicial consequences.
CPS A guide to "reasonable lines of enquiry" and communications evidence 2018	In examining the contents of a mobile device download, the investigator may set parameters relating to timeframes that are proportionate to the facts, for example between the date the complainant and suspect met to a month after the suspect's arrest. If there are messages that are potentially undermining/assisting at either end of the window of time searched, then the search should be extended further. As with all communication evidence, the prosecution must be able to explain to the defence and the court what will be analysed as well as, importantly, what will not. Transparency of the approach that has been taken in every case is of paramount importance. The prosecution should encourage early dialogue with the defence as to what has been considered reasonable.
ENISA Basic Guide for first responders 2014	European Union Agency for Network and Information Security document sets out basic guidance for first responders at digital evidence crime scenes, including data analysis and evaluating and presenting the evidence.

FSR Codes of Practice and Conduct for Forensic Science Providers and Practitioners in the Criminal Justice System 2017	The Forensic Science Regulator (the Regulator) sets out for all practitioners, whether instructed by the prosecution or defence, the values and ideals the profession stands for. This Code of Conduct provides a clear statement to customers and the public of what they have a right to expect. Needs to be read in conjunction with ISO/IEC 17020 and ISO/IEC 17025. The Code currently covers all forensic units that extract and review of crime scene data.
FSR Guidance: Expert Report Guidance 2019	Guidance is applicable to expert reports produced for use in evidence in the CJS in England and Wales. An expert report is required when the witness will, either in the report or in testimony at court, provide evidence of opinion.
Home Office Digital Imaging Procedure 2007	To be read in conjunction with other ACPO Guidance. These procedures cover the areas of preparation; capture, protection and storage; and use of social media evidence. Notes to be read in conjunction with the flowchart in the document.
HM Government (2011). The Government response to seventh report from the House of Commons Science and Technology Committee Session 2010 HC 855. London. HMSO.	The House of Commons Science and Technology Committee published the report of its inquiry into the Forensic Science Service (FSS) on 1 July 2011. The inquiry considered the Government's decision to manage the closure of the Forensic Science Service, focussing in particular on the following issues: • The reasons for the FSS's financial difficulties and the Government's decision-making process; • The impact on forensic science research and development; • The wider implications for the criminal justice system; • The capacity of private forensic service providers; and • The impact of forensic science services carried out by police forces. This Command Paper sets out the Government response to the conclusions and recommendations in the Committee's report.
ISO/IEC 17020 General Criteria for the Operation of Various Types of Bodies Performing Inspection	Specifies requirements for the competence of bodies performing inspection and for the impartiality and consistency of their inspection activities. It applies to inspection bodies of type A, B or C, as defined in ISO/IEC 17020:2012, and it applies to any stage of inspection.
ISO/IEC 17025 General requirements for the competence of testing and calibration laboratories	Specifies the general requirements for the competence, impartiality and consistent operation of laboratories. It is applicable to all organizations performing laboratory activities, regardless of the number of personnel Section 8.3 (Option A) deals with Control of management system documents posters, notices, memoranda, drawings, plans, etc. NOTE: In this context, "documents" can be policy statements, procedures, specifications, manufacturer's instructions, calibration tables, charts, textbooks, These can be on various media, such as hard copy or digital. Note from meeting on 3/10/19 Ruth Morgan raised the issue that these were not suitable for digital/social media evidence. Specifically, she raised the issue that re-performing tests on digital evidence was far more difficult than for other lab tests.
Law Commission (2011). Expert Evidence in Criminal Proceedings in	The decision to address the law on expert evidence was prompted by a call for reform from the House of Commons' Science and Technology Committee, who were concerned that expert opinion

England and Wales. HC 829. London: Stationery Office.	evidence was being admitted in criminal proceedings too readily, with insufficient scrutiny. There are several reasons why special rules on admissibility and disclosure are needed for expert evidence in criminal proceedings, as expert witnesses are quite different from other conventional witnesses: • stand in the very privileged position of being able to provide the jury with opinion evidence on matters within their area of expertise and outside most jurors' knowledge and experience. • a number of recent criminal cases suggest that expert opinion evidence of doubtful reliability is being proffered for admission, and placed before the jury, too readily. • there is a basis for believing that, where expert evidence of questionable reliability is admitted, it is not effectively challenged in cross-examination. • all experts owe an overriding duty to provide the court with impartial evidence within their area of expertise
National Forensic Science Technology Center (NFSTC) A Simplified Guide to Digital Evidence.	A useful guide for the extraction and analysis of social media data. Dividing major forensic categories into three, where evidence can be found 1. Internet-based 2. stand-alone computers 3. devices, and mobile devices the guide assists first responders in the difference evidence-gathering processes, tools and concerns. The guide also look at data analysis – where this is performed, the kind of results expected, and the limitations to this.
PACE Code B 2013	Deals with police powers to search premises and to seize and retain property found on premises and persons.
Sommer (2017) Digital Evidence Handbook (Kindle)	Independent Handbook (Kindle only).

Appendix E(iii)

Policies, Procedures and Guidance – Disclosure

DOCUMENT	NARRATIVE
ACPO Good Practice Guide for Digital Evidence 2012	Section 7.4 outlines the issues relating to disclosure. The main issue relating to disclosure with digital evidence is the sheer volume. Material not used for evidence is known as 'unused material', and it is this material which is the subject of the procedure for disclosure created under the CPIA. Generally, material must be examined in detail by the disclosure officer or the deputy but, exceptionally, the extent and manner of inspecting, viewing or listening will depend on the nature of the material and its form. If such material is not examined in detail, it must nonetheless be described on the disclosure schedules accurately and as clearly as possible. The extent and manner of its examination must also be described together with justification for such action.
Attorney General's Guidelines on disclosure for investigators, prosecutors and defence practitioners 2020	The Guidelines outline the high-level principles which should be followed when the disclosure regime is applied. These Guidelines replace the existing Attorney General's Guidelines on Disclosure issued in 2013 and the Supplementary Guidelines on Digital Material issued in 2013, which is an annex to the general guidelines.
Criminal Procedure and Investigations Act Code of Practice 2015	This code of practice is issued under Part II of the Criminal Procedure and Investigations Act 1996 ('the Act'). It sets out the manner in which police officers are to record, retain and reveal to the prosecutor material obtained in a criminal investigation and which may be relevant to the investigation, and related matters. The Code of Practice was published in 2015 in accordance with section 25(4) of the Criminal Procedure and Investigations Act 1996. Section 3(1)(a) of the CPIA provides a single test for disclosure and requires the prosecution to: "… disclose to the accused any prosecution material which has not previously been disclosed to the accused and which might reasonably be considered capable of undermining the case for the prosecution against the accused or of assisting the case for the accused". "Prosecution material" is defined in section 3(2) as material: (a) which is in the prosecutor's possession and came into his possession in connection with the case for the prosecution against the accused; or (b) which has been inspected in connection with the case for the prosecution against the accused. **Relevant definitions from the Code:** The **disclosure officer** is the person responsible for examining material retained by the police during the investigation; revealing material to the prosecutor during the investigation and any criminal proceedings resulting from it and certifying that he has done this; and disclosing material to the accused at the request of the prosecutor. **Material** is material of any kind, including information and objects, which is obtained or inspected in the course of a criminal investigation and which may be relevant to the investigation. This includes not only material coming into the possession of the investigator (such as documents seized in the course of searching premises) but also material generated by him (such as interview records). Digital material falls into two categories: the first category is material which is created

	natively within an electronic environment (e.g. email, office files, system files, digital photographs, audio etc.); the second category is material which has been digitised from an analogue form (e.g. scanned copy of a document, scanned photograph, a faxed document). Irrespective of the way in which technology changes, the categorisation of digital material will remain the same. The Code details: **General responsibilities** – including the officers in charge and disclosure officers. Recording of information – If material is not recorded in any form, the officer in charge must ensure that it is recorded in a durable or retrievable form (whether in writing, on video or audio tape, or on computer disk). **Retention of documents** – including duty to retain and length of time. **Preparation of material for prosecutor** – The officer in charge, disclosure officer or an investigator may seek advice from the prosecutor about whether any particular item of material may be relevant to the investigation. Material which may be relevant, but the disclosure officer believes will not form part of the prosecution case, must be listed on a schedule. This process will differ depending on whether the case is likely to be heard in the Magistrates' court or the Crown Court. **Revelation of material to prosecutor** Certain unused material must be disclosed to the accused at Common Law if it would assist the defence with the early preparation of their case or at a bail hearing. This material may consist of items such as a previous relevant conviction of a key prosecution witness or the withdrawal of support for the prosecution by a witness. This material must be revealed to the prosecutor for service on the defence with the initial details of the prosecution case. In cases sent to the Crown Court, wherever possible, the disclosure officer should give the schedules concerning unused material to the prosecutor at the same time as the prosecution file in preparation for the first hearing and any case management that the judge may wish to conduct at that stage. The disclosure officer should draw the attention of the prosecutor to any material an investigator has retained which may satisfy the test for prosecution disclosure in the Act and explain why he has come to that view. The disclosure officer must give the prosecutor a copy of any material which falls into the following categories: • information provided by an accused person which indicates an explanation for the offence with which he has been charged; • any material casting doubt on the reliability of a confession; • any material casting doubt on the reliability of a prosecution witness; • any other material which the investigator believes may satisfy the test for prosecution disclosure in the Act. **Subsequent action by disclosure officer** At the time when a schedule of non-sensitive material is prepared for Crown Court cases, the disclosure officer may not know exactly what material will form the case against the accused. In addition, the

	prosecutor may not have given advice about the likely relevance of particular items of material. Once these matters have been determined, the disclosure officer must give the prosecutor, where necessary, an amended certificate or schedule listing any additional material. **Certification by disclosure officer** The disclosure officer must certify to the prosecutor that, to the best of his knowledge and belief, all relevant material which has been retained and made available to him has been revealed to the prosecutor in accordance with this code. He must sign and date the certificate.
Criminal Procedure Rules and Guide 2015	Part 15 of the rules deal with the provisions for disclosure.
Crown Prosecution Service A guide to "reasonable lines of enquiry" and Communication Evidence July 2018	Sets out guidance as to the approach that ought to be adopted by prosecutors, in accordance with their duties under the Criminal Procedure and Investigations Act 1996 ('CPIA'), and the relevant Codes. In particular, it seeks to address the issues that arise in the context of allegations where the accused and the complainant are known to each other, and where the smart phone or similar digital devices of the complainant or others may contain communication that may be relevant to the case and would fall to be disclosed. The guidance should be read in conjunction with the Disclosure – Guidance on Communication Evidence (published 26 January 2018).
Crown Prosecution Service Disclosure Manual 2018	These instructions explain how investigators and the Crown Prosecution Service (collectively, 'the prosecution team') have agreed to fulfil their duties to disclose unused material to the defence. These duties arise under statute and at common law. It is important that the prosecution team adopt consistent practices across England and Wales. This manual contains practical as well as legal guidance relating to disclosure. This is designed to ensure that the statutory duties are carried out promptly, efficiently and effectively. The templates for letters and documents referred to can be found elsewhere on the police and CPS case management systems.
Crown Prosecution Service Disclosure - Guidelines on Communications Evidence 2018	Communications between suspects, complainants or witnesses can be of critical significance whether as evidence in support of the prosecution case or as unused material which either undermines it or assists the defence case. This is particularly so where the complainant and suspect have been in a personal relationship, however briefly, for example, in cases involving allegations of a sexual nature. This guidance is primarily directed to such cases. Its purpose is to ensure that the significance of communication evidence is understood and assessed at the appropriate time and that it is handled correctly. Serious consequences have occurred and will continue to do so if this is not done. Such evidence incudes communications by way of telephone or other electronic device or by social media and is not restricted to communications between the complainant and suspect but may include contact with third parties.
Crown Prosecution Service guidance social media offences. 2018	These Guidelines detail procedures to follow when prosecuting cases involving communications sent via social media. As well as exploring definitions of social media, these guideline also cover substantive offences and communication offences. A selection of charged for such

	offences, including any time limits that might be applicable. It also considers the impact of such offences via Victim Personal Statements and Community Impact Statements.
Crown Prosecution Service Guidance for Experts on Disclosure, Unused Material and Case Management 2019	The instructions are designed to provide a practical guide to preparing expert evidence and to provide guidance on the disclosure obligations of expert witnesses instructed by the Prosecution Team. These instructions will assist expert witnesses, investigators and prosecutors to perform their duties effectively fairly and justly. Expert witnesses are instructed by the Prosecution Team, the police (or another investigator) and the CPS. Expert witnesses have an overriding duty to assist the court and their duty is to the court and not to the Prosecution Team instructing them. This duty includes obligations relating to the disclosure of unused material. The word disclosure is often used in criminal proceedings to refer to the disclosure of unused material, but experts in criminal proceedings have a number of different obligations as to disclosure. Defence and prosecution experts are subject to the obligations contained in the Criminal Procedure Rules both in part 3 as to case management and part 19 as to expert evidence. Further guidance for all experts is contained in the 2015 Criminal Practice Direction that expands upon the Criminal Procedure Rules. These provisions oblige all experts to disclose certain information about themselves and their work. Prosecution experts have further obligations as to the disclosure of unused material. The obligations as to unused material which apply prosecution experts assist in ensuring that the Prosecution Team can comply fully with their disclosure obligations. The prosecution must disclose to the accused any prosecution material which might reasonably be considered capable of undermining the case for the prosecution against the accused or of assisting the case for the accused. This obligation takes precedence over any internal codes of practice or other standards set by any professional organisations to which the expert may belong. Expert obligations as to the disclosure of unused material are set out in part four of this guidance but can be summarised in the key actions of retain, record and reveal. A failure to comply with these guidelines may have a number of adverse consequences which could include: • A prosecution being halted or delayed; • The appellate courts finding that a conviction is unsafe; • The tribunal making an adverse judicial comment about the expert. Such an adverse judicial comment could seriously undermine credibility of the individual as an expert and consequently the fitness to be instructed in future cases; • Professional embarrassment, including possible action by a professional body, loss of accreditation and the potential for civil action by an accused. Conversely, credibility as an expert will be enhanced by the considered application of this guidance and appropriate management of the materials within the investigation.
FSR Guidance: Expert Report Guidance 2019	Sets out the disclosure obligations on expert witnesses. Generally, these requirements are met by providing information in the report issued by the expert. In April 2019 the Criminal Procedure Rules were

	altered to create a requirement for expert witnesses to declare, to the party instructing them, any information which could potentially undermine the expert's credibility. In most cases this information will be provided in the report issued by the expert as there will be a co-existing obligation to disclose the information to the CJS. In cases where the information could undermine the credibility of the expert but could not undermine the credibility of the evidence provided by the expert the information should be provided to the instructing party. This should be done in writing and a record kept of the information provided. "Telecommunications service" means any Internet based services such as web-based email, messaging applications and cloud-based services.
Home Office (2015). Acquisition and Disclosure of Communications Data. Code of Practice. Norwich: Stationery Office.	This code of practice relates to the powers and duties conferred or imposed under Chapter II of Part I of the Regulation of Investigatory Powers Act 2000 ('RIPA'). It provides guidance on the procedures to be followed when acquisition of communications data takes place under those provisions. The code applies to relevant public authorities within the meaning of RIPA: those listed in section 25 or specified in orders made by the Secretary of State under section 25.1. The Code covers procedures to be followed relating to: • Extent of powers • Rules on the granting of authorisations and giving of Notices • Making of contributions towards the costs incurred by communications service providers • Special rules on the granting of Authorisations and giving of notices in specific matters of public interest • Record keeping • Data protection safeguards • Oversight, complaints and contacts
Judiciary of England and Wales, Judicial Protocol on the Disclosure of Unused Material in Criminal Cases Dec 2015	Paras 38 to 43 refer to procedures in large and complex cases in the Crown Court, where disclosure is a particular problem. The legal representatives need to fulfil their duties in this context with care and efficiency; they should co-operate with the other party (or parties) and the court; and the judge and the other party (or parties) are to be informed of any difficulties as soon as they arise. The court should be provided with an up-to-date timetable for disclosure whenever there are material changes in this regard. A disclosure-management document, or similar, prepared by the prosecution will be of particular assistance to the court in large and complex cases. Judges should be prepared to give early guidance as to the prosecution's approach to disclosure, thereby ensuring early engagement by the defence. Cases of this nature frequently include large volumes of digitally stored material. The Attorney General's 2011 guidance (now included as an annex to the Attorney General's Guidelines on Disclosure 2013) is of particular relevance and assistance in this context.
Law Commission, Expert Evidence in Criminal Proceedings in England and Wales, 2011	The decision to address the law on expert evidence was prompted by a call for reform from the House of Commons' Science and Technology Committee, who were concerned that expert opinion evidence was being admitted in criminal proceedings too readily, with insufficient scrutiny. There are several reasons why special rules on admissibility and disclosure are needed for expert evidence in criminal proceedings, as expert witnesses are quite different from other conventional witnesses:

	• stand in the very privileged position of being able to provide the jury with opinion evidence on matters within their area of expertise and outside most jurors' knowledge and experience. • a number of recent criminal cases suggest that expert opinion evidence of doubtful reliability is being proffered for admission, and placed before the jury, too readily. • there is a basis for believing that, where expert evidence of questionable reliability is admitted, it is not effectively challenged in cross-examination. • all experts owe an overriding duty to provide the court with impartial evidence within their area of expertise
Sommer (2017) Digital Evidence Handbook (Kindle edition)	Independent Handbook (Kindle only).

Appendix E(iv)

Policies, Procedures and Guidance – Presentation

DOCUMENT	NARRATIVE
ACPO Good Practice Guide for Digital Evidence 2012	Section 6 outlines procedures for verbal feedback; statement and reports; witness evidence and notes. Also refers to NPIA Forensics21 process maps (possibly on Police College website hub).
AFSP Standards for the formulation of evaluative forensic science expert opinion 2009	See Willis, S. (2010). Standards for the formulation of evaluative forensic science expert opinion Association of Forensic Science Providers. Science & Justice, 1(50), 49 re: letter to editor about article. See also Data Review.
Criminal Procedure Rules and Guide 2015	There are a number of parts that deal with issues relating to presentation of evidence in court. These include: • Part 16 Written witness statements • Part 17 Witness summonses, warrants and orders • Part 18 Measures to assist a witness or defendant to give evidence • Part 19 Expert evidence • Part 20 Hearsay evidence • Part 21 Evidence of bad character • Part 22 Evidence of a complainant's previous sexual behaviour • Part 23 Restriction on cross-examination by a defendant
Law Commission, Expert Evidence in Criminal Proceedings in England and Wales, 2011	The decision to address the law on expert evidence was prompted by a call for reform from the House of Commons' Science and Technology Committee, who were concerned that expert opinion evidence was being admitted in criminal proceedings too readily, with insufficient scrutiny. There are several reasons why special rules on admissibility and disclosure are needed for expert evidence in criminal proceedings, as expert witnesses are quite different from other conventional witnesses: • stand in the very privileged position of being able to provide the jury with opinion evidence on matters within their area of expertise and outside most jurors' knowledge and experience. • a number of recent criminal cases suggest that expert opinion evidence of doubtful reliability is being proffered for admission, and placed before the jury, too readily. • there is a basis for believing that, where expert evidence of questionable reliability is admitted, it is not effectively challenged in cross-examination. • all experts owe an overriding duty to provide the court with impartial evidence within their area of expertise
MoJ Criminal Practice Directions 2015 (and amendments)	A number of parts are applicable to the presentation of social media evidence in court for serious crimes, this includes: • Part 16 Written witness statements • Part 17 Witness summonses, warrants and orders

	• Part 18 Measures to assist a witness or defendant to give evidence • Part 19 Expert evidence • Part 20 Hearsay evidence • Part 21 Evidence of bad character • Part 22 Evidence of a complainant's previous sexual behaviour • Part 23 Restriction on cross-examination by a defendant • Criminal Practice Directions V: Evidence
Sommer (2017) Digital Evidence Handbook (Kindle)	Independent Handbook (Kindle only).

Appendix E(v)

Policies, Procedures and Guidance – Privacy

DOCUMENT	NARRATIVE
ACPO Good Practice Guide for Digital Evidence 2012	Para 7.3.5 When engaging the services of digital forensic contractors, processes and policies for the retention of case-related data should be considered, both on an ongoing basis and following the termination of the contract. Contractors and those engaging them must comply with the terms of the Data Protection Act, and with any local policies of the engaging organisation.
Criminal Procedure and Investigations Act Code of Practice 2015	The code of practice is issued under Part II of the Criminal Procedure and Investigations Act 1996 and sets out the manner in which police officers are to record, retain and reveal to the prosecutor materials obtained in a criminal investigation and which may be relevant to the investigation, and related matters.
EC The Privacy and Electronic Communications (EC Directive) Regulations 2003	These regulations complement the general data protection regime and set out more specific privacy rights on electronic communications. They recognises that widespread public access to digital mobile networks and the internet opens up new possibilities for businesses and users, but also new risks to their privacy. They have been amended a number of times. The EU is in the process of replacing the e-privacy Directive with a new e-privacy Regulation to sit alongside the GDPR.
Home Office Interception of communications: code of practice 2016	The code of practice relates to the powers and duties conferred or imposed under Chapter I of Part I of the Regulation of Investigatory Powers Act 2000 ("RIPA"), amended in 2014 by the Data Retention and Investigatory Powers Act 2014 ("DRIPA").It provides guidance on the procedures that must be followed before interception of communications can take place under those provisions. This code of practice is primarily intended for use by those public authorities listed in section 6(2) of RIPA. It will also allow postal and telecommunication operators and other interested bodies to acquaint themselves with the procedures to be followed by those public authorities. "Telecommunications service" means any Internet based services such as web-based email, messaging applications and cloud-based services.
House of Commons/House of Lords Joint Committee on Human Rights (2019). The Right to Privacy (Article 8) and the Digital Revolution HC 122 HL Paper 14.	This report states that: "The internet has great potential to bring people together, give marginalised people a voice and enable access to learning at a scale that would be impossible offline. But we have heard how it has also led to vast swathes of, sometimes very Personal, data being held and shared without our knowledge, used to make assumptions about us and discriminate against us." The article examines the issues of consent, rights to privacy and risks of discrimination relating to personal data held by others and organisations.
Sommer (2017) Digital Evidence Handbook (Kindle)	Independent handbook (Kindle only).

Appendix F

Literature Framework for Digital Evidence

Data Extraction	Data Review	Disclosure	Presentation	Privacy
• Arshad, Jantan, A and Omolara (2019) • Bell and Boddington (2010) • Boggs and Edwards (2010) • Browning (2010) • Caloyannides (2003) • Casey (2004) • Casey (2005) • Casey and Schatz (2011) • O'Floinn and Ormerod (2011) • O'Floinn and Ormerod (2012) • Garfinkel (2007) • Grispos et al (2015) • Harris (2006) • Mann and Chhabra (2016) • Martini and Choo (2012) • Mason and George (2011) • Mason and Seng (eds.) (2017) • Mason et al (2017) • Montasari (2017) • Myint et al (2019) • Orebaugh (2006) • Rowlingson (2004) • Ruan et al (2013) • Schneider et al (2020) • Sommer (1997)	• Accorsi (2009) • Beebe (2009) • Ćosić and Baća (2010) • Ćosić, Ćosić and Baća (2011) • Ćosić, Ćosić, Ćosić, and Ćosić (2012) • Dean (2013) • Flaglien et al (2011) • FRS (2020) • Granja and Rafael (2017) • Haggerty et al (2012) • Jansen and Ayers (2005) • Jardine (2015) • Liles et al (2009) • Mann and Chhabra (2016) • Marshall and Paige (2018) • Mason et al (2017) • Mazurczyk and Caviglione (2015) • Meyers and Rogers (2004) • Page et al (2019) • Palmer (2002) • Rogers et al (2006) • Rowlingson (2004) • Sommer (2011) • Turner (2005) • Van Buskirk and Liu (2006) • Willis (2010)	• Angus-Anderson (2015) • Argy and Mason (2007) • Attorney General (2018) • House of Commons Justice Committee (2018) • Houses of Parliament (2016) • Montasari (2017) • Schafer et al (??2008) • Sommer (2012)	• Angus-Anderson (2015) • Argy and Mason (2007) • Beth et al (2010) • Boggs and Edwards (2010) • BCS, Expert Panels (2000) • Browning (2010) • Carlson (2015) • Casey (2011) • Chaski (2005) • Goode (2009) • Goodison et al (2015) • Granja and Rafael (2017) • Griffith (2011) • Grubman and Snyder (2011) • Gunby and Carline (2020) • Hoffmeister (2014) • Hornberger (2011) • Ireland and Beaumont (2015) • Kalemi and Yildirim-Yayilga (2016) • Kennedy (2006) • Liu et al (2014) • Makulilo (2018) • Mason and Seng (eds.) (2017) • McKemmish (2008) • Montasari (2017)	• Aminnezhad and Dehghantanha (2014) • Asinari (2004) • Bignami (2007) • Big Brother Watch (2019) • Browning (2010) • Brungs and Jamieson (2005) • Caloyannides (2003) • Halboob et al (2015) • Law et al (2011) • O'Floinn and Ormerod (2011) • Privacy International (2018) • Seyyar and Geradts (2020) • Strutin (2011)

• Sommer (1998) • Sutherland et al (2008) • Taylor et al (2014) • Wegman (2005) • Zdziarski (2008)			• Murphy and Fontecilla (2013) • Nance and Ryan (2011) • O'Floinn and Ormerod (2011) • O'Floinn and Ormerod (2012) • Schatz (2007) • Sholl (2013) • Stockdale (2016) • Thomson (2013) • Wegman (2005)	

Note: See detailed breakdown of each article in Appendices F for full reference

Appendix G(i)

Literature – Data Extraction

ARTICLE	NARRATIVE/ABSTRACT
Arshad, H., Jantan, A., & Omolara, E. (2019). Evidence collection and forensics on social networks: Research challenges and directions. Digital Investigation, 28, 126-138.	Recent article about the challenges of using social media evidence. article explains the current state of evidence acquisition, admissibility, and jurisdiction in social media forensics. It also describes the immediate challenges for the collection, analysis, presentation, and validation of social media evidence in legal proceedings. The authors conclude that there are massive amounts of data available but analysing this is problematic – especially manually. Also, they believe due to the lack of sophisticated supporting tools, it is difficult to ascertain any valuable facts from SM content, therefore, it is essential to develop innovative and better ways to both analyse and present this information to investigators so they can better utilise this information. Suggestion for this include assistance from machine learning techniques and big data methods. The authors also believe improvements are needed in SM forensic extraction and preservation of data and also to achieve heterogeneity across social media.
Bell, G. B., & Boddington, R. (2010). Solid state drives: the beginning of the end for current practice in digital forensic recovery? Journal of Digital Forensics, Security and Law, 5(3), 1.	A technical article about storing digital information, especially reliance in the past on magnetic disc and the shift to technology storage and complex, transistor-based devices for primary storage now.
Boggs, B. C., and Edwards, M. L. (2010). Does what happens on Facebook stay on Facebook? Discovery, admissibility, ethics, and social media. ILL. BJ, 98, 366.	An American article about the discovery, admissibility, ethics of using and social media as evidence in court. It points out the importance of courts allowing the admission of social media evidence, particularly while the case law in this area is still just emerging. It also looks at although the information is discoverable, the authors examine when it becomes admissible. Finally, the authors consider even if the evidence is discoverable and admissible what the ethical considerations are around the use of social media evidence in court.
Browning, J. G. (2010). Digging for the digital dirt: Discovery and use of evidence from social media sites. SMU Sci. & Tech. L. Rev., 14, 465.	American article about the use of social media data as evidence. Explores the areas of identifying and obtaining that evidence; authentication issues; and privacy issues.
Caloyannides, M.A., (2003). ”Digital evidence” and reasonable doubt’. IEEE Security & Privacy 1 (6).	A short article in Privacy Matters detailing that our assumption about what is on the computer is what we put there is totally wrong. The author explores the many ways that data gathered as potential evidence should be called into question as legitimate evidence and that those in the legal profession should view digital evidence with much suspicion.

Casey, E. (2004). Network traffic as a source of evidence: tool strengths, weaknesses, and future needs. Digital Investigation, Vol.1(1), pp.28-43.	This paper discusses the strengths and shortcomings of existing tools in the context of the overall digital investigation process specifically the collection, documentation, preservation, examination and analysis stages. In addition to highlighting the capabilities of different tools, this paper familiarises digital investigators with different aspects of network traffic as a source of evidence. Based on this discussion, a set of requirements is proposed for tools used to process network traffic as evidence in the hope that existing developers will enhance the capabilities of their tools to address the weaknesses.
Casey, E. (2005). Digital arms race-The need for speed. Digital Investigation: The International Journal of Digital Forensics and Incident Response, 2(4), 229-230.	Short editorial article discussing how prepared we are in terms of counter tools compared to criminals who are becoming more sophisticated in understanding digital investigation tools. The editor concludes that more speed is needed in this digital arms race.
Casey, E. and Schatz, B. (2011). Digital investigations in Casey, E. (ed.) (2011) Digital Evidence and Computer Crime. Forensic Science, Computer and the Internet. Elsevier: Academic press. (3rd edition) pp. 187-226.	Chapter 6 in a book edited by E Casey about conducting digital investigations. Includes an in-depth discussion of the main different investigation process models. Identifying and applying for the correct authorisation before undertaking any searches to avoid breaking any laws. Transportation of information, verification and general case management. Also considers the preservation and examination of many types of digital information. Chapter/book is also a good source of further references on many digital evidence topics.
O'Floinn, M., & Ormerod, D. (2012). Social networking material as criminal evidence. Criminal Law Review, 2012(7), 486-512.	Examines issues arising in relation to adducing in criminal proceedings evidence obtained from social networking sites (SNS). Discusses how SNS can be challenged, including challenges to the authenticity of SNS-derived evidence and challenges based on evidentiary exclusionary rules. Provides best practice guidance.
O'Floinn, M., Ormerod, D. (2011) Social networking sites, RIPA and criminal investigations, Criminal Law Review, 10, 766-792.	This, the first of two articles, discusses the uses made by law enforcement agencies of social networking sites (SNSs) for criminal investigation purposes. Explains what SNSs are. Identifies police use of SNSs to investigate known suspects and as a covert surveillance tool to identify and ensnare offenders. Considers the legal issues arising from the use of fake profiles by the police and the regulatory requirements imposed in relation the the various types of police activity on SNSs. Explores potential authorisation problems.
Garfinkel, S. (2007, March). Anti-forensics: Techniques, detection and countermeasures. In 2nd International Conference on i-Warfare and Security (Vol. 20087, pp. 77-84).	This paper explores and categorises traditional anti-forensic techniques and discusses approaches for attacking forensic tools by exploiting bugs in those tools. • Overwriting data and metadata • Cryptography, steganography, and other data hiding approaches • AF techniques that minimize footprint • AF techniques that exploit CFT bugs • AFTs that detect CFTs Finally, it evaluates the effectiveness of these tools for defeating computer forensic tools, presents strategies for their detection, and discusses countermeasures.

	Many of the anti-forensic techniques discussed in the paper can be overcome through improved monitoring systems or by fixing bugs in the current generation of computer forensic tools. Overwriting tools can be frustrated by positioning data so that the attacker does not have the ability to overwrite it. Weak file identification heuristics can be replaced with stronger ones. Compression bombs can be defeated with more intelligent decompression libraries. Although there is anecdotal evidence that file encryption and encrypted file systems are beginning to pose a problem for law enforcement, there are also many reports of officers being able to recover cryptographic passwords and keys using spyware, keyboard loggers, and other tactics. The prudent attacker is safer using a sanitization tool than a cryptographic one, because the sanitizer actually destroys information.
Grispos, G., Glisson, W. B., & Storer, T. (2015). Recovering residual forensic data from smartphone interactions with cloud storage providers. arXiv preprint arXiv:1506.02268.	This research investigates how forensic tools that are currently available to practitioners can be used to provide a practical solution for the problems related to investigating cloud storage environments. The attractiveness of cloud computing is impacting where individuals and organizations store their data. The growing popularity of cloud storage services means that such environments will become an attractive proposition for cybercrime. This could result in an increase in demand for investigations of cloud storage services. However, the issue of conducting digital forensic investigations of cloud computing environments is an increasingly challenging and complex task. One of the biggest challenges facing investigators is the ability to identify and recover digital evidence from the cloud in a forensically sound manner. This work presents the examination of end-devices such as smartphones, which have been used to access cloud storage services. The data recovered from these devices can be used by investigators as a proxy for potential evidence stored in cloud storage services. The effectiveness of this method is dependent on the operating system, specific cloud storage application implementation and usage patterns. In other words, the potential recovery of data increases if a device has been used to view the files through a cloud storage application and the user has not attempted to clear the cache of recently viewed files. Two advantages become apparent to using this investigative approach. First, the investigator can begin the chain of custody process when the device is seized and does not need to rely on the cloud provider to begin this process. Second, the tools and methods which have been used to recover data stored in cloud storage services are widely used by the forensic community. The recovery of metadata artefacts from the smartphone device can, in some scenarios, provide the investigator with insight into further data stored in a cloud service. The information recovered can also help justify a court order requesting assistance from the cloud storage provider to recover further files from the specific account.
Harris, R. (2006). "Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem." Digital Investigation 3 (2006): 44-49.	The authors of this paper attempt to arrive at a standardised view of anti-forensics, via creating a consensus about defining the term firstly and then categorising anti-forensic techniques to create general framework with which anti-forensic issues can be analysed. They conclude that part of the problem in this area is that current definitions tend to concentrate on specific aspects of anti-forensics, rather the issue as a whole. Additionally, they believe that we are placing too much emphasis on forensic

	technology and not on training of people and development of the processes and maybe this needs reprioritising.
Mann, H. K., & Chhabra, G. S. (2016). Volatile Memory Forensics: A Legal Perspective. International Journal of Computer Applications, 155(3).	This is a factual article about the extraction and analysis of volatile data that is available in computer's RAM that is in a running state on windows operating systems and shows the utility of RAM in Computer Forensics that is often neglected while crime scenario with running system is encountered. Keeping in view this necessity, it is essential to consider the issues of digital evidence and their collection, preservation, and admissibility in the court of law. It looks at various active research forensics including disk, network, mobile devices, wireless, live, memory and multimedia, breaking them up into their component parts and looking at tools for analysis. In addition, the authors consider random access memory, virtual memory (including swap space and slack space) and how to recover and analyse volatile data.
Martini, B., and Choo, K. K. R. (2012). An integrated conceptual digital forensic framework for cloud computing. Digital Investigation, 9(2), 71-80.	Increasing interest in and use of cloud computing services presents both opportunities for criminal exploitation and challenges for law enforcement agencies (LEAs). For example, it is becoming easier for criminals to store incriminating files in the cloud computing environment, but it may be extremely difficult for LEAs to seize these files as the latter could potentially be stored overseas. In this paper two of the most widely used and accepted forensic frameworks – McKemmish (1999) and NIST (Kent et al., 2006) – are reviewed to identify the required changes to current forensic practices needed to successfully conduct cloud computing investigations. The authors propose an integrated (iterative) conceptual digital forensic framework (based on McKemmish and NIST), which emphasises the differences in the preservation of forensic data and the collection of cloud computing data for forensic purposes. Cloud computing digital forensic issues are discussed within the context of this framework and finally suggestions for future research are made to further examine this field and provide a library of digital forensic methodologies for the various cloud platforms and deployment models.
Mason, S., & George, E. (2011). Digital evidence and 'cloud' computing. Computer Law & Security Review, 27(5), 524-528.	The term 'cloud computing' has begun to enter the lexicon of the legal world. The term is not new, but the implications for obtaining and retaining evidence in electronic format for the resolution of civil disputes and the prosecution of alleged criminal activities might be significantly affected in the future by 'cloud' computing. This article is an exploratory essay in assessing the effect that 'cloud' computing might have on evidence in digital format in criminal proceedings in the jurisdiction of England & Wales.
Mason, S & Seng, D. (eds.) (2017). Electronic Evidence Fourth Edition. London: Institute of Advanced Legal Studies (IALS) University of London.	Comprehensive book about electronic evidence covering most areas. Specifically, for data extraction it has chapters on: The sources of electronic evidence The characteristics of electronic evidence
Mason, S., Sheldon, A., & Dries, H. (2017). Proof: the technical collection and examination of electronic evidence in Mason, S & Seng, D. (eds.) (2017) Electronic Evidence Fourth	This chapter from a book sets out guidelines for handling digital evidence, including data gathering and review. It covers a range of topics relevant to data retrieval and review: Forensic triage – a term used to cover a range of processes, methodologies, software, and hardware that can be used enable people to prioritise their digital forensic investigations more

Edition. London: Institute of Advanced Legal Studies (IALS) University of London, pp. 285-337.	effectively. There are a number of models that can be used but it is important to balance the need for rapid identification of material of interest with the consequence of stopping further analysis. Handling electronic evidence – including standards required, access issues, and volatility of data. Identifying electronic evidence – source and reliability of the information needs to be assessed. When at an early stage the actions of the investigator may cause changes to the electronic evidence. Gathering electronic evidence – need to determine what, if any, physical evidence, such as computers, printers, computer mice or facsimile machines, should be retained (see ACPO Guide which provides a list of the types of hardware and storage devices that are susceptible to being retained). Copying electronic evidence – the process of copying / acquiring and handling electronic evidence should be is subject to several commonly applied best practices and principles. ACPO Guide1 illustrate the importance of the data collection phase of this process. Preserving electronic evidence: • Validating digital data • HASH collisions • The continuity of custody • Transporting and storing electronic evidence • Cloud computing Analysis of electronic evidence – use of tools to: • Copying the hard drive • Viewing the data • Recovering data • Passwords and encryption Traces of evidence for example through: • Network connections • Logs, files and printing • Use of the Internet o Browser cache o Cookies o Private browsing, VPN proxies and TOR o Email and instant messaging Reporting – should include a range of information pertinent to the case, including: (i) Notes prepared during the examination phase of the investigation. (ii) Details about the way in which the investigation was conducted. (iii) Details about the continuity of custody. (iv) The validity of the procedures used. (v) Details of what was discovered, including: (a) Any specific files or data that were directly related to the investigation. (b) Any further files or data that may support the conclusions reached by the specialist. This will include the

	recovery of any deleted files and the analysis of any graphic files. (c) The types of search conducted, such as key word searches, and the programs searched. (d) Any relevant evidence from the Internet, such as emails and the analysis of websites visited and log files. (e) Indications of names that might demonstrate evidence of ownership of software, such as with whom the software was registered. (f) Whether there was any attempt to hide data in any way, and if so, what methods were used. Analysis of a failure – important to understand the impact on an investigation when the police do not conduct a careful investigation, and the prosecution's failure to understand the weakness of the evidence upon which the charges are preferred. Anti-forensics and interpretation of evidence - as with all fields of forensic analysis, computer forensics is part of a continuous race of catch-up between investigators and criminals. Anti-computer forensics has become the term for the possible countermeasures that criminals may take to prevent, delay or invalidate computer forensic efforts. Computer software has been developed to mitigate against data access and theft, but this is often 'purpose neutral'. In other words, what works as a protection against criminals works as a protection from the police or other investigators trying to obtain access to data evidence. Some common methods of anti-forensics include: • Data destruction • Falsifying data • Hiding data • Attacks against computer forensics • Trail obfuscation The authors concluded that, one of the major difficulties in investigating evidence in digital form relates to the incompatibility of formats used to store digital data. The problems arise when an investigator has to deal with different disk image formats. The difficulty is compounded when dealing with different types of electronic evidence, such as network data logs, or the contents of mobile devices. Cloud computing and trusted computing affect the way digital evidence professionals obtain evidence, which means that great care must be taken over how such evidence is obtained, which will doubtless be the subject of careful cross-examination. In addition, the methods used by attackers in the digital environment will mean it is increasingly necessary to take into consideration the use of rarer techniques to obtain evidence in the future.
Montasari, R. (2017, January). Digital Evidence: Disclosure and Admissibility in the United Kingdom Jurisdiction. In International Conference on Global Security, Safety, and Sustainability (pp. 42-52). Springer, Cham.	This paper explores how the admissibility of digital evidence is governed within the United Kingdom jurisdictions, comparing in parts to the differences with the United States. It examines the procedures required for acquiring digital evidence under "proper authorisation", including search warrants and subpoenas, prior to seizing and searching devices.

Myint, O. M., Thein, M. M., and Hling, N. N. (2019). Analysis for various digital forensic and their open-source digital forensic tools with effective function in crime investigation. Journal of Research and Applications (JRA), UCSMTLA Volume-01, Issue-01.	This article looks at the various digital forensic tools used by law enforcement agencies and details the various types of forensics which can be used. These include digital image forensics; mobile device forensics; network forensics; memory forensics; volatile memory forensics; database forensics; application system forensics; file forensic; email forensics; operating system forensics; removeable media forensics; and website forensics.
Orebaugh, A. (2006). Proactive forensics. Journal of digital forensic Practice, 1(1), 37-41.	General article written in 2006 detailing as then, current and future proactive forensic techniques. The author points out that there are several obstacles to proactive forensics. First, network forensic analysis tools require large storage systems. Second, additional personnel are often required to analyse the large amounts of data being monitored and stored. Third, storing network data can present some liability issues since it often contains confidential, personal, and sensitive information. In addition, searching through vast amounts of logged data is time consuming and exhaustive. Finally, proactive forensic technique involves legal and privacy issues. But taking a proactive stance on gathering and using evidence can also serve as a deterrent.
Rowlingson, R. (2004). A ten step process for forensic readiness. International Journal of Digital Evidence, 2(3), 1-28.	The paper proposes a ten-step process for an organisation to implement forensic readiness. These include: 1. Defining the business scenarios that require digital evidence. 2. Identifying available sources and different types of potential evidence. 3. Determining the evidence collection requirement. 4. Establishing a capability for securely gathering legally admissible evidence to meet the requirement. 5. Establishing a policy for secure storage and handling of potential evidence. 6. Ensuring monitoring is targeted to detect and deter major incidents. 7. Specifying circumstances when escalation to a full formal investigation (which may use the digital evidence) should be launched. 8. Training staff in incident awareness, so that all those involved understand their role in the digital evidence process and the legal sensitivities of evidence. 9. Documenting an evidence-based case describing the incident and its impact. 10. Ensuring legal review to facilitate action in response to the incident.
Ruan, K., Carthy, J., Kechadi, T., & Baggili, I. (2013). Cloud forensics definitions and critical criteria for cloud forensic capability: An overview of survey results. Digital Investigation, 10(1), 34-43.	This article details the results and analysis of a survey that was widely circulated among digital forensic experts and practitioners internationally on cloud forensics in order to better understand the key fundamental issues of cloud forensics such as its definition, scope, challenges, opportunities as well as missing capabilities based on the 257 collected responses. Areas considered include: • Cloud forensics and definitions

	• Cloud forensics techniques and research (challenges and opportunities) • Critical criteria for cloud forensic capability (including cloud forensic capability and guidelines, agreement, policy, and staffing importance) The authors concluded that there was general consistency in responses and a working definition was proposed. Areas of critical importance for research and development were also identified and agreed among respondents. That there is an urgent need in the establishment of cloud forensic capabilities including a set of toolkits and procedures for cloud investigations.
Schneider, J., Wolf, J., & Freiling, F. (2020). Tampering with Digital Evidence is Hard: The Case of Main Memory Images. Forensic Science International: Digital Investigation, 32, 300924.	Technical article looking at how easy it is to tamper with digital evidence, which if successful may jeopardise its correct interpretation in court and lead to cases being dismissed. The researchers undertook a number of controls experiments in an effort to manipulate copies of main memory taken during a digital investigation. In line with previous results, the research confirmed that it is quite hard to undertake and that most forgeries are easily detected, though some changed the analysis effect results. Although the numbers were low and therefore not statistically significant, the authors concluded that overall, tampering with main memory dumps appeared to be harder than tampering with hard disc images but the probability to fool an analyst is higher too. Good article for references for general tampering with digital evidence.
Sommer, P. (1997). Downloads, logs and captures: Evidence from cyberspace. Journal of Financial Crime, 5(2), 138-151.	Early article about capturing digital evidence from 'cyberspace'. Discusses in detail various tests to ensure evidential integrity. Tests include: • Remote Computer's Correct Working Test • Provenance of Computer Source Test • Content / Party Authentication Test • Acquisition Process Test • Continuity of Evidence / Chain of Custody Test • Quality of Forensic Presentation Test
Sommer, P. (1998). Digital footprints: Assessing computer evidence. Criminal Law Review Special Edition, 61-78.	This early article describes some of the more common of the forms of computer evidence and techniques of evidence acquisition, preservation and analysis. It explores how inferences are being drawn from computer-derived materials that would not usually be viewed by the ordinary computer user and attempts to indicate some of the practical problems of assessing reliability. Finally, it makes some provisional policy suggestions.
Sutherland, I., Evans, J., Tryfonas, T., & Blyth, A. (2008). Acquiring volatile operating system data tools and techniques. ACM SIGOPS Operating Systems Review, 42(3), 65-73.	This paper emphasises the importance of understanding the potential value of volatile data and how best to collate forensic artifacts to the benefit of the investigation, ensuring the preservation and integrity of the evidence. The paper reviews current methods for volatile data collection, assessment of capabilities, limitations and liabilities of current tools and techniques available to the forensic investigator.
Taylor, MJ, Haggerty, J, Gresty, D, Almond, P and Berry, T (2014). Forensic	Article aimed at finding commonly available guidelines for organisations to undertake their own forensic investigation of social networking applications. The authors consider the process of

investigation of social networking applications. Network Security (11). pp. 9-16.	obtaining evidence from social media and the the aspects of this for organisations.
Wegman, J. (2005). Computer forensics: admissibility of evidence in criminal cases. Journal of Legal, Ethical and Regulatory Issues, 8(1/2), 1.	This American article provides an introduction to the legal issues of using digital evidence in criminal cases. It examines the US laws for search and seizure of digital data, interception of communication and accessing stored digital information.
Zdziarski, J. (2008). iPhone forensics: recovering evidence, personal data, and corporate assets. " O'Reilly Media, Inc.". (Book)	A book telling the reader how to access and recover evidence from an iPhone aimed at among others, law enforcement personnel. Includes chapter on forensic recovery; electronic discovery; desktop tracing and help case studies.

Appendix G(ii)

Literature – Data Review

ARTICLE	NARRATIVE/ABSTRACT
Accorsi, R. (2009, September). Safe-keeping digital evidence with secure logging protocols: State of the art and challenges. In 2009 Fifth International Conference on IT Security Incident Management and IT Forensics (pp. 94-110).	The authors examine the increasing use of log data as digital evidence in court and find that the extent to which existing secure logging protocols used to collect log data fulfil the legal requirements for admissible evidence remain largely unclear. While log data are being increasingly used as digital evidence in judicial disputes, the authors show that protocols used to collect, and store log data fail to satisfy some of the security and hence legal requirements for admissible evidence. As a consequence, more often than not, digital evidence based on log data can be successfully challenged in the court, leading to in-admissibility or loss on probative force.
Beebe, N. (2009, January). Digital forensic research: The good, the bad and the unaddressed. In IFIP International Conference on Digital Forensics (pp. 17-36). Springer, Berlin, Heidelberg.	This paper examines where the discipline of digital forensics is at this point in time and what has been accomplished in order to critically analyse what has been done well and what ought to be done better. The paper also takes stock of what is known, what is not known and what needs to be known. It is a compilation of the author's opinion and the viewpoints of twenty-one other practitioners and researchers, many of whom are leaders in the field. Having reviewed the current state of digital forensics, the authors identify strategic directions for research in this field. Their study reveals four major themes: (i) volume and scalability, (ii) intelligent analytical approaches, (iii) digital forensics in and of non-standard computing environments, and (iv) forensic tool development.
Ćosić, J., & Baca, M. (2010, June). Do we have full control over integrity in digital evidence life cycle? In Proceedings of the ITI 2010, 32nd International Conference on Information Technology Interfaces (pp. 429-434).	This paper examines the problems that occur through the chain of custody of digital evidence during forensic investigations. To prove chain of custody, investigators must know all details on how the evidence was handled every step of the way. List of personnel who can act on the digital evidence include First responders; Forensic investigators; Court expert witness; Law enforcement personnel; Police officers; Victim; Suspect; and Passerby. All can influence the digital evidence. The authors propose a DEMF ("Digital Evidence Management Framework"). Use of all the factors contained in this provide safe and secure chain of custody, to ensure that digital evidence will be accepted by the court.
Ćosić, J., Ćosić, Z., & Baća, M. (2011). An ontological approach to study and manage digital chain of custody of digital evidence. Journal of Information and Organizational Sciences, 35(1), 1-13.	This paper deals with the chain of custody of digital evidence, essential if evidence is to be accepted in court as valid. By this it must be known who exactly, when, where, why, and how came into contact with the potential evidence at each stage of the process. The aim of the paper was to develop ontology to provide a new approach to study and better understand chain of custody of digital evidence. They propose a taxonomy that is modelled top-down, where specific concepts are identified and defined. It is based on the concepts of openness and modularity, so each new entity could be added in the future and described with attributes that are missing. As such this allows us to share a common understanding of the structure of digital forensic among forensic investigators and others that deal with digital evidence.

Ćosić, J., Ćosić G., Ćosić, J., & Ćosić, Z. (2012). Chain of custody and life cycle of digital evidence. Computer Technology and Aplications, 3, 126-129.	The authors present another paper on the concept of the chain of custody relating to digital evidence. Such a chain they state is very difficult to maintain and prove, however, investigators and expert witnesses must know all details on how the evidence was handled every step of the way throughout the investigatory process. The authors argue that at each stage of the process there are threats that can affect the validity of digital evidence (human, technical and natural). The authors also consider the archiving of digital evidence.
Dean, M. D. (2013). Authenticating Social Media in Evidentiary Proceedings. Crim. Just., 28, 49.	Article from US about the authentication of social media content for admissibility in court. Author states that in the US such evidence should be able to show (1) that the content came from an account associated with the purported author, and (2) of author identity. The importance of this and experts who can provide witness statements to verify these are discussed.
Flaglien, A. O., Mallasvik, A., Mustorp, M., & Årnes, A. (2011). Storage and exchange formats for digital evidence. Digital Investigation, 8(2), 122-128.	Digital evidence is becoming increasingly important in a wide variety of criminal investigations and the formats used to store and exchange evidence can have a large impact on both the trustworthiness of evidence and the efficiency of the tools processing the evidence. The authors perform a comparative evaluation of the suitability of different formats by evaluating them against a set of evaluation criteria. Standard file formats include: Raw; EnCase; SMART; DEB; AFF; Gfzip; and ProDiscover. These were evaluated against the following criteria: integrity; metadata; error recording; file splitting; software support; compression; password/encryption; evidence type; and processing and presentation. They discuss research-based storage and exchange formats that aim to improve the representation, processing, and presentation of the evidence. These formats are key initiatives in developing new and more intelligent forensic analysis tools that take advantage of cloud computing and service-oriented systems.
Forensic Science Regulator (FSR) (2020). Annual Report Annual Report 17 November 2018 – 16 November 2019 17 November 2018 – 16 November 2019. Birmingham: FSR.	Forensic Science Regulator (FSR) Annual Report 2018-19. Reports on: • Quality Standards in Place for all Forensic Science Disciplines • Full Compliance with Quality Standards • Shared Understanding of Quality and Standards
Granja, F. M., & Rafael, G. D. R. (2017). The preservation of digital evidence and its admissibility in the court. International Journal of Electronic Security and Digital Forensics, 9(1), 1-18.	This article's objective is to screen and analyse the common models of digital preservation that exist, the elements, the degree of compliance with the general guidelines, the use of techniques and compliance with specific requirements as well as to evaluate the need for a solution to the environment of criminal investigation institutions, in the scenario that lacks a specific model. The importance of the preservation of digital objects is currently heavily analysed. Several aspects may serve to make the digital objects worthless, such as the uselessness of hardware, the deficiency of ancient computing formats to support their use, human errors and malicious software. The majority of crimes currently have a digital component, such that governments and the police are obliged by law to indefinitely hold digital evidence for a case's history. Until the presentation of the digital evidence in court, the evidence must be collected, preserved and properly distributed. The systems currently used often involve multiple steps that do not meet the demands of the growing digital world.

	The volume of digital evidence continues to grow, and these steps will soon become operationally and economically unfeasible for agencies responsible for performing these tasks.
Haggerty, J., Casson, M. C., Haggerty, S., & Taylor, M. J. (2012). A Framework for the forensic analysis of user interaction with social media. International Journal of Digital Crime and Forensics (IJDCF), 4(4), 15-30.	Current tools for the examination of digital evidence find data problematic as they are not designed for the collection and analysis of online data. Therefore, this paper presents a framework for the forensic analysis of user interaction with social media. In particular, it presents an inter-disciplinary approach for the quantitative analysis of user engagement to identify relational and temporal dimensions of evidence relevant to an investigation. This framework enables the analysis of large data sets from which a (much smaller) group of individuals of interest can be identified. In this way, it may be used to support the identification of individuals who might be 'instigators' of a criminal event orchestrated via social media, or a means of potentially identifying those who might be involved in the 'peaks' of activity. In order to demonstrate the applicability of the framework, this paper applies it to a case study of actors posting to a social media Web site.
Jansen, W., & Ayers, R. (2005). An overview and analysis of PDA forensic tools. Digital Investigation, 2(2), 120-132.	This paper gives an overview of forensic software tools for Personal Digital Assistants (PDA). A set of generic scenarios was devised to simulate evidentiary situations and applied to a set of target devices to gauge how selected tools react under various situations. The paper summarizes those results, giving a snapshot of the capabilities and limitations of present-day tools, and also provides background information on PDA hardware and software.
Jardine, E. (2015). The Dark Web dilemma: Tor, anonymity and online policing. Global Commission on Internet Governance Paper Series, (21).	An article about the problems of anonymity and online policing of the Dark Web published by The Global Commission on Internet Governance. It was established in January 2014 to articulate and advance a strategic vision for the future of Internet governance.
Liles, S., Rogers, M., & Hoebich, M. (2009, January). A survey of the legal issues facing digital forensic experts. In IFIP International Conference on Digital Forensics (pp. 267-276). Springer, Berlin, Heidelberg.	This paper discusses the results of a survey focusing on the legal issues facing digital forensic experts in the US. The survey attracted 71 respondents from law enforcement, academia, government, industry and the legal community. It extends the well-known Brungs-Jamieson research on attitudes and priorities of the Australian digital forensic community. The results are compared with those from the Brungs-Jamieson study to determine if digital forensic experts from different countries share priorities and concerns. Several differences are observed between stakeholder groups regarding the importance of specific legal issues. Nevertheless, the results indicate that, despite differing opinions, it is possible to find a common ground that can help craft public policy and set funding priorities.
Mann, H. K., and Chhabra, G. S. (2016). Volatile Memory Forensics: A Legal Perspective. International Journal of Computer Applications, 155(3).	In today's world of fast changing technology where everything is governed by Internet directly or indirectly, the trend of crime has undergone a dramatic change over the past few years. Today, one can commit a crime with just a click of a button on laptop or computer and enjoy the garb of anonymity and impunity to a great extent. In such a scenario, it has become imperative to throw some light on the emerging issue of tackling cybercrimes in 21st century. This paper describes the extraction and analysis of volatile data that is available in computer's RAM that is in a running state on windows operating systems and shows the utility of RAM in Computer Forensics that is often neglected while crime

	scenario with running system is encountered. Keeping in view this necessity, it is essential to consider the issues of digital evidence and their collection, preservation, and admissibility in the court of law.
Mason, S., Sheldon, A., & Dries, H. (2017). Proof: the technical collection and examination of electronic evidence in Mason, S & Seng, D. (eds.) (2017) Electronic Evidence Fourth Edition. London: Institute of Advanced Legal Studies (IALS) University of London, pp. 285-337.	This chapter from a book sets out guidelines for handling digital evidence, including data gathering and review. It covers a range of topics relevant to data retrieval and review: Forensic triage – a term used to cover a range of processes, methodologies, software and hardware that can be used enable people to prioritise their digital forensic investigations more effectively. There are a number of models that can be used but it is important to balance the need for rapid identification of material of interest with the consequence of stopping further analysis. Handling electronic evidence – including standards required, access issues, and volatility of data. Identifying electronic evidence – source and reliability of the information needs to be assessed. When at an early stage the actions of the investigator may cause changes to the electronic evidence. Gathering electronic evidence – need to determine what, if any, physical evidence, such as computers, printers, computer mice or facsimile machines, should be retained (see ACPO Guide which provides a list of the types of hardware and storage devices that are susceptible to being retained). Copying electronic evidence – the process of copying / acquiring and handling electronic evidence should be is subject to several commonly applied best practices and principles. ACPO Guide1 illustrate the importance of the data collection phase of this process. Preserving electronic evidence • Validating digital data • HASH collisions • The continuity of custody • Transporting and storing electronic evidence • Cloud computing Analysis of electronic evidence – use of tools to: • Copying the hard drive • Viewing the data • Recovering data • Passwords and encryption Traces of evidence for example through: • Network connections • Logs, files and printing • Use of the Internet o Browser cache o Cookies o Private browsing, VPN proxies and TOR o Email and instant messaging

	Reporting – should include a range of information pertinent to the case, including: (i) Notes prepared during the examination phase of the investigation. (ii) Details about the way in which the investigation was conducted. (iii) Details about the continuity of custody. (iv) The validity of the procedures used. (v) Details of what was discovered, including: (a) Any specific files or data that were directly related to the investigation. (b) Any further files or data that may support the conclusions reached by the specialist. This will include the recovery of any deleted files and the analysis of any graphic files. (c) The types of search conducted, such as key word searches, and the programs searched. (d) Any relevant evidence from the Internet, such as emails and the analysis of websites visited and log files. (e) Indications of names that might demonstrate evidence of ownership of software, such as with whom the software was registered. (f) Whether there was any attempt to hide data in any way, and if so, what methods were used. Analysis of a failure – important to understand the impact on an investigation when the police do not conduct a careful investigation, and the prosecution's failure to understand the weakness of the evidence upon which the charges are preferred. Anti-forensics and interpretation of evidence - as with all fields of forensic analysis, computer forensics is part of a continuous race of catch-up between investigators and criminals. Anti-computer forensics has become the term for the possible countermeasures that criminals may take to prevent, delay or invalidate computer forensic efforts. Computer software has been developed to mitigate against data access and theft, but this is often 'purpose neutral'. In other words, what works as a protection against criminals works as a protection from the police or other investigators trying to obtain access to data evidence. Some common methods of anti-forensics include: • Data destruction • Falsifying data • Hiding data • Attacks against computer forensics • Trail obfuscation The authors concluded that, one of the major difficulties in investigating evidence in digital form relates to the incompatibility of formats used to store digital data. The problems arise when an investigator has to deal with different disk image formats. The difficulty is compounded when dealing with different types of electronic evidence, such as network data logs, or the contents of mobile devices. Cloud computing and trusted computing affect the way digital evidence professionals obtain evidence, which means that great care must be taken over how such evidence is obtained, which will doubtless be the subject of careful cross-examination. In addition, the methods used by attackers in the digital environment will mean it is increasingly necessary to take

	into consideration the use of rarer techniques to obtain evidence in the future.
Mazurczyk, W., & Caviglione, L. (2015). Information hiding as a challenge for malware detection. arXiv preprint arXiv:1504.04867.	This article looks at how information can be hidden, making it difficult to notice. It is different than encryption, in which the content is unreadable, as it is instead overt. The authors organise existing hiding-capable malware according to the methodology used to implement covert communications. As such, they introduce three major groups: Group 1—methods that hide information by modulating the status of shared hardware/software resources, Group 2—methods that inject secret data into network traffic, and Group 3—methods that embed secret data by modifying a digital file's structure or using digital media steganography, for example, by manipulating image pixels or sound samples. The article concludes with the following future trends for hiding information: • New information-hiding techniques will be continually introduced, and their degree of sophistication will increase. Hence, future malware-related traffic could be harder to detect. • Information hiding offers a decoupled design. Therefore, it can be easily incorporated into every type of malware to provide stealthy communication of both control commands and the exfiltration of confidential user data as well as communication from isolated environments or networks. • Information hiding–capable malware can remain cloaked for a long period of time while slowly but continuously leaking sensitive user data. Thus, this type of malware must be considered a new advanced persistent threat and must be addressed properly.
Meyers, M., & Rogers, M. (2004). Computer forensics: The need for standardization and certification. International Journal of Digital Evidence, 3(2), 1-11.	In this paper published in 2004 the American authors call for standardisation and certification for the computer forensics field. It examines the need for standardization and certification by analysing federal and state court cases (criminal and civil) and concludes with suggestions for dealing with some of the issues raised.
Page, H., Horsman, G., Sarna, A., & Foster, J. (2019). A review of quality procedures in the UK forensic sciences: What can the field of digital forensics learn?. Science & Justice, 59(1), 83-92.	This article explores the quality issues related to forensic science to ensure the validity of results and maintaining the trust of the Criminal Justice System in the findings. Firstly, considering the quality management systems utilised for the examination and analysis of fingerprint, body fluid and DNA evidence, it then proceeds to highlight an apparent lack of comparable quality assurance mechanisms within the field of digital forensics. Proposals are provided for the improvement of quality assurance for the digital forensics arena, drawing on the experiences of, and more well-established practices within, other forensic disciplines. It concludes advising that providers of digital forensic examinations seek to integrate additional quality measures in order to reassure the Criminal Justice System that any results presented are valid and consistent, meeting the standards required of ISO accreditation and those laid out within the Codes of Practice and Conduct.
Palmer, G. L. (2002). Forensic analysis in the digital world.	Published in 2002 this quite old article considers the increase in digital forensics and the issues this raises. Specifically, the

International Journal of Digital Evidence, 1(1), 1-6.	complexity involved in the technology, meaning that experts are required to understand this technology as a prerequisite to stating opinions or conclusions about evidence. And secondly, sufficient conclusive research must stand behind techniques and methods (including tools) employed to analyse and examine exhibits that could become evidence or proof.
Rogers, M. K., Goldman, J., Mislan, R., Wedge, T., & Debrota, S. (2006). Computer forensics field triage process model. Journal of Digital Forensics, Security and Law, 1(2), 2.	This article discusses a particular triage model - The Cyber Forensic Field Triage Process Model (CFFTPM). As some traditional models take time, the CFFTPM proposes an onsite or field approach for providing the identification, analysis and interpretation of digital evidence in a short time frame, without the requirement of having to take the system(s)/media back to the lab for an in-depth examination or acquiring a complete forensic image(s). The proposed model adheres to commonly held forensic principles and does not negate the ability that once the initial field triage is concluded, the system(s)/storage media be transported back to a lab environment for a more thorough examination and analysis.
Rowlingson, R. (2004). A ten-step process for forensic readiness. International Journal of Digital Evidence, 2(3), 1-28.	The paper proposes a ten-step process for an organisation to implement forensic readiness. These include: 1. Defining the business scenarios that require digital evidence. 2. Identifying available sources and different types of potential evidence. 3. Determining the evidence collection requirement. 4. Establishing a capability for securely gathering legally admissible evidence to meet the requirement. 5. Establishing a policy for secure storage and handling of potential evidence. 6. Ensuring monitoring is targeted to detect and deter major incidents. 7. Specifying circumstances when escalation to a full formal investigation (which may use the digital evidence) should be launched. 8. Training staff in incident awareness, so that all those involved understand their role in the digital evidence process and the legal sensitivities of evidence. 9. Documenting an evidence-based case describing the incident and its impact. 10. Ensuring legal review to facilitate action in response to the incident.
Sommer, P. (2011). Certification, registration and assessment of digital forensic experts: The UK experience. digital investigation, 8(2), 98-105.	The article provides a history and review of the various attempts within the UK at assessing, certifying and registering expert witnesses including those who specialise in digital evidence. It analyses the various actors and stakeholders involved in the process and the different needs of law enforcement employers, prosecutors, defence lawyers and judges, There is also an examination of the economics of assessment: the more rigorous the testing the greater the cost e which is probably going to be borne by the applicant and may act as a deterrent to taking on forensic work. The main conclusion is that designers of assessment schemes need to be clear about their aims, and to consider carefully whether in some circumstances these can be achieved by better court procedural rules and vetting schemes based on lawyers acting as referees.

Turner, P. (2005). Unification of digital evidence from disparate sources (digital evidence bags). Digital Investigation, 2(3), 223-228.	Technical paper outlining a new approach to the acquisition and processing of digital evidence obtained from disparate digital devices and sources. To date the capture of digital based evidence has always been in its entirety from the source device and different methods and containers (file types) are used for different types of digital device (e.g. computer, PDA, mobile phone). This paper defines a new approach called a Digital Evidence Bag (DEB) that is a universal container for the capture of digital evidence. The Digital Evidence Bag concept could be used to permit the streamlining of data capture and allow multiple sources of evidence to be processed in a multiprocessor distributed environment and thereby maximizing the use of available processing power. The approach described in this paper allows for the first time the forensic process to be extended beyond the traditional static forensic capture of evidence into the real-time 'live' capture of evidence. In addition to this the Digital Evidence Bag can be used to provide an audit trail of processes performed upon the evidence as well as integrated integrity checking. This article examines this detailing advantages, experiences, best practice and recommendations for future research.
Van Buskirk, E., and Liu, V. T. (2006). Digital evidence: Challenging the presumption of reliability. Journal of Digital Forensic Practice, 1(1), 19-26.	This article examines the general tendency among courts to presume that forensic software reliably yields accurate digital evidence. As a judicial construct, this presumption is unjustified in that it is not tailored to separate accurate results from inaccurate ones. The authors illustrate this unfortunate truth by the presentation of two currently uncorrected weaknesses in popular computer forensic tools, methods, and assumptions. Some percentage of these forensic software errors (and ones like them) will necessarily have negative effects on parties, whether in terms of faulty criminal convictions or improper civil judgments. The authors argue that the collective value of these negative effects among parties is far larger than the costs of research and development required to prevent such negative effects. Under a purely rational economic approach to the law, this dynamic constitutes an inefficiency to be corrected through the proper application of rules. The authors advance two approaches to cure current defects. One is through the proper application of scientific jurisprudence to questions of digital evidence and the other is through some combination of certain broad market and social corrections.
Willis, S. (2010). Standards for the formulation of evaluative forensic science expert opinion Association of Forensic Science Providers. Science and Justice, 1(50), 49.	Letter from Shelia Willis, Chair of the AFSP in relation to Ian Evett's editorial in a previous issue of the Science and Justice journal. Although pleased with the promotion, was disappointed to note that the version of the standards published in the journal with the editorial did not have the rich source of references upon which the standards are based.

Appendix G(iii)

Literature – Disclosure

ARTICLE	NARRATIVE/ABSTRACT
Angus-Anderson, W. (2015). Authenticity and Admissibility of Social Media Website Printouts. Duke Law & Technology Review, 14(1), 33-47.	An American article which sets out to examine two authentication routes courts take (either the Texas or Maryland approach). Rather than identify the differences and the stronger approach, the author finds that courts are merely responding to a lack of evidence connecting the proffered content to the purported author.
Argy, P. N., & Mason, S. (2007). Electronic evidence: disclosure, discovery and admissibility. LexisNexis Butterworths.	This book introduces lawyers to the practical concepts of electronic evidence, how it is created, stored and structured, including computer forensics and experts. It covers disclosure, procedural process and admissibility. The aim is to bring to the attention of lawyers information about electronic evidence, such that they begin to understand what questions to ask of experts, rather than to rely upon experts exclusively, and to make experts appreciate the finer points of procedural and evidential issues relating to electronic evidence.
Attorney General's Review of the efficiency and effectiveness of disclosure in the criminal justice system 2018	The Review builds on previous reports conducted by members of the judiciary and the policing and prosecution inspectorates over recent years. This document should be seen as a plan of practical actions to tackle those problems from the point an allegation is considered by the investigator to the end of the case. All those handling a case – investigators, prosecutors and defence lawyers – have an important part to play, underpinned by oversight from the judiciary. Prosecutions must not be brought based on insufficient evidence, and both the accused and accuser must not be caused unnecessary suspense and uncertainty. The central importance of the duty of disclosure must be seen from the twin perspective of fairness to the accused and as a vital guarantor of a secure conviction. Cases that collapse or are stayed and convictions that are quashed because of serious deficiencies in disclosure are fair neither to the complainant and the defendant nor to the public and they undermine confidence in the administration of criminal justice. It is clear that there must be a new emphasis on compliance with the duty of disclosure much earlier in the process than is currently the practice, supported by better training and methods, an appropriate use of technology, improved data collection and management information on the performance of the obligation, and by strengthened oversight by the Criminal Justice Board, where ministers can hold the system to account. That emphasis has already begun with the National Disclosure Improvement Plan introduced by the previous Director of Public Prosecutions and police leaders to whom I am grateful for this vital initiative. It is also clear that each of the parties to our system must assume the responsibility for making it work by providing the consistent leadership and impetus that it requires.
House of Commons Science and Technology	This inquiry sought to investigate the likely implications of the Government's plan to develop the Forensic Science Service (FSS) as

Committee (2005). Seventh Report.	a Government owned company (GovCo) and possibly a public-private partnership (PPP). It recommends that a Forensic Science Advisory Council be established to act as a regulator of the forensic services market, and to provide a much-needed overview of the process by which forensic science is used in the criminal justice system. In light of the changing status of the FSS, the Council could also provide a source of independent impartial advice on forensic science to the Government, police and others. It further criticise the fact that the Home Office has failed to establish an independent body to oversee the work of the National DNA Database, or to make adequate provision for ethical and lay input. Additionally, it notes the need for better management of the technology transfer process to facilitate exploitation of academic research with potential for application to crime prevention and detection technologies.
Houses of Parliament (2016). Digital Forensics and Crime: Postnote No 520. London: Parliamentary Office of Science and Technology.	This note looks at the use of digital forensics by UK law enforcement agencies. It covers how evidence is obtained, the legislation and regulation in this area, and the efforts being made to address the challenges faced by practitioners.
Montasari, R. (2017). Digital Evidence: Disclosure and Admissibility in the United Kingdom Jurisdiction. In International Conference on Global Security, January 2017 Safety, and Sustainability (pp. 42-52). Springer, Cham.	This paper explores how the admissibility of digital evidence is governed within the United Kingdom jurisdictions, comparing in parts to the differences with the United States. It explores the three issues UK judges usual consider before deciding whether or not to admit digital evidence in court. These include issues relating to search warrants, reliability of evidence and best evidence. The "best evidence" rule refers to a legal principle that an original copy of a document is superior evidence. The authors comments that with the rise in digital evidence and ease of copying and duplicating such data, that the best evidence rule is now near defunct. They go on to discuss the admissibility of copies and the importance of the 'hearsay' rule, which relates to an expert witness verifying the truthfulness of the evidence presented.
Schafer, Burkhard Aitken C.G.G., and Mavridis, D. (2008) Daubert in the UK – Second order evidence between courts and commissions. Joseph Bell Centre University of Edinburgh	This paper analyses some of the conceptual and procedural issues that are raised by the gradual reception of the US Daubert ruling in the UK for admissibility of expert witness statements.
Sommer, P. (2012). Digital Evidence. Digital Investigations and E-Disclosure: A Guide to Forensic Readiness for Organizations, Security Advisers and Lawyers, The Information Assurance Advisory Council (IAAC)	PowerPoint guide for digital evidence in general.

Appendix G(iv)

Literature – Presentation

ARTICLE	NARRATIVE/ABSTRACT
Angus-Anderson, W. (2015). Authenticity and Admissibility of Social Media Website Printouts. Duke Law & Technology Review, 14(1), 33-47.	An American article which sets out to examine two authentication routes courts take (either the Texas or Maryland approach). Rather than identify the differences and the stronger approach, the author finds that courts are merely responding to a lack of evidence connecting the proffered content to the purported author.
Argy, P. N., & Mason, S. (2007). Electronic evidence: disclosure, discovery and admissibility. LexisNexis Butterworths.	(From a book review) This book introduces lawyers to the practical concepts of electronic evidence, how it is created, stored and structured, including computer forensics and experts. It covers disclosure, procedural process and admissibility. The aim is to bring to the attention of lawyers information about electronic evidence, such that they begin to understand what questions to ask of experts, rather than to rely upon experts exclusively, and to make experts appreciate the finer points of procedural and evidential issues relating to electronic evidence.
Beth C. Boggs & Misty L. Edwards, (2010). Does What Happens on Facebook Stay on Facebook? Discovery, Admissibility, Ethics, and Social Media, 98 Ill. B.J. 366, 367.	Early and relatively simple article about admissibility of social media evidence and the use of such sites for lawyers to mine for information about litigants, witnesses, jurors, and more. What are the limits on discovery and admissibility of content gathered on social media sites? What legal-ethics issues do these sites raise? This article looks at the emerging case law. As social networking sites become more popular and attorneys become more knowledgeable about their potential, courts will address more cases about the discovery, admissibility, and ethics of accessing information on social networking sites.
Boggs, B. C., and Edwards, M. L. (2010). Does what happens on Facebook stay on Facebook? Discovery, admissibility, ethics, and social media. ILL. BJ, 98, 366.	An American article about the discovery, admissibility, ethics of using and social media as evidence in court. It points out the importance of courts allowing the admission of social media evidence, particularly while the case law in this area is still just emerging. It also looks at although the information is discoverable, the authors examine when it becomes admissible. Finally, the authors consider even if the evidence is discoverable and admissible what the ethical considerations are around the use of social media evidence in court.
BCS, Expert Panels: Legal Affairs Expert Panel, Submission to the Criminal Courts Review, Lord Justice Auld, 2000.	A submission by The British Computer Society to the Criminal Courts Review. The submission is two-fold: 1. Computer Evidence Commentary on problems arising from current criminal court practice and procedure relating to computer evidence, and proposals intended to improve the fairness and efficiency of the criminal justice process in dealing with such evidence. This part of our submission deals with how the criminal justice process needs to adjust to accommodate changing forms of evidence that are relevant to both traditional crimes and the new forms of e-crime. They suggest that this part of our submission can also be seen as a special case of how the criminal justice process generally needs to adjust to accommodate novel forms of evidence.

	2. Expert evidence on Computer Evidence Commentary on problems arising from current criminal court practice and procedure relating to expert evidence regarding computer evidence, and proposals intended to improve the fairness and efficiency of the criminal justice process in dealing with such expert evidence. This part of our submission deals with how the criminal justice process needs to adjust to accommodate changing demands for expert evidence that are relevant to both traditional crimes and the new forms of e-crime. They suggest that this part of our submission can also be seen as a special case of how the criminal justice process generally needs to adjust to accommodate demands for expert evidence that involve novel science. **Problems with criminal cases involving computer evidence** • Technical complexity • Quantity of evidence • Interpretation of data as evidence • Techno-Speculation • Mishandling of evidence • Contested admissibility • Assumption of reliability • Reliance on a single stream of evidence • Technical expertise of the courts • Inequity in case preparation resources • Possible misuse of criminal court process **Problems of expert evidence in criminal cases involving computer evidence** • What are the expert's duties? • Who is an expert? • Problems facing experts on computer evidence **Problems facing defence experts on computer evidence** Defence experts face particularly difficult problems in criminal cases involving computer evidence. For example, difficulty, delay and cost are frequently incurred in: a) rectifying the absence of technical data identifying the computing environment in which the evidence was seized b) assessing the relevance of vast quantities of computer evidence c) establishing precisely what steps were taken to secure, preserve and/or copy the evidence d) distinguishing evidence that has been produced from data recovered from undeleted files and/or slack space from evidence produced from intact files e) linking disparate sources of computer evidence due to incompatible or inconsistent exhibit numbering systems f) attempting to obtain software licences needed to examine proprietary forensic file formats g) applying to the courts to obtain specifications of proprietary forensic software used to handle and/or investigate the evidence h) applying to the courts to obtain adequate access to disks which contain pornographic and paedophile material. i) having to fund the acquisition of computer hardware and/or software for no other reason than for its use in a single case j) dealing with unnecessary requests from law enforcement agencies

	to agree confidentiality undertakings k) dealing (unpaid) with applications for Legal Aid
Browning, J. G. (2010). Digging for the digital dirt: Discovery and use of evidence from social media sites. SMU Sci. & Tech. L. Rev., 14, 465.	American article about the use of social media data as evidence. Explores the areas of identifying and obtaining that evidence; authentication issues; and privacy issues.
Carlson, S. (2015). When is a Tweet Not an Admissible Tweet: Closing the Authentication Gap in the Federal Rules of Evidence? U. Pa. L. Rev., 164, 1033.	An American article that examines the use of social media given as evidence in US courts and it's authentication, challenging some of the American laws that stood at the time the article was written and deciding whether old rules could be fitted to this new agenda, or whether indeed new rules were needed.
Casey, E. (2011). Digital Evidence in the Courtroom in Casey, E. (ed.) (2011) Digital Evidence and Computer Crime. Forensic Science, Computer and the Internet. Elsevier: Academic press. (3rd edition) pp35-38.	Chapter 3 in a book edited by E Casey about digital evidence given in the courtroom. They outline that the role of digital investigators in this context is to present supporting facts and probabilities. As such, courts depend on the trustworthiness of digital investigators and their ability to present technical evidence accurately; it is their duty to present findings in a clear, factual, and objective manner. They must resist the influence of others' opinions and avoid jumping to conclusions. This chapter covers topics including: duty of experts; admissibility of digital evidence; levels of certainty in digital forensics; direct and circumstantial evidence; and presenting the evidence.
Chaski, C. E. (2005). Who's at the keyboard? Authorship attribution in digital evidence investigations. International journal of digital evidence, 4(1), 1-13.	This article considers the issue of author attribution for digital evidence presented in court. The outline that who was at the keyboard can be approached through several avenues: biometric analysis of the computer user; qualitative analysis of "idiosyncrasies" in the language in question and known documents; and quantitative, computational stylometric analysis of the language in questioned and known documents. Their experiments demonstrated the possibility of a reliable method for determining authorship which uses linguistically defensible units of analysis and is forensically feasible in terms of the brevity and scarcity of texts. Because this particular method obtains a high degree of reliability when it is subjected to a cross-validated statistical procedure, it really is possible to determine who was at the keyboard.
Goode, S. (2009). The admissibility of electronic evidence. Review of Litigation, 29(1), 1-64.	US article about the admissibility of electronic evidence generally following the principles of the UK. Talks about the different ways of authenticating evidence (specifically by personal knowledge, distinctive characters etc, process or systems); the issue of hearsay; and best evidence rules.
Goodison, S. E., Davis, R. C., & Jackson, B. A. (2015). Digital evidence and the US criminal justice system: identifying technology and other needs to more effectively acquire and utilize digital evidence. Santa Monica,	This report describes the results of a National Institute of Justice (NIJ)-sponsored research effort to identify and prioritise criminal justice needs related to digital evidence collection, management, analysis, and use. Through structured interaction with police digital forensic experts, prosecuting attorneys, a privacy advocate, and industry representatives, the effort identified and prioritized specific needs to improve utilization of digital evidence in criminal justice.

CA: RAND Corporation, 2015.	
Granja, F. M., & Rafael, G. D. R. (2017). The preservation of digital evidence and its admissibility in the court. International Journal of Electronic Security and Digital Forensics, 9(1), 1-18.	This article's objective is to screen and analyse the common models of digital preservation that exist, the elements, the degree of compliance with the general guidelines, the use of techniques and compliance with specific requirements as well as to evaluate the need for a solution to the environment of criminal investigation institutions, in the scenario that lacks a specific model. The importance of the preservation of digital objects is currently heavily analysed. Several aspects may serve to make the digital objects worthless, such as the uselessness of hardware, the deficiency of ancient computing formats to support their use, human errors and malicious software. The majority of crimes currently have a digital component, such that governments and the police are obliged by law to indefinitely hold digital evidence for a case's history. Until the presentation of the digital evidence in court, the evidence must be collected, preserved and properly distributed. The systems currently used often involve multiple steps that do not meet the demands of the growing digital world. The volume of digital evidence continues to grow, and these steps will soon become operationally and economically unfeasible for agencies responsible for performing these tasks.
Griffith, H. L. (2011). Understanding and Authenticating Evidence from Social Networking Sites. Wash. JL Tech. and Arts, 7, 209.	This American article provides background information about social networks and explores how to authenticate common types of evidence available on social networking sites. This including authenticating with distinct and non-distinct characteristics; authenticating email and chats from social media sites; and authentication of photos and videos from social media sites. The author concludes that such evidence must be distinctive enough to show who authored the communication and ff the evidence does not contain such distinctive characteristics, the court will require additional foundational evidence for authentication, such as testimony of a witness with knowledge or testimony from a computer expert. Proper foundational evidence will help the proponent of the evidence properly authenticate evidence from social networking sites.
Grubman, S. R., & Snyder, R. H. (2011). Web 2.0 Crashes Through the Courthouse Door: Legal and Ethical Issues Related to the Discoverability and Admissibility of Social Networking Evidence. Rutgers Computer & Tech. LJ, 37, 156.	US article about the issues relating to the discoverability and admissibility of social media evidence in court. Covers areas of relevancy; authentication; hearsay and character evidence from a US legal perspective but still has some principles applicable to UK law.
Gunby, C., & Carline, A. (2020). The Emotional Particulars of Working on Rape Cases: Doing Dirty Work, Managing Emotional Dirt and Conceptualizing 'Tempered Indifference'. The British Journal of	This paper looks at the emotional impact on barristers involved in rape cases; how this may affect their behaviours and what mechanisms they may employ to manage stigma and retain the ability to still feel good about the work they undertake. Developing dirty work theory and scholarship on emotions within criminology more broadly the authors argue that these emotion and sensations cannot be entirely disidentified and develop a concept of 'tempered indifference' to capture the ways advocates strategically turn their emotions down but not to the point of neutrality. This explicates that,

Criminology, 60(2), 343-362.	for rape barristers, a key component of their emotional labour involved turning feelings down – albeit not to the point of neutrality – in order to manage the contradictions stemming from their job. Authors also noted that the tempering of feelings over the years of the profession could have implications for being able to emotionally orientate longer term. Finally, along with high levels of work responsibility and professional expectation being major causes of work stress, the managing of clients' difficult emotions and behaviours contribute to this.
Hoffmeister, T. A. (2014). Social Media in the Courtroom: A New Era for Criminal Justice? ABC-CLIO.	This US book explores the impact of social media on the law, specifically the key players in the criminal justice system – the citizens, law enforcers, attorneys, jurors and judges interact with and use social media. It looks at the processes for admitting social media into evidence including relevancy; authenticity; hearsay; best evidence rule and character evidence.
Hornberger, S. (2011). Social networking websites: Impact on litigation and the legal profession in ethics, discovery, and evidence. Touro L. Rev., 27, 279.	US article on basic information for attorneys regarding social media sites and the impact on their legal professions and working roles.
Ireland, J., & Beaumont, J. (2015). Admitting scientific expert evidence in the UK: reliability challenges and the need for revised criteria–proposing an Abridged Daubert. Journal of Forensic Practice. 17(1), 3-12.	This British paper considers 'scientific' expert evidence in particular where it is considered as unreliable, leading to appeals and acquittals. The authors chart the development of legal criteria for admitting 'scientific' evidence to court. It examined the benefits and difficulties of approaches and proposes an amendment to criteria for increased transparency and evidenced decision making. The findings indicated a range of difficulties with such 'expert' evidence Admissibility including inconsistency, narrow focus of some areas, interpretation difficulties, and the potential to unfairly restrict evidence. The authors propose a two-stage approach to consider whether or not to admit expert evidence. The former seeks to critically review the evidence and define its nature. The latter applies two sets of criteria; a Daubert application for generally accepted physical sciences and proposes an Abridged-Daubert for novel and social/behavioural sciences. The authors also propose an increased involvement by experts reviewing their own evidence and providing statement of limitations. The paper concludes by outlining the importance of developing such an approach for the UK legal system. It focuses on the application of specific criterion which could assist both Courts and witnesses to evaluate the quality of evidence prior to submission by accounting for the nature of the opinion evidence provided.
Kalemi, E., & Yildirim-Yayilgan, S. (2016). Ontologies for social media digital evidence. International Journal of Computer, Electrical, Automation, Control and Information Engineering, 10(2), 335-340.	This article gives an overview on how OSNs are being used to solve crimes and the different methods used to extract digital evidence from them and then how to use that evidence in court. The authors (from Albania) focus on analysing existing ontological models for cyber forensics and propose an initial ontology to fill the need of developing smarter tools for intelligence gathering form OSNs. The purpose of the paper is to start the development of an ontological prototype for supporting crime solving with data found in OSNs and open up further research topics which may benefit from this model. Includes useful diagram about the components of OSNs.

Kennedy, I. (2006). Presenting digital evidence to court. BCS The Chartered Institute for IT.	Article written by Ian Kennedy, at the time a forensic computer analyst for Kent Police, looking at presenting digital evidence in court. Highlighting the importance of having a procedure, he outlines the four principles detailed by ACPO. In addition, adding weight to the argument looking at UK law where each offence has what are known as 'points to prove'. Issues affecting how to present including providing strange evidence for each legal point to prove for a given offence. He considers the challenge for the forensic examiner in that the technical complexity of such cases frequently surpasses the technical knowledge and experience of the court. Therefore, raw computer evidence must be presented with an accurate interpretation, which clearly identifies its significance in the context of where it was found. This interpretation must be undertaken by a suitable qualified person and then presented in a human readable form for consumption by a court. Over-simplification is dangerous as it could lead to the data becoming open to interpretation. Finally, the article looks at planning for a defence. One of the responsibilities of the forensic examiner working for the prosecution is to identify and examine possible areas of defence that may arise. Probably the most common defence identified at the police interview stage of an investigation is that of a Trojan or 'pop-up' being responsible for the presence of any illegal material.
Liu, C., Singhal, A., & Wijesekera, D. (2014). Relating admissibility standards for digital evidence to attack scenario reconstruction. Journal of Digital Forensics, Security and Law, 9(2), 15.	Attackers tend to use complex techniques such as combining multi-step, multi-stage attack with anti-forensic tools to make it difficult to find incriminating evidence and reconstruct attack scenarios that can stand up to the expected level of evidence admissibility in a court of law. As a solution, we propose to integrate the legal aspects of evidence correlation into a Prolog based reasoner to address the admissibility requirements by creating most probable attack scenarios that satisfy admissibility standards for substantiating evidence. Using a prototype implementation, we show how evidence extracted by using forensic tools can be integrated with legal reasoning to reconstruct network attack scenarios. Our experiment shows this implemented reasoner can provide pre-estimate of admissibility on a digital crime towards an attacked network.
Makulilo, A. B. (2018). The admissibility and authentication of digital evidence in Zanzibar under the new Evidence Act. Digital Evidence & Elec. Signature L. Rev., 15, 48.	This article looks at the admissibility and authentication of digital evidence in Zanzibar specifically since the introduction of the Zanzibar Evidence Act in 2016. It explores the usual issues (such as authentication; admissibility; hearsay; disclosure; privacy etc.) encountered by all countries when using digital evidence and makes some international comparisons.
Mason, S & Seng, D. (eds.) (2017). Electronic Evidence Fourth Edition. London: Institute of Advanced Legal Studies (IALS) University of London.	Comprehensive book about electronic evidence covering most areas. Specifically, for presentation it has chapters on: • The foundations of evidence in electronic form • Hearsay • Software code as the witness • The presumption that computers are 'reliable'
McKemmish, R. (2008, January). When is digital evidence forensically sound? In IFIP international conference on	"Forensically sound" is a term used extensively in the digital forensics community to qualify and, in some cases, to justify the use of a particular forensic technology or methodology. Such a wide application of the term can only lead to confusion. This paper examines the various definitions of forensic computing (also called

digital forensics (pp. 3-15). Springer, Boston, MA.	digital forensics) and identifies the common role that admissibility and evidentiary weight play. Using this common theme, the paper explores how the term "forensically sound" has been used and examines the drivers for using such a term. Finally, a definition of "forensically sound" is proposed and four criteria are provided for determining whether or not a digital forensic process may be considered to be "forensically sound."
Montasari, R. (2017, January). Digital Evidence: Disclosure and Admissibility in the United Kingdom Jurisdiction. In International Conference on Global Security, Safety, and Sustainability (pp. 42-52). Springer, Cham.	This paper explores how the admissibility of digital evidence is governed within the United Kingdom jurisdictions, comparing in parts to the differences with the United States. It explores the three issues UK judges usual consider before deciding whether or not to admit digital evidence in court. These include issues relating to search warrants, reliability of evidence and best evidence. The "best evidence" rule refers to a legal principle that an original copy of a document is superior evidence. The authors comments that with the rise in digital evidence and ease of copying and duplicating such data, that the best evidence rule is now near defunct. They go on to discuss the admissibility of copies and the importance of the 'hearsay' rule, which relates to an expert witness verifying the truthfulness of the evidence presented.
Murphy, J. P., & Fontecilla, A. (2013). Social media evidence in government investigations and criminal proceedings: A frontier of new legal issues. Richmond Journal of Law & Technology, 19(3), 11.	This US article examines the importance of social media in government investigations and criminal litigation, including access to and use of social media evidence, constitutional issues that social media evidence raises, the authentication and admissibility of such evidence, in addition to the impact of social media on jurors. It considers the importance of social media; publicly available social media data; social media companies, subpoenas and warrants; defending criminal cases with social media evidence; admissibility; jurors and social media.
Nance, K., & Ryan, D. J. (2011). Legal aspects of digital forensics: a research agenda. In 2011 44th Hawaii International Conference on System Sciences (pp. 1-6). IEEE January 2011.	The evolution of the Information Age has necessitated and facilitated the relatively new field of digital forensics. As a largely practitioner-driven field, there is no clearly defined research agenda to promote top-down research in related areas so that the evolution can be more solidly based on research findings. This paper builds on previously published topical research agendas for digital forensics and introduces a preliminary research hierarchy for legal issues associated with digital forensics. Topics discussed include constitutional law, property law, contract law, tort law, cybercrime, criminal procedure, evidence law, and cyber war. In addition, some special associated problems and overarching areas are identified for consideration and for future research.
O'Floinn, M., & Ormerod, D. (2012). Social networking material as criminal evidence. Criminal Law Review, 2012(7), 486-512.	Examines issues arising in relation to adducing in criminal proceedings evidence obtained from social networking sites (SNS). Discusses how SNS can be challenged, including challenges to the authenticity of SNS-derived evidence and challenges based on evidentiary exclusionary rules. Provides best practice guidance.
O'Floinn, M., Ormerod, D. (2011) Social networking sites, RIPA and criminal investigations, Criminal Law Review, 10, 766-792.	This, the first of two articles, discusses the uses made by law enforcement agencies of social networking sites (SNSs) for criminal investigation purposes. Explains what SNSs are. Identifies police use of SNSs to investigate known suspects and as a covert surveillance tool to identify and ensnare offenders. Considers the legal issues arising from the use of fake profiles by the police and the regulatory requirements imposed in relation the the various types of police activity on SNSs. Explores potential authorisation problems.

Schatz, B. L. (2007). Digital evidence: representation and assurance (Doctoral dissertation, Queensland University of Technology).	This dissertation examines at a fundamental level the nature of digital evidence and investigation, in order that improved techniques which address investigation efficiency and assurance of evidence might be identified. The work follows three themes – representation, analysis techniques and information assurance.
Sholl, E. W. (2013). Exhibit Facebook: The discoverability and admissibility of social media evidence. Tul. J. Tech. & Intell. Prop., 16, 207.	US article from 2013 covering privacy, discoverability and admissibility of digital evidence. Includes topics of relevance, hearsay and authentication under US legalisation. Some principles applicable to UK law.
Stockdale, M. (2016) Expert Evidence in Criminal Proceedings: Current Challenges* Old Bailey Lecture to the Criminal Bar Association of England and Wales Tuesday March 1st, 2016.	Paper from an Old Bailey Lecture given to the Criminal Bar Association of England and Wales in 2016 by Dr Michael Stockdale. The purpose of the paper was to examine the principles that currently govern the admissibility of expert evidence in criminal proceedings, the provisions of CrimPR Part 19 and CrimPD 19A and the Law Commissions' recommendations in order to identify key areas in relation to which additional clarification by the appellate courts, by amendments to CrimPD 19A and/or to CrimPR Part 19 itself would be desirable.
Thomson, L. L. (2013). Mobile devices: New challenges for admissibility of electronic evidence. Scitech Lawyer, 9(3), 32.	No article from Headnote: As mobile devices, social media, and web archives change the nature of digital evidence, will the courts be able to address the increasing complexity? Millions of people are now creating documentation that may become "evidence" in cases around the world. Now in court proceedings, traditional eyewitness testimony can be greatly enhanced and corroborated by introducing digital evidence. Adding to the layers of complexity, web archives are being created by global organizations; regular captures are being made of websites, and the digital material is being saved and preserved for the future. The widespread use of mobile devices has created unprecedented challenges in legal proceedings as the courts decide how to properly authenticate digital information under the current judicial rules and procedures. Although the basic legal requirements for establishing a foundation for admissibility of evidence in US courts are well-established, their applicability to digital data and devices from which electronic evidence is generated raises many difficult evidentiary issues and questions. As a result, courts have applied widely different standards for similar types of evidence when computer-generated.
Wegman, J. (2005). Computer forensics: admissibility of evidence in criminal cases. Journal of Legal, Ethical and Regulatory Issues, 8(1/2), 1.	This paper will provides an introduction to the most significant legal issue in computer forensics: admissibility of evidence in criminal cases. The law of search and seizure, as it relates to digital equipment, will be reviewed. Interception of electronic communications and accessing stored digital information will be examined. Public policy in the form of federal legislation will be discussed. Finally, ethical concerns will be considered.

Appendix G(v)

Literature – Privacy

ACT	NARRATIVE/ABSTRACT
Aminnezhad, A., & Dehghantanha, A. (2014). A survey on privacy issues in digital forensics. *International Journal of Cyber-Security and Digital Forensics (IJCSDF)*, 3(4), 183-199.	This article looks at the challenges forensics investigators, and developers have faced in finding the balance between retrieving key evidence and infringing user privacy. The paper identified various privacy issues in cyber security and digital forensics, issues that use for protecting privacy of data in forensic investigation, whereby how forensics investigators may have infringed user privacy while conducting forensics investigations, and how user privacy is always under threat without proper protection. It also reviewed the current development trend shift in this industry, why such trend could have happened and its drive. The paper concluded that while every development has its positive approach and finds the solution to what the authors want to solve, the issue of privacy preservation still exists, with the consideration of non-technical aspects in professionalism in practice and the ambiguity of scenarios causing some approaches to be counterproductive. The paper also analyses on how at a technical level, advanced technologies in digital forensics and security are facing a bottleneck in development and could bring about as equal harms to the current efforts in preserving privacy.
Asinari, M. V. P. (2004). Legal constraints for the protection of privacy and personal data in electronic evidence handling. International Review of Law, Computers & Technology, 18(2), 231-250.	This article provides a brief discussion about gathering evidence and issues surrounding personal privacy. It focuses mainly on the application of Directive 95/46/EC rules to the digital environment. It also makes reference to the legal risks derived from the collection and processing of e-evidence in violation of privacy and personal data protection law.
Bignami, F. (2007). Privacy and law enforcement in the European union: the data retention directive. *Chi. J. Int'l L.*, *8*, 233.	This Article examines a recent twist in European Union ("EU") data protection law. In the 1990s, the European Union was a market-creating organization and the law of data protection was designed to prevent rights abuses by market actors. Since the terrorist attacks in New York, Madrid, and London, however, cooperation in law enforcement has accelerated. Now the challenge for the European Union is to protect privacy in its emerging system of criminal justice. This Article analyses the first EU law to address data privacy in law enforcement-the Data Retention Directive (or "Directive"). Based on a detailed examination of the Directive's legislative history, this Article finds that privacy-as guaranteed under Article 8 of the European Convention on Human Rights and the Council of Europe's Convention on Data Protection-is adequately protected in the Directive. This positive experience can serve as guidance for guaranteeing other fundamental rights in the rapidly expanding area of EU cooperation on criminal matters.
Browning, J. G. (2010). Digging for the digital dirt: Discovery and use of evidence from social media	Article that explores how the various social networking sites represent a significant shift in the way people communicate and share information. Such sharing, the author points out comes with a price. Lawyers and judges have ready and willing to plunder this digital treasure. Moreover, judges are more and more amenable to

sites. *SMU Sci. & Tech. L. Rev*., 14, 465.	allowing access to the plethora of photos, comments, status updates, and other postings that many users of social media might regard, at least in their own minds, as off limits. The shifting balance between privacy rights and evidence gathering, in the context of a search for the truth, reflects the broader debate being waged not only across the legal landscape, but the cultural one as well. In a society in which individuals live more and more of their lives online, just how much privacy can one expect?
Brungs, A., & Jamieson, R. (2005). Identification of legal issues for computer forensics. Information Systems Management, 22(2), 57-66.	The aim of this study was to identify the key legal issues facing the development of the computer forensics field within the context of the Australian legal environment. A panel of 11 experts in Australia from government law enforcement (police), government regulators, the private sector (consultants), and one academic participated in the study. A set of 17 issues was initially identified from a brainstorming session and then each participant ranked them in terms of importance from their own work relevance perspective. The authors then categorized the 17 issues into a taxonomy of three key issue areas, Judicial Flexibility, Privacy, and Multi-Jurisdictional Nature. For the area of privacy, the authors found that at the time of the research many were unaware of the extensiveness of data surveillance and transparency of the Web. The authors acknowledged that the demand for privacy will impact on computer forensics and therefore, the implications of privacy for computer forensics were yet to be fully realized. Therefore, as they do, further technologies and protocols will need to be adopted to preserve forensic incisiveness in the face of privacy restrictions.
Caloyannides, M. A. (2003). Digital. IEEE Security & Privacy, (6), 89-91.	A short article in Privacy Matters detailing that our assumption about what is on the computer is what we put there is totally wrong. The author explores the many ways that data gathered as potential evidence should be called into question as legitimate evidence and that those in the legal profession should view digital evidence with much suspicion.
O'Floinn, M., Ormerod, D. (2011) Social networking sites, RIPA and criminal investigations, Criminal Law Review, 10, 766-792.	This, the first of two articles, discusses the uses made by law enforcement agencies of social networking sites (SNSs) for criminal investigation purposes. Explains what SNSs are. Identifies police use of SNSs to investigate known suspects and as a covert surveillance tool to identify and ensnare offenders. Considers the legal issues arising from the use of fake profiles by the police and the regulatory requirements imposed in relation the various types of police activity on SNSs. Explores potential authorisation problems.
Halboob, W., Mahmod, R., Udzir, N. I., & Abdullah, M. T. (2015). Privacy levels for computer forensics: toward a more efficient privacy-preserving investigation. Procedia Computer Science, 56, 370-375.	Computer forensics tools try to discover and extract digital evidence related to a specific crime, while privacy protection techniques aim at protecting the data owner's privacy. As a result, finding a balance between these two fields is a serious challenge. Existing privacy preserving computer forensics solutions consider all data owner's data as private and, as a result, they collect and encrypt the entire data. This increases the investigation cost in terms of time and resources. So, there is a need for having privacy levels for computer forensics so that only relevant data are collected, and then only private relevant data are encrypted. This research paper proposes privacy levels for computer forensics. privacy levels are proposed for privacy-preserving computer forensics solutions. They can help improve the investigation efficiency when the privacy is a concern.

Law, F. Y., Chan, P. P., Yiu, S. M., Chow, K. P., Kwan, M. Y., Hayson, K. S., & Lai, P. K. (2011, May). Protecting digital data privacy in computer forensic examination. In 2011 Sixth IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering (pp. 1-6). IEEE.	There does not exist a forensically sound model for protecting private data in the context of digital investigation and it poses a threat to privacy If the investigation involved the processing of such kind of data. In this paper, the authors present a cryptographic model designed to be incorporated into the current digital investigation framework, thereby adding a possible way to protect data privacy in digital investigation. A simulated scenario was carried out to verify the feasibility of the approach and to understand the effect of encryption on the data content. Authors acknowledge that this is not the only solution to the problem but hope that the paper brings this issue to the attention of the community to help develop a forensically sound procedures to solve this problem.
Privacy International (2018) Digital stop and search: how the UK police can secretly download everything from your mobile phone. London: Privacy International.	This article discusses the issue of data extraction from mobile phones. Privacy International has uncovered that in the UK police are using highly intrusive technology to extract and store data from individual's phones, on a questionable legal basis. When a Police Officer obtains a personal mobile device in the UK, Privacy International's understanding is that data extractions, at least in low level crimes, are carried out at one of three places: 1. Self Service Kiosks (SSK), where forensic analysis on the device is carried out within the local police force. 2. Frontline supported service 'Hubs', which can serve a number of forces. 3. Police forces may also equip officers with portable mobile phone extraction kits, which can carry out an analysis outside of any police facilities. From FOI requests they found a number of forces who stated uncertainty as to the legal basis under which they can extract data from mobile phones. Some stated they were governed by Section 20 of the Police and Criminal Evidence Act 1984 (PACE), which grants police the "power to require any information stored in any electronic form" this view was not consistently held. Also, absence and confusion of whether there exists a lack of national guidance. Previous from NPIA now replaced by the College of Policing and they have not issued guidance. The Met has some but that is obviously not national. The NPCC stated that: "The Regulator's codes are helpful here in that they specify accreditation requirements for digital forensics including "the screening or recovery of data from a device using an off the shelf tool for factual reporting" e.g., mobile phone kiosks." But the authors after contacting the FSR were told "Regulator has not produced reviews, reports or guidance additional to that contained in the Statement of Accreditation Requirements on this topic." The speed at which extraction kiosks have been rolled out contrasts with the comparative lack of necessary public information raises concerns. For example, it is unclear: (1) Whether victims, witnesses and suspects, including those released without charge or found innocent, are aware that personal information may have been taken from their phones without their knowledge. (2) If consent is given by the user to the police force to extract data from mobile phones, how informed is that consent; (3) What happens to the vast amount of data that is copied from the device;

	(4) Whether data is shared with other bodies; (5) If this data is deleted, and if so, after how long; and (6) How securely the data is stored. Authors were concerned that police forces are obtaining vast quantities of personal data about people not charged with any crime without their consent, for indefinite periods without clear oversight, guidance or legislation and make a number of recommendations in the article to address all of their concerns found during the research.
Seyyar, M. B., & Geradts, Z. J. M. H. (2020). Privacy impact assessment in large-scale digital forensic investigations. Forensic Science International: Digital Investigation, 200906.	The large increase in the collection of location, communication, health data etc. from seized digital devices like mobile phones, tablets, IoT devices, laptops etc. often poses serious privacy risks. To measure privacy risks, privacy impact assessments (PIA) are substantially useful tools and the Directive EU 2016/80 (Police Directive) requires their use. While much has been said about PIA methods pursuant to the Regulation EU 2016/679 (GDPR) less has been said about PIA methods pursuant to the Police Directive. Yet, little research has been done to explore and measure privacy risks that are specific to law enforcement activities which necessitate the processing of large amounts of data. This study tries to fill this gap by conducting a PIA on a big data forensic platform as a case study. This study also answers the question how a PIA should be carried out for large-scale digital forensic operations and describes the privacy risks, threats we learned from conducting it. Finally, it articulates concrete privacy measures to demonstrate compliance with the Police Directive.
Strutin, K. (2011). Social media and the vanishing points of ethical and constitutional boundaries. Pace L. Rev., 31, 228.	A US article lead by New York State Defenders Association who filled at the time a void in guidance and advice for criminal defense discovery or investigation within networked social spaces can be found in existing statutes and ethics codes.

Appendix H

Additional useful references for the use of digital evidence

Abdalla, A., and Yayilgan, S. Y. (2014, June). A review of using online social networks for investigative activities. In *International Conference on Social Computing and Social Media* (pp. 3-12). Springer, Cham.

Abulaish, M.N. and Haldar, A.H. (2020). Advances in Digital Forensics Frameworks and Tools: A Comparative Insight and Ranking in Bhatele, K. R. R., Mishra, D. D., Bhatt, H., & Das, K. (2020). The Fundamentals of Digital Forensics and Cyber Law. In *Cyber Warfare and Terrorism: Concepts, Methodologies, Tools, and Applications* (pp. 165-191). IGI Global.

Alharbi, S., Weber-Jahnke, J., and Traore, I. (2011, August). The proactive and reactive digital forensics investigation process: A systematic literature review. In *International Conference on Information Security and Assurance* (pp. 87-100). Springer, Berlin, Heidelberg.

Ami-Narh, J. T., and Williams, P. A. (2008). Digital forensics and the legal system: A dilemma of our times. In *Australian digital forensics conference* March 2008 (p. 41).

Angelopoulou, O. and Vidalis, S. (2013) Towards 'crime specific' digital investigation frameworks, in Proceedings of 3rd International conference on Cybercrime, Security and Digital Forensics, 8-9 June 2013, University of Cardiff, Cardiff, Wales, UK.

Atkinson, J. S. (2014). Proof is not binary: the pace and complexity of computer systems and the challenges digital evidence poses to the legal system. *Birkbeck Law Review*, *2*, 245.

Bartholomew, P. (2014). Seize first, search later: The hunt for digital evidence. *Touro Law Review*, *30*(4), 10.

Beebe, N. L., and Clark, J. G. (2005). A hierarchical, objectives-based framework for the digital investigations process. *Digital Investigation*, *2*(2), 147-167.

Berman, K. J., Glisson, W. B., and Glisson, L. M. (2015, January). Investigating the impact of global positioning system evidence. In *2015 48th Hawaii International Conference on System Sciences* (pp. 5234-5243).

Bhatele, K. R. R., Mishra, D. D., Bhatt, H., & Das, K. (2020). The Fundamentals of Digital Forensics and Cyber Law in Bhatele, K. R. R., Mishra, D. D., Bhatt, H., & Das, K. (2020). The Fundamentals of Digital Forensics and Cyber Law. In *Cyber Warfare and Terrorism: Concepts, Methodologies, Tools, and Applications* (pp. 64-81). IGI Global.

Boux, H. J., & Daum, C. W. (2015). At the intersection of social media and rape culture: How Facebook postings, texting and other personal communications challenge the real rape myth in the criminal justice system. *U. Ill. JL Tech. & Pol'y*, 149.

Brown, C. S. (2015). Investigating and prosecuting cyber crime: Forensic dependencies and barriers to justice. *International Journal of Cyber Criminology*, *9*(1), 55.

Browning, J. G. (2010). Digging for the digital dirt: Discovery and use of evidence from
Carrier, B., and Spafford, E. H. (2003). Getting physical with the digital investigation process. *International Journal of digital evidence*, *2*(2), 1-20.

Casey, E. (2009). *Handbook of digital forensics and investigation*. Academic Press.

Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers, and the internet*. Academic press.

Casey E (2019). *Editorial 2019* Trust in digital evidence in *Digital Investigation: The International Journal of Digital Forensics & Incident Response.* Dec 2019 (31/C).

Casey, E. (2020). Standardization of forming and expressing preliminary evaluative opinions on digital evidence. *Forensic Science International: Digital Investigation*, 200888.

Caviglione, L., Wendzel, S., and Mazurczyk, W. (2017). The future of digital forensics: Challenges and the road ahead. *IEEE Security and Privacy*, *15*(6), 12-17.

Church, E., Fafinski, S. (2011) Social networks, crime and the law, *Student Law Review*, Autumn 2011, 13-16.

Cohen, F. B. (2012). *Digital forensic evidence examination*. Livermore: Fred Cohen & Associates.

Cole, K. A., Gupta, S., Gurugubelli, D., and Rogers, M. K. (2015). A review of recent case law related to digital forensics: The current issues. *Annual ADFSL Conference on Digital Forensics, Security and Law 20th May.*

Collie, J. (2018). Commentary: Digital forensic evidence—Flaws in the criminal justice system. *Forensic science international*, *289*, 154-155.

Daly, E. (2021). Making new meanings: The entextualisation of digital communications evidence in English sexual offences trials. *Crime, Media, Culture*, 17416590211048251.

David, A., Morris, S., & Appleby-Thomas, G. (2020). A Two-Stage Model for Social Network Investigations in Digital Forensics. *Journal of Digital Forensics, Security and Law*, *15*(2), 1.

Du, X., Le-Khac, N. A., and Scanlon, M. (2017). Evaluation of digital forensic process models with respect to digital forensics as a service. *arXiv preprint arXiv:1708.01730*.

Dulhare U.N. and Rasool, S. (2020). Digital Evidence in Practice: Procedure and Tools in Bhatele, K. R. R., Mishra, D. D., Bhatt, H., & Das, K. (2020). The Fundamentals of Digital Forensics and Cyber Law. In *Cyber Warfare and Terrorism: Concepts, Methodologies, Tools, and Applications* (pp. 1-22). IGI Global.

Gelb, D. K. (2012). Defending a Criminal Case from the Ground to the Cloud. *Crim. Just.*, *27*, 28.

Glasgow, D. (2010). The potential of digital evidence to contribute to risk assessment of internet offenders, *Journal of Sexual Aggression*, 16:1, 87-106.

Global Justice Information Sharing Initiative (2013). *Developing a Policy on the Use of Social Media in Intelligence and Investigative Activities. Guidance and Recommendations*. US: Global Advisory Committee.

Grajeda, C., Breitinger, F., & Baggili, I. (2017). Availability of datasets for digital forensics–And what is missing. *Digital Investigation*, *22*, S94-S105.

Graves, L., Glisson, W. B., & Choo, K. K. R. (2020). LinkedLegal: Investigating social media as evidence in courtrooms. *Computer Law & Security Review*, *38*, 105408.

Hegarty, R., Lamb, D. J., & Attwood, A. (2014, July). Digital Evidence Challenges in the Internet of Things. In *INC* (pp. 163-172).

HM Inspector of Constabulary (HMIC) (2015). *Real lives, real crimes: A study of digital crime and policing*. London: HMIC.

Hesketh, I., & Williams, E. (2017). A new canteen culture: the potential to use social media as evidence in policing. *Policing: A Journal of Policy and Practice*, *11*(3), 346-355.

Horsman, G. (2020). ACPO principles for digital evidence: Time for an update?. *Forensic Science International: Reports*, 100076.

Jackson, D. W. (2016). Social media evidence. *Oklahoma Bar Journal*, *87*, 2333-2338.

Jackson, G., Jones, S., Booth, G., Champod, C., Evett, I.W., 2006. The nature of forensic science opinion and possible framework to guide thinking and practice in investigation and in court proceedings. Sci. Justice 46 (1), 33e44

Jaquet-Chiffelle, D. O., Casey, E., Pollitt, M., & Gladyshev, P. (2018). *A framework for harmonizing forensic science practices and digital/multimedia evidence* (No. 0002).

Johnston, D. and Hutton, G. (2021) *Blackstone's Police Manual Volume 2: Evidence and Procedure*. Oxford: Oxford University Press.

Kävrestad, J. (2020). Collecting Evidence. In *Fundamentals of Digital Forensics* (pp. 69-78). Springer, Cham.

Karagiannis, C., & Vergidis, K. (2021). Digital evidence and cloud forensics: contemporary legal challenges and the power of disposal. *Information*, *12*(5), 181.

Kessler, G. C. (2010). *Judges' awareness, understanding, and application of digital evidence*. Nova Southeastern University.

Kessler, G. C., and Carlton, G. H. (2020). Exploring Myths in Digital Forensics: Separating Science From Ritual. In *Cyber Warfare and Terrorism: Concepts, Methodologies, Tools, and Applications* (pp. 1299-1308). IGI Global.

Khan, S., Gani, A., Wahab, A. W. A., Shiraz, M., and Ahmad, I. (2016). Network forensics: Review, taxonomy, and open challenges. *Journal of Network and Computer Applications*, *66*, 214-235.

Kirmani, M.S. and Banday, M.T. (2020). Digital Forensics in the Context of the Internet of Things Sample in Bhatele, K. R. R., Mishra, D. D., Bhatt, H., & Das, K. (2020). The Fundamentals of Digital Forensics and Cyber Law. In *Cyber Warfare and Terrorism: Concepts, Methodologies, Tools, and Applications* (pp. 1178-1200). IGI Global.

Köhn, M., Olivier, M. S., & Eloff, J. H. (2006, July). Framework for a Digital Forensic Investigation. In *ISSA* (pp. 1-7).

Kruse II, W. G., and Heiser, J. G. (2001). *Computer forensics: incident response essentials*. Pearson Education.

Law Society (2018). *Artificial Intelligence and the Legal Profession*. London: The Law Society.

Loewen, K. (2015). Rejecting the Purity Myth: Reforming Rape Shield Laws in the Age of Social Media. *UCLA Women's LJ*, *22*, 151.

McMillan, J. E. R., Glisson, W. B., and Bromby, M. (2013, January). Investigating the increase in mobile phone evidence in criminal activities. In 2013 46th Hawaii International Conference on System Sciences (pp. 4900-4909).

Makura, S. M., Venter, H. S., Ikuesan, R. A., Kebande, V. R., and Karie, N. M. (2020, February). Proactive Forensics: Keystroke Logging from the Cloud as Potential Digital Evidence for Forensic Readiness Purposes. In *2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT)* (pp. 200-205).

Mante, R. V., and Khan, R. (2020, March). A Survey on Video-based Evidence Analysis and Digital Forensic. In *2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC)* (pp. 118-121). IEEE.

Mante, R. V., and Khan, R. (2020). A Machine Learning approach for Video-based Evidence Analysis and Digital Forensic. *Sustainable Humanosphere*, *16*(1), 2100-2105.

Marshall, P., Christie, J., Ladkin, B., Littlewood, B., Mason, S., Newby, M., & Thomas, M. (2020). Recommendations for the probity of computer evidence. *Digital Evidence and Electronic Signature Law Review*, *18*.

Mohay, G. (2005). Technical challenges and directions for digital forensics. In *First International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE'05)* (pp. 155-161).

Mothi, D., Janicke, H., & Wagner, I. (2020). A novel principle to validate digital forensic models. *Forensic Science International: Digital Investigation*, 200904.

National Institute of Justice (NIJ) (2001). *Electronic Crime Scene Investigation: A Guide for First Responders*. Washington: U.S. Department of Justice Office of Justice Programs.

Nelson, B., Philips, A., and Steuart, C. (2006). *Guide to computer forensics and investigations. Course Technology*. Florence, KY.

Novak, M. (2020). Digital Evidence in Criminal Cases Before the US Courts of Appeal: Trends and Issues for Consideration. *Journal of Digital Forensics, Security and Law*, *14*(4), 3.

Owen, P., and Thomas, P. (2011). An analysis of digital forensic examinations: Mobile devices versus hard disk drives utilising ACPO and NIST guidelines. *Digital Investigation*, *8*(2), 135-140.

Parichha, P. K. (2020). Introduction to Digital Forensics. In *Big Data Analytics and Computing for Digital Forensic Investigations* (pp. 1-19). CRC Press.

Parkavi, R., and Divya, K. (2020). Digital Crime Evidence. In Critical Concepts, Standards, and Techniques in Cyber Forensics (pp. 116-143). IGI Global.

Pollitt, Mark, 2013. History, historiography, and the hermeneutics of the hard drive. In: Peterson, G., Sujeet, Shenoi (Eds.), *Advances in Digital Forensics IX*. Springer, New York, pp. 3e17, 2013.

Powell, A., & Haynes, C. (2020). Social media data in digital forensics investigations. In *Digital Forensic Education* (pp. 281-303). Springer, Cham.

Powles, S, Waine, L. and May, R. (2015) *May on Criminal Evidence* (6th ed). London: Sweet and Maxwell.)

Radhakant, A., and Diskin, M. (2013). How Social Media Are Transforming Litigation. *Litigation, 39,* 17.

Ramírez Sanabria, P. R. (2020). *Guidelines and tools for a digital evidence investigation process: a case study for a business data leak*. Thesis for Bachelor of Engineering, Information and Communications Technology: Turku University of Applied Sciences.

Richard III, G. G., and Roussev, V. (2006). Next-generation digital forensics. *Communications of the ACM*, *49*(2), 76-80.

Rogers, M., Scarborough, K., Frakes, K., and San Martin, C. (2007). Survey of law enforcement perceptions regarding digital evidence. In *IFIP International Conference on Digital Forensics* (pp. 41-52). Springer, New York, NY.

Rumney, P. N., & McPhee, D. (2020). The Evidential Value of Electronic Communications Data in Rape and Sexual Offence Cases. *The Criminal Law Review. (Accepted for publication)*

Ryser, E., Spichiger, H., & Casey, E. (2020). Structured decision making in investigations involving digital and multimedia evidence. *Forensic Science International: Digital Investigation*, *34*, 301015.

Seigfried-Spellar, K. C., and Leshney, S. C. (2016). The intersection between social media, crime, and digital forensics: # WhoDunIt?. In *Digital forensics* (pp. 59-67). Syngress.

Selamat, S. R., Yusof, R., & Sahib, S. (2008). Mapping process of digital forensic investigation framework. *International Journal of Computer Science and Network Security*, *8*(10), 163-169.

Solomon, M. G., Rudolph, K., Tittel, E., Broom, N., and Barrett, D. (2011). *Computer forensics jumpstart*. John Wiley and Sons.

Sommer, P. (2004). Emerging problems in digital evidence. *Criminal Justice Matters*, *58*(1), 24-25.

Sommer, P. (2005). *Directors and corporate advisors' guide to digital investigations and evidence*. Cambridge: IAAL.

Sommer, P. (2012). *Digital Evidence: Emerging Challenges*. PPT presentation. Fundacion Ramon Areces.

Sommer, P. (2012). Digital Evidence. *Digital Investigations and E-Disclosure: A Guide to Forensic Readiness for Organizations, Security Advisers and Lawyers, The Information Assurance Advisory Council (IAAC)*.

Sorenson, M., 2019. *Flaws in Cellphone Evidence Prompt Review of 10,000 Verdicts in Denmark*. New York Times. Aug 20, 2019.

Spyt, W. S. (2017). *Social Media and Police investigations: Understanding the strategies that officers pursue when they encounter social media in their investigations* (Doctoral dissertation, University of Portsmouth).

Surendar, A. (2020). Computer Forensic Investigation in Cloud of Things in Bhatele, K. R. R., Mishra, D. D., Bhatt, H., & Das, K. (2020). The Fundamentals of Digital Forensics and Cyber Law. In *Cyber Warfare and Terrorism: Concepts, Methodologies, Tools, and Applications* (pp. 855-865). IGI Global.

Tanner, A., and Dampier, D. (2009, January). Concept mapping for digital forensic investigations. In *IFIP International Conference on Digital Forensics* (pp. 291-300). Springer, Berlin, Heidelberg.

Tassone, C., Martini, B., Choo, K. K. R., and Slay, J. (2013). Mobile device forensics: A snapshot. *Trends and Issues in Crime and Criminal Justice*, (460), 1.

Turnbull, B., Taylor, R., and Blundell, B. (2009, March). The anatomy of electronic evidence–Quantitative analysis of police e-crime data. In *2009 International Conference on Availability, Reliability and Security* (pp. 143-149). IEEE.

Walden, I. (2014). Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent. *Queen Mary School of Law Legal Studies Research Paper No. 74/2011*.

Wilson, J. S. (2007). Myspace, your space, or our space-new frontiers in electronic evidence. *Or. L. Rev.*, *86*, pp. 1201-1240.

Yan, W. Q., Wu, X., & Liu, F. (2018). Progressive scrambling for social media. *International Journal of Digital Crime and Forensics (IJDCF)*, *10*(2), 56-73.

Appendix I

Acts of Parliament

***Computer Misuse Act 1990. c.18*.**
Available at: https://www.legislation.gov.uk/ukpga/1990/18/contents

Criminal Justice Act 2003. c.44.
Available at: https://www.legislation.gov.uk/ukpga/2003/44/contents

Criminal Justice and Police Act 2001. c.16.
Available at: *https://www.legislation.gov.uk/ukpga/2001/16/contents*

Criminal Procedures and Investigations Act 1996. c.25.
Available at: *https://www.legislation.gov.uk/ukpga/1996/25/contents*

Data Protection Act 2018. c.12
Available at: https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

Digital Economy Act 2017. c.30.
Available at: https://www.legislation.gov.uk/ukpga/2017/30/contents

Electronic Communications Act 2000. c.7.
Available at: https://www.legislation.gov.uk/ukpga/2000/7/contents

Human Rights Act 1998. c.42.
Available at: https://www.legislation.gov.uk/ukpga/1998/42/contents

Investigatory Powers Act 2016. c.25.
Available at: https://www.legislation.gov.uk/ukpga/2016/25/contents

Police Act 1997. c.50.
Available at: https://www.legislation.gov.uk/ukpga/1997/50/contents

Police and Criminal Evidence Act (PACE) 1984. c.60.
Available at: https://www.legislation.gov.uk/ukpga/1984/60/contents

Policing and Crime Act 2017. c.3.
Available at: https://www.legislation.gov.uk/ukpga/2017/3/contents

Police, Crime, Sentencing and Courts Act 2022.c.32.
https://www.legislation.gov.uk/ukpga/2022/32/contents/enacted

Regulation of Investigatory Powers Act (RIPA) 2000. c.23.
Available at: https://www.legislation.gov.uk/ukpga/2000/23/contents

Serious Crime Act 2015. c.9.
Available at: https://www.legislation.gov.uk/ukpga/2015/9/contents

Endnotes

[1] Schatz, B. L. (2007). *Digital evidence: representation and assurance* (Doctoral dissertation, Queensland University of Technology).
[2] Browning, John G. "Digging for the digital dirt: Discovery and use of evidence from social media sites." *SMU Sci. & Tech. L. Rev.* 14 (2010): 465.
[3] Lindsey, T. (2006). Challenges in digital forensics. In The Digital Forensic Research Workshop (DFRWS), New York; Mohay, G. (2005, November). Technical challenges and directions for digital forensics. In First International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE'05) (pp. 155-161); and Casey, E. (2005). Digital arms race-The need for speed. Digital Investigation: The International Journal of Digital Forensics and Incident Response, 2(4), 229-230.
[4] To Catch a Sex Offender, *Panorama, Channel 4*, 15th August 2020. https://www.channel4.com/programmes/crime-and-punishment/on-demand/64655-007
[5] Forensic investigation processes described by Hershensohn, (2005); Ryder, (2002); Yeager (2006), detailed in Ami-Narh, J. T., and Williams, P. A. (2008). Digital forensics and the legal system: A dilemma of our times. In Australian digital forensics conference March 2008 (p. 41).
[6] For example, see Asinari, M. V. P. (2004). Legal constraints for the protection of privacy and personal data in electronic evidence handling. International Review of Law, Computers and Technology, 18(2), 231-250.
[7] Attorney General (2013). Attorney General's guidelines on disclosure for investigators, prosecutors and defence practitioners.
[8] Crown Prosecution Service (CPS) (2018). Disclosure Manual.
[9] Forensic Science Regulator (FSR) (2021). Codes of Practice and Conduct for Forensic Science Providers and Practitioners in the Criminal Justice System (Issue 4). Birmingham: FSR.
[10] Forensic Science Regulator (FSR) (2020). Guidance: Expert Report Guidance FSR-G-200 Issue 3. Birmingham: FSR.
[11] See https://www.iso.org/standard/66912.html for further details.
[12] ACPO (2012). Good Practice Guide for Digital Evidence https://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf
[13] Horsman, G. (2020). ACPO principles for digital evidence: Time for an update? Forensic Science International: Reports Vol 2 100076.