1

The sources and characteristics of electronic evidence and artificial intelligence

Steven J. Murdoch, Daniel Seng, Burkhard Schafer and Stephen Mason

1.1 Given the ubiquity of electronic devices and the evidence that they produce, lawyers are required to offer appropriate advice to clients in relation to data in electronic form. Trying to persuade lawyers that they need to keep up to date with technology is far from new.[1] In 1904, judges and lawyers were urged to make themselves aware of photography because 'they might otherwise accept what appears to be pure untouched work as reliable which was all the time outrageously worked on'.[2] And in 1959, an academic noted that 'hundreds of important cases involving disputed typewriting have been tried but there are still lawyers here and there who apparently have never heard of them and courthouses where a disputed typewriting has never been considered'.[3] Although written more than 60 years ago, the statement is undoubtedly still true today in many jurisdictions.

1 For instance, the observations by Hallett LJ in the case of *R. v Hallam (Sam)* [2012] EWCA Crim 1158, [2012] 5 WLUK 518 illustrate the failure to understand that a proper forensic investigation requires the use of the correct equipment, otherwise evidence will be tainted and therefore subject to being rejected by a trial judge – for which, see a more detailed discussion below.

2 'Photographs as Evidence' (1904) 66 ALJ 17.

3 Winsor C. Moore, 'The questioned typewritten document' (1959) 43(4) Minn L Rev 727, 727–728 n 3.

1.2 Electronic evidence and computer forensics are relatively recent additions to the means of proof in legal proceedings. Unlike many older forensic disciplines that were often introduced into the trial process with little or no legal debate and scrutiny, electronic evidence has caused considerable, and often controversial, discussion among legal professionals. Different legal systems have reacted in various ways to this new challenge.[1] Some systems have introduced new legislation to specifically address electronic evidence. Other systems try to establish a 'closest match' to existing evidentiary concepts and have applied wherever possible existing rules analogously: for instance, whether electronic evidence was admissible depended on whether it was similar to proof by (paper) document or proof by visual inspection. Most systems adopt a combination of both strategies. Where new legislation is introduced, the emphasis is on the differences between electronic and traditional forms of evidence. This can prevent lawyers from utilizing their collective institutional experience in evaluating and interpreting such evidence, often creating a sense of confusion and uncertainty. Where analogous approaches are used, the emphasis is on the similarities between traditional and digital evidence. Although this permits lawyers to draw on their experience in assessing the strength of the competing narratives that are argued by the parties, this can result in the inappropriate application of evidentiary rules. In

Steven J. Murdoch, Daniel Seng, Burkhard Schafer and Stephen Mason, 'The sources and characteristics of electronic evidence and artificial intelligence', in Stephen Mason and Daniel Seng (eds.), *Electronic Evidence and Electronic Signatures* (5th edn, University of London 2021) 1–50.

either case, it is important for lawyers to be aware of the distinctive characteristics of electronic evidence to enable them to confidently and reliably evaluate its use.

1 See Stephen Mason (ed), *International Electronic Evidence* (British Institute of International and Comparative Law 2008) for the outline of the following jurisdictions: Argentina, Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Egypt, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Italy, Japan, Latvia, Lithuania, Luxembourg, Malta, Mexico, Netherlands, Norway, Poland, Romania, Russia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Thailand and Turkey.

1.3 Various devices are capable of creating and storing data in digital form, and such data may serve as evidence. The aim of this chapter is to introduce the reader to the technologies, their underlying principles and the general characteristics that set evidence in digital form apart from evidence in analogue or physical form. The content of this chapter does not deal with any of these matters in depth. Neither does it aim to be a comprehensive review of the devices and technologies that create electronic evidence. Rather, the aim is to provide a broad brush introduction to the relevant technical issues, and to highlight features that a digital evidence professional and a legal professional should be concerned about when investigating electronic evidence and dealing with electronic evidence issues.

Digital devices

1.4 Historically, the term 'computer' was often used to describe almost any form of processing unit. Now, digital computation and storage facilities are characteristic of many devices that seem far removed in form and function from traditional computers. Such devices include games consoles, wearable technologies (such as fitness trackers and smart watches) and 'smart' domestic components (such as smart energy meters and automated central heating systems). Most of these digital devices share important features with more recognizably conventional computing devices such as desktop computers, laptops and computer tablets. These features are based on what is sometimes called an input–processing–output model:

> The device receives an *input* of some sort, by way of a local file, sensor, mouse, keyboard or through a communication channel (such as a network connection).
>
> It *processes* the information.
>
> It produces an *output* to a display, local file or printer, for instance.
>
> It must be able to *store* (and/or relay) information.
>
> It must be able to *control* what it does.

1.5 In the following, we detail the role played by the main components of digital devices.

Processors

1.6 The digital device contains one or more processors, each of which varies in the extent to which it is dedicated to a specific task. An example of a highly specific processer is one responsible for efficiently moving data between the network and the digital device, such as the network interface controller (NIC) chip. Another specific processor is the trusted platform module (TPM), responsible for certain tasks related to securing the digital device. In contrast, the main processor of a digital device, also

called the central processing unit (CPU), is not designed with any specific purpose and is the functional core constituent of every such device. Sitting somewhere between highly specialized (such as a TPM) and highly generic (for example, a CPU) is a graphical processing unit (GPU). As the name suggests, a GPU is designed to display complex and fast-moving 2D and 3D graphics. In recent years GPUs have become more capable and are now able to perform certain tasks more efficiently than CPUs, notably machine-learning tasks. Each processor is itself made up of a number of constituent parts. Together, these parts receive data, perform logical or arithmetic operations and output the results. The results are passed to another processor, a local storage facility or a display unit, or 'uploaded' via a network connection to another device.

Mobile devices

1.7 Hand-held devices are now ubiquitous. These include tablets and smartphones that combine personal computer functionality with telephone and camera capabilities. Such devices are computers, since they have one or more processors, memory, a keypad or mouthpiece (input), and a screen or earpiece (output). Like computers, hand-held devices have volatile and non-volatile memory. The non-volatile memory stores the system software and application software, and the user's data. The volatile memory is used by software to store data that is currently being worked on. (A more detailed discussion of memory and storage follows.) While data that is stored in volatile memory will be lost when the device loses power, turning 'off' a hand-held device usually places the device in a mode that uses a small amount of power to retain data in volatile memory and enables it to continue with essential tasks. Non-volatile memory in modern devices will usually be flash memory, a form of solid-state memory chip that is capable of retaining content without power. Other types of specialist mobile device include digital music players and ebook readers that can use wireless technology to download large volumes of data from a main computer.

1.8 All these devices, together with laptop computers, are increasingly used by organizations as components in an extended information technology infrastructure. Where relevant, such devices may be investigated for electronic evidence, although the amount of information that can be obtained will vary. For instance, while one may find only a list of the most recent telephone numbers called from an ordinary mobile telephone, a smartphone will probably yield substantial amounts of data, including emails and other data from a network that might aid an investigation.

1.9 The examples given above emphasize the types of electronic evidence that can be revealed by means of a forensic examination, including hidden or deleted data. Only a highly skilled person could remove all traces of evidence on a digital device, and such skills are very rare. Some forensic techniques exist that can recover data even when it has been strictly overwritten on disk. Whether these techniques will be used or implemented will depend on the type and value of the data sought to be recovered.

Embedded devices

1.10 The ubiquity of the microprocessor has led to the increasing use of embedded devices. An embedded device or embedded system is a computer system in its own

right that combines a processor, memory, and input and/or output peripheral devices to execute a dedicated function within a larger mechanical or electrical system. The three functions – processor, memory and peripheral interfaces – may in turn be combined into a specialized or dedicated microprocessor known as a microcontroller. Unlike multitasking computers, embedded devices typically handle one highly specialized task, but can be combined with other similar devices to form highly complex structures, such as the different embedded devices that together enable an autonomous car to drive. Embedded devices control many systems in common use today,[1] and have consumer, industrial, automotive, home appliance, medical, telecommunications, commercial and military applications.[2] These include, among other things, white electronic goods, burglar alarms, industrial robots, spectrometers and neutron transmission monitors,[3] breath alcohol intoximeters,[4] radar devices,[5] traffic control systems[6] and hotel telephone call-billing systems. Consequently, any evidence produced using or generated by any of these devices is electronic evidence.[7] The versatility and range of these Internet of Things devices means that data from embedded systems is a rapidly increasing source of data.

1 Around 98 per cent of all microprocessors produced each year are used in embedded devices. See Michael Barr, 'Real men program in C', Embedded, 1 August 2009, https://www.embedded.com/real-men-program-in-c/.
2 Embedded system (Wikipedia), https://en.wikipedia.org/wiki/Embedded_system#Applications.
3 *R v Wood (Stanley William)* [1982] 6 WLUK 191, (1983) 76 Cr App R 23, [1982] Crim LR 667, [1983] CLY 636; *PP v Ang Soon Huat* [1990] 2 SLR(R) 246.
4 *Castle v Cross* [1984] 1 WLR 1372, [1985] 1 All ER 87, [1984] 7 WLUK 180, [1985] RTR 62, [1984] Crim LR 682, (1984) 81 LSG 2596, (1984) 128 SJ 855, [1985] CLY 3048.
5 *The Statue of Liberty Owners of Motorship Sapporo Maru v Owners of Steam Tanker Statue of Liberty* [1968] 1 WLR 739, [1968] 2 All ER 195, [1968] 1 Lloyd's Rep 429, [1968] 3 WLUK 65, (1968) 112 SJ 380, [1968] CLY 1546.
6 By way of example, see Thomas Novak and Christoph Stoegerer, 'Embedded system platform for safety-critical road traffic signal applications' in Friedemann Bitsch, Jérémie Guiochet and Mohamed Kaâniche (eds) *Computer Safety, Reliability, and Security*, 32nd International Conference, SAFECOMP 2013, Toulouse, France, 14–27 September, Proceedings (Springer 2013), 138–145.
7 Daniel Seng, 'Computer output as evidence' [1997] SJLS 130, 135–137, 173–175.

1.11 From a forensic perspective, particularly problematic types of embedded device are medical or similar devices that are embedded in biological bodies, sometimes in humans – in the form of intelligent pacemakers – but also sometimes in other animals.[1] Both are sometimes collectively referred to as examples of the 'Internet of Bodies', in juxtaposition to the Internet of Things.[2] For obvious reasons, collecting evidence from these devices while the host is still alive poses significant legal, ethical and technological challenges.

1 https://expmag.com/2020/06/health-tracking-implants-can-create-bionic-cows-are-humans-next/.
2 Andrea M. Matwyshyn, 'The Internet of Bodies' (2019) 61 Wm & Mary L Rev 77.

1.12 Data from embedded devices can have a high level of forensic relevance. These systems regularly operate in autonomous ways and collect data (sometimes including video or audio data) without the need for human intervention. Furthermore, the user or owner will often have only very limited ways to obtain access to, delete or manipulate the data on these devices. If the system in which these devices are embedded is mobile, they will regularly generate geolocation data that can help locate the user and reveal their activity at a specific moment in time. Embedded devices

also pose investigative challenges;[1] sometimes, knowledge of the characteristics of the hardware and the surrounding environment are needed to correctly access and interpret the data on these devices. The diversity of the types of device available and their proprietary nature, which will be protected by trade secrets, can make it difficult to establish general protocols and methods.

1 Ronald Van der Knijff, 'Embedded systems analysis' in Eoghan Casey (ed) *Handbook of Digital Forensics and Investigation* (Academic Press 2010), 383–435.

1.13 Data preservation in embedded systems poses particular challenges. It will not always be obvious if embedded systems are switched on or off, which other components of a particular system they are connected to, or if those components can change the data on the target device. For example, carrying an object with an embedded device from a crime scene to a police station can cause a change in geolocation data through the mere act of movement. Sometimes, extraction of the device or its chips will be impossible or overly expensive, and sometimes it is not possible to switch off the device without risking harm to others (as with a traffic control system).

Software

1.14 Software consists of programs that give instructions to the digital device. There are three main categories of software: firmware, system software and application software.

Firmware

1.15 Firmware is software that is highly specialized to the component that it controls, and will usually be written by the same organization that produces the hardware component. Firmware may be stored on the component itself or may be stored as part of the system software and loaded onto the component when the digital device is switched on. Firmware is responsible for controlling the component and its interaction with other components that are part of the digital device.

System software

1.16 As the name suggests, system software is required for the basic operation of a device. The set of software programs that manage the basic operation of a digital device is called the operating system. The operating system controls the flow of data, allocates memory and manages any hardware components of the device, such as the display, input device(s), network interaction, etc. The operating system also permits the user to manage any user-specific files, enabling multiple users to share the use of the digital device, and acts as an interface between the hardware and the application software.

Application software

1.17 Broadly speaking, for more traditional computing devices such as desktop computers, smartphones, laptops and tablets, the application software (or 'apps' as they are also known) provides the user-facing side of the system. This is 'special purpose' software that enables the user to undertake specific kinds of tasks on the

computer. These include word processing, desktop publishing, web browsing, emailing, social networking, preparing and delivering presentations, performing complex sets of numerical calculations, among others. Examples of application software include Microsoft Word, Outlook, PowerPoint, Excel, Chrome and LibreOffice. These and other application programs represent the main reasons for which most people use computers and smart mobile devices (that is, to perform specific tasks, which are made simpler by means of the computer and its application software). For other digital devices, the user may only engage the application software through a limited range of functions, such as status checks on a fitness tracker or energy consumption on a smart meter.

The clock

1.18 One further component must be discussed in relation to the operation of digital devices: the clock. The clock serves two functions:

> (1) It is a device that produces pulses of electrical signals that oscillate between a high state and a low state to ensure that events are synchronized and occur in a predictable order. The clock coordinates all the components of the device, including the processor and other digital circuits. Each step in any operation must follow in sequence, although some operations run at different speeds. All parts of the circuit are synchronized to the pulses of the electronic clock. The frequency of pulses is controlled by a phase locked loop (PLL), which, in turn is regulated by a quartz crystal. The speed at which the crystal oscillates, the step-up ratio of the PLL and the number of steps that each instruction requires will determine the speed at which the computer operates.
>
> (2) Also known as a real-time clock, RTC or system clock, the clock also often serves to keep the time of day and date in a human sense. Larger computer systems synchronize their clocks with a reliable time source available over the Internet, using a system interface such as the Network Time Protocol. This allows devices attached to the Internet to synchronize their time settings (taking into account geographical locations and time zones) with Internet time servers. There are two important reasons to provide for the synchronization of time. The first is to ensure that events occur on time, and in the correct sequence. This permits events to be scheduled and enables the fact that they have occurred to be registered accurately. The second is to enable the retrieval of information concerning past events, including establishing when the events occurred and the sequence in which they occurred. This is only possible if accurate time stamps are available. Examples include the time-stamping mechanism relating to authentication, digital signatures and the diagnosis of faults recorded on system event logs. Likewise, email systems and other messaging systems generally time-stamp messages using Coordinated Universal Time, so that the client email system can display the date and time of the message using the client's local time zone.

1.19 In most implementations the built-in real-time clock is powered by a battery and runs continuously even when the device is switched off. Devices that have lain for a long time without being powered on may not 'boot up' when they are switched on, because the battery has run down and may require recharging or replacing. We should also note that the clock in digital devices is often imprecise. Usually, the clock can be adjusted (and even incorrectly set) manually. This can result in the system clock being

slightly incorrect (through 'drift' in timekeeping) relative to the actual time in the local region. Such inaccuracy may affect uses of the clock for event scheduling and logging, since both aspects may depend on the time as derived from the system clock. Where the accuracy of time is important, the clock usually requires occasional adjustment to bring the time back into line with better reference sources (such as Internet time servers). This is a matter of some significance, since unquestioned and out-of-context assumptions about the accuracy or otherwise of a clock may result in a misleading conclusion.

Time stamps

1.20 From the perspective of electronic evidence, the system clock often plays a vital role in time-stamping events. For instance, the operating system uses the date and time settings to annotate its record of events such as the creation or modification of a file. In computers, such information is often referred to as file 'metadata' (the data that describes or interprets the base data), since the date and time information is associated with the file, but is not part of the data in the file or data that the user has any direct control over. Time stamps are also recorded against system events such as user logins, password changes and – depending on the purpose of the device – sensor-recorded events such as the number of steps walked by the device wearer and the wearer's pulse rate. The time and date information associated with such events is recorded in system log files (event logs). Such logs are often an important source of event sequence information and afford insights on purported specific user activity.

1.21 As noted earlier, the system clock in a computer can be set by the user and may not be configured to maintain the correct current time (such as by using the Network Time Protocol). Incorrect time settings will be reflected in the date and time stamps subsequently recorded by the system. Obviously, this potential anomaly must be considered when dealing with data that is time-stamped. Since the time zone is also set in the system, an incorrect choice of zones may result in an incorrect current date or time. In addition, because of the critical role the clock plays, it features a great deal in electronic evidence, particularly where it is manipulated by the defendant to hide changes made to critical evidence.[1]

1 Chet Hosmer, 'Proving the integrity of digital evidence with time' (2002) 1(1) Intl J of Digital Evidence; Chris Boyd and Pete Forster, 'Time and date issues in forensic computing – a case study' (2004) 1(1) Digital Investigation 18; Malcolm W. Stevens, 'Unification of relative time frames for digital forensics' (2004) 1(3) Digital Investigation 225.

Memory and storage

1.22 In order to retain programs, output results and other data on which programs operate, digital devices rely on storage. There are generally speaking two forms of storage: primary storage and secondary storage. Primary storage is storage that is directly accessible by the processor. In general, this takes the form of semiconductor memory, such as:

> (1) An internal storage chip known as *random access memory* (RAM).[1] This chip is capable of repeatedly storing (writing) and retrieving stored data (reading) at very high speeds.

(2) An internal storage chip that is capable of storing data once, but does not allow the data to be rewritten. Once data has been entered, this type of chip only allows the data to be read. This is called *read-only memory* (ROM).[2]

(3) An internal storage chip that stores data and behaves as a ROM during its normal operation, but permits data to be erased and replaced. This form of device is known as *erasable programmable read-only memory* (EPROM).[3] A flash ROM is a type of EPROM.

1 Random-access memory (Wikipedia), https://en.wikipedia.org/wiki/Random-access_memory.
2 Read-only memory (Wikipedia), https://en.wikipedia.org/wiki/Read-only_memory.
3 EPROM (Wikipedia), https://en.wikipedia.org/wiki/EPROM.

1.23 Secondary storage is storage that is not directly accessible by the processor. Where data on which it is stored is required, the processor will use its input/output channels to obtain access to the secondary storage and transfer the required data into the primary storage. Unlike RAM, secondary storage is non-volatile: it retains its data when the device is powered down. Hard disk drives (HDDs), solid-state drives (SSDs) and Universal Serial Bus (USB) 'thumb drives' used as storage media are typical forms of secondary storage. They may be permanently attached to the computer (internal storage) or attached when required (external storage). Other forms of external storage may be less proximal to the computer, such as network-attached storage (NAS),[1] tape drives or 'cloud' storage. Because secondary storage is non-volatile, the hard disk and associated offline storage media are a significant source of electronic evidence for a device. But the fact that primary memory such as RAM is volatile does not mean that its data cannot be retrieved. An experiment on 'freezing' RAM chips before physical removal and transfer to a different computer revealed an unusual context in which it was possible to recover RAM data from the treated chips.[2]

1 Network-attached storage (Wikipedia), https://en.wikipedia.org/wiki/Network-attached_storage.
2 J. Alex Halderman, Seth D. Schoen, Nadia Heninger, William Clarkson, William Paul, Joseph A. Calandrino, Ariel J. Feldman, Jacob Appelbaum and Edward W. Felten, 'Lest we remember: cold boot attacks on encryption keys' in *Proceedings of the 17th Conference on Security Symposium* (USENIX Association 2008); and (2009) 52(5) Communications of the ACM 91, https://www.usenix.org/legacy/event/sec08/tech/full_papers/halderman/halderman.pdf.

Data storage facilities

1.24 The increasingly varied methods of storing digital data and the variety of storage contexts mean that locating relevant data as prospective evidence may not be a simple matter. Data may be stored locally on a computing device, such as on hard disks, DVDs or CDs, flash drives, memory sticks or micro memory devices (commonly found in smartphones). But data may also be stored remotely on NAS, remote networks or 'cloud' facilities. Of concern to many digital investigators is the difficulty inherent in locating and obtaining legal access to data that is stored remotely from an individual's computer.

1.25 A further level of complexity has developed since 2009 with a significant increase in distributed data storage. A well-known example is blockchain. In these approaches to data storage, distributed ledgers are maintained across a considerable number of machines (the 'nodes'). Replicating data on such a scale provides for the

quality of the data and makes the storage medium particularly resilient to attacks directed against availability and integrity. Authenticity of the copies at each node are provable through computation, creating a system of 'computational trust' in which no node has priority over another. The inherent transparency of the blockchain and similar decentralized data storage technologies offers advantages in forensic investigations.[1] However, the use of encryption can also pose challenges. From a legal perspective, the decentralized nature of the storage causes similar problems to cloud computing when it comes to questions of applicable jurisdiction, while concepts such as computational trust and data replication pose further challenges to traditional evidential concepts such as the original/copy dichotomy.[2]

1 Blockchain technology was accepted as a means of authentication in China in the case of *Hangzhou Huatai Yimei Culture Media Co., Ltd. v Shenzhen Daotong Technology Development Co., Ltd*. (2018) Zhe 0192 Civil Case, First Court No. 81, Hangzhou Internet Court of the People's Republic of China, translated by Dr Jiong He, Digital Evidence and Electronic Signature Law Review (2019) 16, 61–70.

2 Joseph Ricci, Ibrahim Baggili and Frank Breitinger, 'Blockchain-based distributed cloud storage digital forensics: where's the beef?' (2019) 17(1) IEEE Security & Privacy, 34–42; S. Naqvi, 'A126: Challenges of cryptocurrencies forensics: a case study of investigating, evidencing and prosecuting organised cybercriminals' in *ARES 2018: Proceedings of the 13th International Conference on Availability, Reliability and Security* (27 August–30 August 2018), 1–5, http://www.open-access.bcu.ac.uk/6093/1/Challenges%20of%20cryptocurrencies%20forensics.pdf.

1.26 The common data storage contexts are summarized in the table below.

Memory type	**Volatile**	**Local**
RAM	Yes	Yes
HDD (internal) SSD (internal)	No	Yes
HDD (portable) SSD (portable)	No	Perhaps
Flash/USB	No	Perhaps
CD/DVD	No	Perhaps
Network	No	Perhaps
Cloud	No	Typically No

Data formats

1.27 Digital data may be broadly classified into binary data, where the information is represented in binary form, and text data, including alpha, numeric and punctuation data. Text can be entered into the computer by a range of methods:

(i) The typing of letters, numbers and punctuation, mainly when using a keyboard.

(ii) Scanning a page with an image scanner and converting the image into data by using optical character recognition (OCR)[1] software.

(iii) Using a bar code. The bar code represents alphanumeric data and is read with an optical device called a wand or scanner. The scanned code is converted into binary signals, enabling a bar code translation component to read the data.

(iv) Reading the magnetic stripe on the back of a credit card.

(v) Using voice data, where a person speaks into a microphone capable of recording the sounds. This form of data, as well as video data, is encoded in binary form.

(vi) Converting from speech to text. Here, the user speaks into a microphone that is connected to the computer and a dedicated software application analyses the input signal and converts this to a textual representation of the spoken words.

1 Optical character recognition (Wikipedia), https://en.wikipedia.org/wiki/Optical_character_recognition.

1.28 To enable a user to view text and numbers, and to see images or hear sound, the binary form of the data must be converted using a code. Computers manipulate binary (base 2) information, but for human convenience it is more common to represent computer numbers in the octal (base 8) or hexadecimal (base 16) system. A range of codes exists to represent text data in numerical form (to enable machine processing).[1] Some of the codes in common use are the American Standard Code for Information Exchange (ASCII),[2] Extended Binary Code Decimal Interchange Code (EBCDIC),[3] Unicode Transformation Format–8 (UTF-8)[4] and Unicode Transformation Format-16 (UTF-16).[5] UTF-8 and UTF-16 are capable of encoding the characters standardized by the Unicode Consortium, including all commonly used characters in currently spoken languages, but the two standards differ in how text data is represented in binary form. Computers running Microsoft Windows commonly use ASCII and UTF-16, and most others use ASCII and UTF-8. EBCDIC is commonly found on IBM mainframe computers and some applications designed for such systems, particularly banking software. Tools are available to display binary data used in computers to enable a digital investigator to view features that are normally not visible to the computer user. For instance, documents stored in the Microsoft Word format contain application metadata that are normally not visible. By using certain types of software program, a digital evidence professional is able to view all aspects of the data and such data may reveal crucial information that may help an investigation.

1 Character encoding (Wikipedia), https://en.wikipedia.org/wiki/Character_encoding.
2 ASCII (Wikipedia), https://en.wikipedia.org/wiki/ASCII; Vinton Cerf, 'RFC 20 – ASCII format for Network Interchange' (Internet Engineering Task Force, 16 October 1969), https://tools.ietf.org/html/rfc20.
3 EBCDIC (Wikipedia), https://en.wikipedia.org/wiki/EBCDIC; J. M. Winett, 'RFC 183 – The EBCDIC Codes and Their Mapping to ASCII' (Internet Engineering Task Force, 21 July 1971), https://tools.ietf.org/html/rfc183; R. T. Braden, 'RFC 338 – EBCDIC/ASCII Mapping for Network RJE' (Internet Engineering Task Force, 17 May 1972), https://tools.ietf.org/html/rfc338.
4 UTF-8 (Wikipedia), https://en.wikipedia.org/wiki/UTF-8; F. Yergeau, 'RFC 3629 – UTF-8, a transformation format of ISO 10646' (Internet Engineering Task Force, November 2003), https://tools.ietf.org/html/rfc3629.
5 UTF-16 (Wikipedia), https://en.wikipedia.org/wiki/UTF-16; P. Hoffman and F. Yergeau, 'RFC 2781 – UTF16, an encoding of ISO 10646' (Internet Engineering Task Force, February 2000), https://tools.ietf.org/html/rfc2781.

Starting a computer

1.29 Every time a digital device is switched on, various components must interact with each other for it to begin working. This is called the start-up process or 'booting' the system. Most devices have a program stored in the non-volatile memory called

variously a boot loader, boot process, boot strap or initial program load. It is this program that enables the system to start. In general terms, this is how it works:

> (1) When the system is powered on, control is first transferred to the bootstrap loader, bootstrap or boot loader.[1] On a PC, this is sometimes known as the basic input and output system (BIOS),[2] a small program located permanently in the non-volatile memory of the device.
>
> (2) The boot loader tests the various components of the system, verifying that they are active and working. The results of the various tests it carries out may appear on the system output. The boot process can also clear local primary memory of all historical data and metadata. It then loads up a second-stage boot loader which it has found on booting the device (a non-volatile storage device) to continue the start-up process. On a PC, the BIOS locates the first (or default) secondary storage device, looks for an operating system on the storage device and passes control to the operating system's boot record (a set of instructions starting at a specific location on the storage device).
>
> (3) The second-stage boot loader takes control of the system. It loads and tests the configuration of the device before loading the operating system.
>
> (4) Finally, the operating system will display any startup dialogue (for instance, the identity of the mobile telephone service provider) and, if the user is authorized (for instance, by providing a code), grant access to application-level programs. The user can then take control of the device through an application.

1 Booting (Wikipedia), https://en.wikipedia.org/wiki/Booting.
2 BIOS (Wikipedia), https://en.wikipedia.org/wiki/BIOS.

Networks

1.30 Gone are the days when most computers stood alone on a desk. The majority of computers are now connected, or are intermittently connected, to other computers or a network. Given the trails left by the assortment of logs and files in computers, going online can produce electronic evidence in abundance, including the use of email, connection to the Internet and the websites viewed, and the transfer of files between computers. Other sources of electronic evidence can be obtained from server logs, the contents of devices connected to the network and the records of traffic activity. In many instances, even if a digital device has been destroyed or disposed of, relevant evidence may still be retrieved through the network to which the device has been connected.

Types of network

The Internet

1.31 The Internet was developed from its precursor, the ARPANET, which was created in 1969 to facilitate collaboration between research institutions, initially within the US and then later internationally. A wide range of applications have been developed to make use of the Internet, but the introduction of the World Wide Web in 1989, which provides a relatively easy-to-use way to share information, contributed to the dramatic growth of the Internet. When a digital device connects to the Internet, it uses a set of protocols called Transmission Control Protocol/Internet Protocol (TCP/IP).[1] This set of communication standards can be regarded as a common language that enables various

types of network to communicate, each with the other. A digital device connected to a network is referred to as a 'host'. The device uses a modem or an NIC[2] to send and receive information, although medium-sized and large organizations will have a Local Area Network (LAN)[3] gateway to the Internet. Application software running on hosts provides services to users, building on the functionality that TCP/IP provides. The network itself does not have any knowledge of what the application is doing – only the application software running on the hosts at the ends of the connection interprets the data being carried over the network. This, called the end-to-end principle, is desirable because new Internet applications can be created without having to request the permission of the organizations running the network. Similarly, application software need not be concerned with the details of how the network transfers data from one end of the communication to another, and so networks may change the way they work provided they still preserve the functionality that applications expect.

1 Internet protocol suite (Wikipedia), https://en.wikipedia.org/wiki/Internet_protocol_suite; Vinton Cerf, 'RFC 675 – Specification of Internet Transmission Control (Internet Engineering Task Force, December 1974), https://tools.ietf.org/html/rfc675; F. Baker, 'RFC 1812 – Requirements for IP Version 4 Routers' (Internet Engineering Task Force, June 1995), https://tools.ietf.org/html/rfc1812.
2 Network interface controller (Wikipedia), https://en.wikipedia.org/wiki/Network_interface_controller.
3 Local area network (Wikipedia), https://en.wikipedia.org/wiki/Local_area_network.

1.32 A further component of the modern communication infrastructure is the server. These are hosts that run application software, but rather than providing a service to the individual sitting in front of the computer, they provide a range of customers with a service over the network, for instance hosting an organization's web service or email facility. Some servers permit anyone to obtain access to their resources without limitation. Other servers restrict access to some resources to authorized users only, usually by means of a username and password. Sources of electronic evidence from servers include the data necessary to provide the web service hosted by the servers, as well as the logs recording when a user connects to a server, whether to get access to the Internet or to download email.

IP addresses

1.33 The purpose of an Internet Protocol (IP) address is to identify a particular device connected to the Internet. Each unit of data (packet) sent over the Internet includes the IP address of the device for which the packet is intended (the destination). The devices responsible for directing packets to the correct destination (routers) use this destination IP address to make decisions on how best to dispatch packets. Routers may also be responsible for filtering traffic that is not permitted and keeping logs of activity. Packets also contain the IP address allocated to the device that sent the packet (the source), to allow that packet to be replied to. IP addresses currently in use take one of two forms: version 4 (IPv4), for example 198.51.100.42, and version 6 (IPv6), for example 2001:0db8:85a3:0000:0000:8a2e:0370:7334. For a device to be able to communicate over the public Internet directly, that device needs to be allocated a public IP address. Each public IP address should be allocated to at most one device worldwide. If two or more devices are allocated the same public IP address, then problems are likely to occur, so network providers put in place technical and procedural controls to prevent this occurring.

1.34 IP addresses may also be private. Such IP addresses are allocated to devices which do not directly connect to the Internet. Devices allocated a private IP address may only communicate with the public Internet via an intermediary which has been allocated a public IP address. There are many devices worldwide, each allocated a private IP address, but packets with a source or destination IP address that is private should not be sent over the public Internet. Network providers also have in place technical and procedural controls to prevent this occurring.

1.35 There are just over 4 billion possible IPv4 addresses, and far more IPv6 addresses.[1] To ensure that no two devices are allocated the same public IP address, IP addresses are distributed by a central organization: the Internet Assigned Numbers Authority (IANA). IANA delegates large groups of IP addresses to regional authorities, which in turn delegate smaller groups of IP addresses to network operators. For example, the regional authority for Europe is Réseaux IP Européens (RIPE), the regional authority for North America is the American Registry for Internet Numbers (ARIN) and the regional authority for the Asia Pacific region is the Asia Pacific Network Information Centre (APNIC). Information about which network operator is responsible for a particular group of IP address is listed in a WHOIS database maintained by the relevant regional authority. Public IP addresses are frequently used to attribute behaviour to individuals, but IP addresses identify Internet-connected devices, not people. There are three main ways in which one IP address can correspond to multiple people, all of which may occur simultaneously.

1 Specifically, 340,282,366,920,938,463,463,374,607,431,768,211,456 or approximately 3 followed by 38 zeros.

1.36 First, the operator of a network may allocate a given public IP address to different devices at different points in time. This scheme of IP address allocation is known as dynamic allocation. The period of time for which an IP address is dynamically allocated to a given device could be anything from a few hours to a few months. An alternative scheme of IP address allocation is static allocation, where the network operator allocates the same IP address to a particular device, if that is feasible. Even if static allocation is used, there may still be changes in which a device is allocated a particular IP address for operational reasons.

1.37 Second, the operator of a network may allocate private IP addresses to a group of devices, then connect these devices to the public Internet via an intermediary device with a single public IP address. From the perspective of the public Internet, all devices within this group will share the same IP address. This configuration is common for a home network: all devices within the home have private IP addresses, and the home router performs Network Address Translation (NAT) to allow all these devices to share the single public IP address allocated to the home router. In addition, operators of mobile networks (carriers) commonly use NAT to share a single public IP address between hundreds or even thousands of different customers. This scheme is known as Carrier-Grade NAT (CGN). CGN (sharing a public IP address between different customers) can be used in combination with home NAT (sharing a public IP address, which may itself be shared, with multiple devices using a home router). NAT is common for IPv4 connections because there are not enough IPv4 addresses for every device connected to the Internet to have its own address. IPv6 has more than enough addresses, but network providers may nevertheless decide to apply NAT.

1.38 Third, a single device may have multiple users – sequentially or concurrently. These multiple users may be authorized by the owner of the device or may be unauthorized (that is, they have hacked into the computer and are using it without authorization). From the perspective of the public Internet, all users of a device will share the same public IP address that the device uses to connect to the Internet (directly or indirectly). Redirecting communication via another computer is known as proxying the connection.

1.39 In summary, a single public IP address may be used by different customers at different times. At any one time, a single public IP address may be used by multiple customers (CGN). Each customer may be sharing their IP address over many devices (NAT). Each device may have many users (authorized or unauthorized), at the same time or at different times. Consequently, attributing Internet activity requires consulting a wide range of stored logs, each of which have limitations in terms of the extent that they may be relied upon.[1]

1 Richard Clayton, 'Anonymity and traceability in cyberspace', PhD thesis, University of Cambridge, November 2005, https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-653.html.

Corporate intranets

1.40 An intranet, usually run by a large organization, is a private network that in principle is only available to members and employees of the organization or others with authorization to obtain access to and use the information contained on the network. The intranet may look like a smaller version of the Internet, providing websites, mail servers and time servers among other facilities. Usually situated within the corporate firewall, an intranet is built to support the internal needs of the organization, as well as to improve workforce connectivity and business operations. As such, it generally aims to keep those outside the organization from gaining access, and is usually well protected.

Wireless networking

1.41 A further development in this form of networking is wireless technology. One implementation of wireless networking is Wi-Fi[1] (a mark used by the Wi-Fi Alliance), mainly through the 2.4 GHz and 5 GHz radio bands based on the 802.11 communications standard.[2] Another wireless technology standard, known as Bluetooth,[3] is a standard for exchanging data between devices over short distances using ultra high frequency (UHF) radio waves in the 2.402 GHz to 2.480 GHz band. From an evidential perspective, logs exist to record the use of wireless networks, affording evidence of the use that a device has made of a network.

1 Wi-Fi (Wikipedia), https://en.wikipedia.org/wiki/Wi-Fi.
2 The number 802 is the name given to the interoperability standard developed by the Institute of Electrical and Electronic Engineers for Local Area Networks and Metropolitan Area Networks, and Wi-Fi is based on 802.11, which is a subset of the 802 standard relating to wireless local area networks.
3 Bluetooth (Wikipedia), https://en.wikipedia.org/wiki/Bluetooth.

Cellular networks

1.42 A cellular network or mobile network is a communications network that enables portable devices such as cellular telephones to communicate with each other. The

network is made up of a number of cell sites (base stations) within a defined geographical area. An individual connected to a cell site can make and receive calls over the network. Each cell site is connected to a central computing infrastructure, comprising telephone exchanges or switches, which are in turn connected to the public telephone network. This infrastructure processes the calls by routing them to their destination, and retains logs for the purpose of sending out bills, maintenance and, if necessary, carrying out investigations. The most recent developments in cellular technology include General Packet Radio Services (GPRS),[1] the third generation (3G),[2] the Universal Mobile Telecommunications System (UMTS),[3] the fourth generation (4G,)[4] the Long-Term Evolution (LTE)[5] standard and the fifth generation (5G) standard,[6] developments that provide for faster transmission rates and enable applications such as mobile web access, IP telephony, gaming services, high-definition mobile TV and video conferencing. Many mobile service providers plan to introduce these new systems to replace the Global System for Mobile Communications (GSM)[7] standard, which is now considered to have exploitable security flaws.

1 General Packet Radio Service (Wikipedia), https://en.wikipedia.org/wiki/General_Packet_Radio_Service.
2 3G (Wikipedia), https://en.wikipedia.org/wiki/3G.
3 UMTS (telecommunication) (Wikipedia), https://en.wikipedia.org/wiki/UMTS (telecommunication).
4 4G (Wikipedia), https://en.wikipedia.org/wiki/4G.
5 LTE (telecommunication) (Wikipedia), https://en.wikipedia.org/wiki/LTE (telecommunication).
6 5G (Wikipedia), https://en.wikipedia.org/wiki/5G.
7 GSM (Wikipedia), https://en.wikipedia.org/wiki/GSM; H. Haverinen and J. Salowey (eds.), 'RFC 4186 – Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM)' (Internet Engineering Task Force, January 2006), https://www.ietf.org/rfc/rfc4186.txt.

1.43 A mobile telephone has several numbers that identify the device. The manufacturer includes an electronic serial number (ESN)[1] or the International Mobile Equipment Identity (IMEI)[2] number as a code to uniquely identify mobile devices. The International Mobile Subscriber Identity (IMSI)[3] number is a unique identification number, usually located in the SIM card of the telephone, to identify the subscriber of a cellular network. To prevent the subscriber from being identified, this number is rarely sent. What is sent in its place is the Temporary Mobile Subscriber Identity (TMSI),[4] which is randomly generated and assigned to the telephone the moment it is switched on to enable communications between the mobile device and the base station. Finally, the mobile identification number (MIN) or mobile subscription identification number (MSIN)[5] is the unique telephone directory number for the mobile subscription that is used to identify a telephone. It is derived from the last part of the IMSI.

1 Electronic serial number (Wikipedia), https://en.wikipedia.org/wiki/Electronic_serial_number.
2 International Mobile Station Equipment Identity (Wikipedia), https://en.wikipedia.org/wiki/International_Mobile_Station_Equipment_Identity.
3 International mobile subscriber identity (Wikipedia), https://en.wikipedia.org/wiki/International_mobile_subscriber_identity.
4 Mobility management (Wikipedia), https://en.wikipedia.org/wiki/Mobility_management#TMSI.
5 Mobile identification number (Wikipedia), https://en.wikipedia.org/wiki/Mobile_identification_number.

1.44 To ensure the telephone company knows the correct base station to which to direct the call, the position of the telephone is constantly tracked when it is switched on. Thus, there is a broad range of electronic evidence associated with the use of a mobile telephone, including where the telephone was located geographically, details

of calls made and received, and the contents of text messages.[1] Where a telephone is capable of being used in other ways, such as making micro-payments, data relating to such services are also capable of being retrieved.[2]

1 In *R v Brooker* [2014] EWCA Crim 1998 also cited as *AG's Ref: 071 of 2014, R v B (R C A) (2014)* (available on the LexisNexis database), Brooker falsely accused her former partner, Paul Fensome, of various crimes including rape and assault. Cell site analysis determined that Brooker was not at various locations as she claimed. In addition, because Mr Fensome retained all of the text messages exchanged with Brooker, it was possible to establish that the relationship between the two was not as alleged by Brooker.

2 Svein Yngvar Willassen, 'Forensics and the GSM mobile telephone system' (2003) 2(1) Intl J of Digital Evidence.

Cloud computing

1.45 Cloud computing is not new. Back in the 1960s, computer bureaus would allow companies to rent time on a mainframe as a 'time-sharing' service. With the rise of the personal computer, which made affordable computer ownership possible, it fell into relative obscurity, but became popular again in the early 2000s.[1] Today, cloud computing refers to the use of high-speed and high-capacity network access to make computer system resources available to users at any time and anywhere, without direct active management by the users – who may be individuals or corporations.[2] These resources tend to be data storage (cloud storage), computing power and applications, and are provided as service models in which the cloud computing providers offer various 'services' according to different service models, such as 'Software as a service' (SaaS), 'Platform as a service' (PaaS) and 'Infrastructure as a service' (IaaS).[3] By sharing resources among users, cloud providers bring the economies of scale to users and enable them to avoid or minimize the cost of putting IT infrastructure into place. The 'pay-as-you-go' model also offers users the ability to increase or reduce their use of the resources depending on their needs.

1 Steve Ranger, 'What is cloud computing? Everything you need to know about the cloud explained', ZDNet, 13 December 2018, https://www.zdnet.com/article/what-is-cloud-computing-everything-you-need-to-know-about-the-cloud/.

2 Cloud computing (Wikipedia), https://en.wikipedia.org/wiki/Cloud_computing.

3 See NIST (National Institute for Standards and Technology) at https://csrc.nist.gov/publications/detail/sp/800-145/final#:~:text=Cloud%20computing%20is%20a%20model,effort%20or%20service%20provider%20interaction.

1.46 When reference is made to data that is being stored 'in the cloud', it does not mean that there is no tangible form for the data. The data still has to reside on the servers that companies set up in their data centres or, as is predominantly the case, multiple data centres that are geographically distributed. This architecture is intended to improve the performance, resilience and reliability of cloud computing services, especially since the data is constantly transferred and replicated across data centres, thereby providing for data redundancy. It also raises issues of security, data ownership, confidentiality, privacy and jurisdiction,[1] because resources are always available online (and sometimes in different geographical areas) and the service provider can accidentally or intentionally obtain access to the data on its servers at any time, or use the data for unauthorized purposes.[2] This also subjects cloud service providers to court orders and warrants that mandate that they share information with third parties, which in turn behoves the use of encryption by users to protect their data stored on

the cloud. Organizations as users have also changed the way they use the cloud,[3] for instance combining cloud resources with on-premises resources (hybrid cloud) to better manage their resources. This has also affected the way electronic evidence on the cloud is located and collected for forensic purposes. A further discussion follows.

1 Miranda Mowbray, 'The fog over the Grimpen Mire: cloud computing and the law' (2009) 6(1) Scripted Journal of Law, Technology and Society 133, https://script-ed.org/archive/volume-6/issue-61-1-193/.
2 For example, see Mark D. Ryan, 'Cloud computing privacy concerns on our doorstep', Communications of the ACM (January 2011) 54(1), 36, DOI: 10.1145/1866739.1866751.
3 See NIST at https://csrc.nist.gov/publications/detail/sp/800-145/final#:~:text=Cloud%20computing%20is%20a%20model,effort%20or%20service%20provider%20interaction.

The Internet of Things

1.47 While the Internet was originally conceived as a network to enable people to communicate with one another, today it is also being used as a network to allow interrelated computing devices to transfer data between each other without requiring human interaction or intervention. This development is referred to as the Internet of Things (IoT).[1] In the consumer market, IoT is associated with products such as always-on speakers, home security systems and smart thermostats. In organizations, IoT has been used in the health care sector, manufacturing and logistics to enable the integration of sensors, trackers and other processing devices. The ubiquity of IoT has led to evidential discovery claims in the US being made against the companies that collect and store the data recorded by IoT devices.[2] At the same time, the advent of IoT has raised serious concerns about the adequacy of security in its implementation, which in turn raises questions about individual privacy and the quality of the electronic evidence collected by such devices.

1 Internet of Things (Wikipedia), https://en.wikipedia.org/wiki/Internet_of_things.
2 For example, see Nadeem Bohsali, 'Alexa: hear no evil', Blog Post, Richmond Journal of Law and Technology, 13 February 2020, https://jolt.richmond.edu/2020/02/13/alexa-hear-no-evil/.

The deep web and the dark web

1.48 The role of the Internet is simply to carry data from one computer to another, but for this to be a useful service to a user, application software must be created. For example, an email client allows its user to send and receive messages, and a web browser allows its user to view pages on the World Wide Web. Certain Internet applications, such as the web browser, are now considered to be a standard part of Internet provision. However, not all web pages can be viewed using only a web browser. Additional software can be used to increase the level of convenience or security for individuals providing or obtaining access to information. Such web pages make up the 'dark web'.[1]

1 Dark web (Wikipedia), https://en.wikipedia.org/wiki/Dark_web.

1.49 One example of dark-web software is corporate virtual private networks (VPNs), where web pages are available only to employees. The VPN software ensures that only authorized individuals can obtain access to the web pages and that, through the use of encryption, eavesdroppers are unable to view the content of pages being viewed. While a corporate VPN meets the criteria for the dark web, the term is more

often associated with software designed to protect the identity of those providing the content of web pages. One of the most popular technologies of this type is Tor onion services, where website addresses end in .onion. Like a VPN, Tor onion services protect the content of web pages through encryption, but, unlike a VPN, Tor also hides the IP addresses of both the individual providing the web page and the individual obtaining access to the web page.

1.50 The additional level of security that Tor offers, as compared to a VPN, is desirable for people who want to share material censored in their country, and indeed Tor is used for this purpose. However, Tor onion services gained notoriety for enabling online marketplaces selling illicit products. When used for illegal purposes, the privacy Tor offers disrupts investigations of law enforcement authorities into the operator of the marketplace, as well as the sellers and purchasers of products. Cryptocurrencies are also used on such marketplaces, to reduce the risk that payments will be traced through the banking system.[1] Tor's security is far from perfect, however, and law enforcement authorities have shut down Tor onion sites participating in illegal activities and have discovered the identities of both the operators of the sites and their users. Examples include one of the first popular marketplaces for illegal drugs, The Silk Road, set up in 2011 and shut down by the FBI in 2013.[2] Law enforcement authorities are rarely explicit about the methods they use to trace individuals involved in dark websites, but approaches undoubtedly include some combination of the following:

> (1) Exploiting design flaws and security vulnerabilities in software installed on the computer serving the dark web pages and/or the computers used to access them.
>
> (2) Monitoring networks used by people suspected of being involved in running or using the website, and looking for patterns of use. Such timing patterns are not hidden by Tor's encryption and so can provide information about who is using which service.
>
> (3) Gathering information from the dark website and linking this activity to another website to which an identity can more easily be attributed.
>
> (4) Recruiting informants involved in the running of services and inducing them to collect information on behalf of law enforcement authorities.
>
> (5) Tracing flows of cryptocurrencies until they can be linked to an identity.

1 For example, see Dr Clare Jones, Associate Professor Banking and Finance Law, Bristol Law School, Faculty of Business and Law, University of the West of England, Bristol, 'Digital currencies and organised crime update', https://core.ac.uk/download/pdf/323892795.pdf.

2 *United States of America v Ross William Ulbricht, a/k/a Dread Pirate Roberts, a/k/a Silk Road, a/k/a Sealed Defendant 1, a/k/a DPR*, 858 F.3d 71 (2nd Cir 2017).

1.51 The use of encryption for providing access to a website and for making payments increases the complexity of collecting and interpreting evidence. Some of this evidence will be statistical in nature and so particular care is needed when applying probabilistic reasoning to reach conclusions. However, the underlying principles behind attributing Internet activity remain the same regardless of whether a standard website or a dark website are used. The nature of the dark web makes it difficult to assess how it is being used, but while it is used for illegal activities, the normal World Wide Web is still the preferred option for online crime.[1] The notoriety of illicit marketplaces attracts media attention, but it is probable that these make up only a small proportion of the around

175,000 Tor onion services (as of August 2020).[2] The technologies used for the dark web are not restricted to just providing websites. There are also dark-web equivalents of instant messaging networks, and file sharing.

1 In 2019, 0.2 per cent of child sexual abuse images assessed by the Internet Watch Foundation were hosted on onion services. See IWF 2019 Annual Report at https://www.iwf.org.uk/report/iwf-2019-annual-report-zero-tolerance; Chandrika Nath and Thomas Kriechbaumer, 'The darknet and online anonymity', POSTNOTE 488 (Parliamentary Office of Science & Technology, March 2015), https://post.parliament.uk/research-briefings/post-pn-488/.
2 https://metrics.torproject.org/hidserv-dir-onions-seen.html.

1.52 The dark web is frequently confused with the deep web. While it is necessary to use special software to obtain access to the dark web, the deep web refers to content that can be viewed using a normal web browser but which is password-protected or otherwise restricted in terms of who can view it. These pages include web mail, online banking, private social media pages and profiles, web forums that require registration for viewing and services that must be paid for to enable access ('paywalls'), such as video on demand and online content.[1] The deep web cannot be included in the index of search engines because their indexing software does not possess the passwords and other credentials that would allow them to obtain access to the deep web. Consequently, such content is less visible than that on the rest of the World Wide Web. Most search engines also do not include the dark web in their index, but this is because these search engines have made the business decision that dark web content is not sufficiently popular, rather than because they are not able to do so. There are, however, specialized search engines which can find pages on the dark web. Addresses of pages on the dark web can also be shared through links on standard web pages and through email, chat rooms or word of mouth. Content on the dark web can also be restricted through password protection, which would result in this content being inaccessible even to dark-web search engines.

1 Deep web (Wikipedia), https://en.wikipedia.org/wiki/Deep_web.

Common network applications

Email

1.53 A significant amount of correspondence undertaken within organizations and between organizations and individuals takes the form of the exchange of email. Email is, essentially, an unstructured form of communication, whose content determines its purpose. Email is an important source of electronic evidence. However, emails should be treated with some discretion, because a person can conceal his identity and hide behind a false email address with relative ease. It is very straightforward to send an email that appears to come from someone other than the real source. Forging emails might be effortless, but email is freely admitted into legal proceedings, both criminal and civil.

1.54 To obtain access to email, it is necessary to interact with two different services, one for outgoing mail and one for incoming mail. These services may or may not be provided by the same server. To read email, the individual must direct the email program to connect to a mail server using one of a number of protocols, the most common of which are: Post Office Protocol (POP),[1] Internet Message Access Protocol (IMAP)[2] and

a Proprietary Microsoft Protocol called Messaging Application Programming Interface (MAPI).[3]

1 Post Office Protocol (Wikipedia), https://en.wikipedia.org/wiki/Post_Office_Protocol; J. Myers and M. Rose, 'RFC 1939 – Post Office Protocol – Version 3' (Internet Engineering Task Force, May 1996), https://tools.ietf.org/html/rfc1939.
2 Internet Message Access Protocol (Wikipedia), https://en.wikipedia.org/wiki/Internet_Message_Access_Protocol; M. Crispin, 'RFC 3501 – Internet Message Access Protocol – Version 4rev1' (Internet Engineering Task Force, March 2003), https://tools.ietf.org/html/rfc3501.
3 MAPI (Wikipedia), https://en.wikipedia.org/wiki/MAPI.

1.55 The POP protocol (POP3 is the most widely used version) permits the user to read her email by downloading it from a remote server onto the storage facility of her local computer or device. Once the email has been downloaded from the server, it is optionally deleted from the live server, but probably not from the backup server that will invariably be used by the mail service provider for the purpose of recovering from a failure for any reason. By contrast, the IMAP protocol (IMAP4 being the most widely used) enables the user to leave all her email on the mail server by default. Both POP and IMAP protocols require a user to have a username and a password before the user can obtain access to the mail download service. In addition, the protocol servers may keep logs of who checked emails and when they were checked. The existence of logs will enable an investigator to look for evidence of email traffic even where a user has deleted all of her emails.

1.56 Outgoing email uses a different protocol called Simple Mail Transfer Protocol (SMTP),[1] although MAPI also supports outgoing email. The servers supporting SMTP do not normally require a user to use a password. This makes it very easy for an individual to forge a message. However, the SMTP server may keep a log of the messages that pass through the system.

1 Simple Mail Transfer Protocol (Wikipedia), https://en.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol; J. Klensin (ed.), 'RFC 5321 – Simple Mail Transfer Protocol' (Internet Engineering Task Force, October 2008), https://tools.ietf.org/html/rfc5321.

1.57 When an email is sent from a computer, it will pass on to one of a number of Message Transfer Agents (MTA). The MTAs act in the same way as post offices handling physical mail. A local MTA will receive the email. Upon receipt, it will add to the top of the email message received the current time and date, the name of the MTA and additional information. This information is in what is called the header of the email. As the message passes through various MTAs, each MTA will add further date and time stamps to the header. The most recent information will be at the top of the header. Another item of information that tends to be collected in the header is the IP address of the computer or system connecting to the server. Technically astute users of email who may wish to hide their identity can send messages through anonymous or pseudonymous re-mailing services. When email is sent through such a re-mailing agent, the header information may be stripped before the message is sent on to its destination. However, other forms of electronic evidence are transferred during such a process, and it is possible for forensic investigators to attempt to find evidence that may be useful.[1]

1 See Craig Earnshaw and Sandeep Jadav, 'E-mail tracing' (2004) 15(3) Computers & Law, 7 for an introduction.

Instant messaging

1.58 Instant messaging (IM) is a form of online communications service that enables the user to transmit a variety of text, voice and image messages to other individuals in real time over the Internet. This form of communication is similar to a conversation over the telephone, but the users communicate by typing messages into the software. The technology also permits the user to share files. Instant messaging has become popular because the software implementing the service can be downloaded at no cost, and is easy to install and use. Popular instant messaging software includes WhatsApp, Facebook Messenger, WeChat, Viber, LINE and Telegram. Data from such systems is also increasingly used as evidence in legal proceedings.[1]

1 For example, see *U.S. Commodity Future Trading Commission v Amaranth Advisors, L.L.C.*, 554 F Supp 2d 523 (SDNY 2008); *CX Digital Media, Inc. v Smoking Everywhere, Inc.*, 2011 WL 1102782 (SD Fla Mar 23, 2011).

1.59 Depending on the type of software used, the program will, when a message is initiated, connect the two devices, either via a direct point-to-point configuration or via a client–server configuration, through the ports of the devices. There are two significant problems with this in respect of producing reliable electronic evidence. First, in a client–server configuration the instant message server may not necessarily log such messages, which means that such conversations can be considered conceptually similar to conversations over the telephone. Second, the program may have a feature that allows for messages to pass through legitimate open ports if others are not available. Whether such conversations are recorded will depend on the software used. In an earlier variation of Instant Messaging known as Internet Relay Chat (IRC),[1] conversations take place in a similar way to a conference call. IRC is mainly designed for group communications, though it also allows for one-on-one communications via private messages. It frequently suffers from the same issues as instant messaging, in that the servers relaying messages are not necessarily configured to log conversations.

1 Internet Relay Chat (Wikipedia), https://en.wikipedia.org/wiki/Internet_Relay_Chat; C. Kalt, 'RFC 2812 – Internet Relay Chat: client protocol' (Internet Engineering Task Force, April 2000), https://tools.ietf.org/html/rfc2812; and 'RFC 2813 – Internet Relay Chat: server protocol' (Internet Engineering Task Force, April 2000), https://tools.ietf.org/html/rfc2813.

1.60 Since instant messaging requires various intermediaries to relay the messages from sender to recipient, to resist the interception of the message and loss of privacy, many instant messaging software packages have implemented encryption. These implementations may vary in the level of security they provide: some implementations secure the messages as between users (end-to-end encryption), but others only encrypt the messages in transit (link encryption), which enables the service provider to gain access to them. This allows the service provider to implement filtering, blocking and other editorial features, and also enables a party to require the service provider to preserve or disclose evidence.[1]

1 For instance, see the US cases of *Duhn Oil Tool, Inc. v Cooper Cameron Corporation*, 609 F.Supp.2d 1090 (E.D. Cal. 2009), reconsidered in *Duhn Oil Tool, Inc. v Cooper Cameron Corporation*, 2009 WL 3381052; *People for the Ethical Treatment of Animals, Inc. v Dade City's Wild Things, Inc.*, 2017 WL 5187770 (M.D. Fla. Nov. 9, 2017).

Peer-to-peer networking

1.61 As personal computers have developed, so has their capacity and power increased. As a result, there is less of a dividing line between a client and a server. This is because any host can be made a server by installing appropriate software onto the computer. This software then permits other clients to obtain access to the resources of the computer over the network. This is called peer-to-peer networking (P2P),[1] and is often the subject of litigation regarding intellectual property, especially regarding the downloading of music and films without payment. For instance, in Hong Kong a *Norwich Pharmacal*[2] order was granted in the case of *Cinepoly Records Co Ltd v Hong Kong Broadband Network Ltd*[3] in respect of a number of IP addresses, and in the case of *Polydor Ltd v Brown*[4] summary judgment was granted against the second defendant, Mr Bowles, for copyright infringement after a *Norwich Pharmacal* order was made against various Internet service providers whose subscribers' IP addresses had been identified as being used for allegedly infringing activity. In both cases the infringers were identified by the Internet service providers from their electronic records of the IP addresses assigned to their subscribers at the date and time when the allegedly infringing activity was taking place.[5]

1 Geoff Fellows, 'Peer-to-peer networking issues – an overview' (2004) 1(1) Digital Investigation 3; Peer-to-peer (Wikipedia), https://en.wikipedia.org/wiki/Peer-to-peer; G. Camarillo (ed.), 'RFC 5694 – Peer-to-peer (P2P) architecture: definition, taxonomies, examples, and applicability' (Internet Engineering Task Force, November 2009), https://tools.ietf.org/html/rfc5694.

2 *Norwich Pharmacal Co v Customs and Excise Commissioners* [1973] 3 WLR 164, [1973] 2 All ER 943, [1973] 6 WLUK 112, [1973] FSR 365, [1974] RPC 101, (1973) 117 SJ 567, [1973] CLY 2643. See generally Paul Torremans, *Holyoak and Torremans Intellectual Property Law* (9th edn, Oxford University Press 2019).

3 [2006] HKCFI 84, [2006] 1 HKLRD 255, HCMP 2487/2005 (26 January 2006).

4 [2005] EWHC 3191 (Ch), [2005] 11 WLUK 760, (2006) 29(3) IPD 29021.

5 For a similar case in Denmark, see Per Overbeck, 'The burden of proof in the matter of alleged illegal downloading of music in Denmark' (2010) 7 Digital Evidence and Electronic Signature Law Review 87; Per Overbeck, 'Alleged illegal downloading of music: the Danish Supreme Court provides a high bar for evidence and a new line of direction regarding claims for damages and remuneration' (2011) 8 Digital Evidence and Electronic Signature Law Review 165; similar comments were made by Baker DJ in *VPR Internationale v Does 1-1017*, 2011 WL 8179128; Thomas M. Dunlap and Nicholas A. Kurtz, 'Electronic evidence in torrent copyright cases' (2011) 8 Digital Evidence and Electronic Signature Law Review 171.

Social networking

1.62 The advent of Web 2.0 has seen an enormous increase in websites that permit users to provide their own content. This varies in type from uploaded video clips (on sites such as YouTube), photographs (on sites such as Flickr), personal musings in the form of blogs (personal Web logs), and interactive exchanges with a wider audience in the form of social networking sites (such as Facebook and Twitter) and their more business-oriented alternatives (such as LinkedIn). As social networking has increased in popularity, with a significant increase in participating users, several contexts arise in which the content of an individual's social network contribution may constitute evidence. For instance, an individual may be located at a specific place by means of his geotagged submissions to such a site,[1] and photographs uploaded to a social networking site often retain their geotag data and reflect the time and place at which they were taken. Many sites with contributions that contain such information have been used for the purposes of grooming[2] and blackmail.[3]

1 Jiebo Luo, Dhiraj Joshi, Jie Yu and Andrew Gallagher, 'Geotagging in multimedia and computer vision – a survey' (2011) 51(1) Multimed Tools Appl 187, https://doi.org/10.1007/s11042-010-0623-y.
2 *R. v Scott (Michael Lawrence)* [2008] EWCA Crim 3201, [2008] 12 WLUK 671; *R. v B (C)* [2010] EWCA Crim 3009, [2010] 12 WLUK 262.
3 *R. v Breakwell (Jake)* [2009] EWCA Crim 2298, [2009] 10 WLUK 647.

1.63 In a different vein, data from social media can also play an evidential role in both criminal and civil proceedings. This is obviously the case when the social media contribution itself constitutes a crime or a tort, for instance defamation, copyright violations or incitement to terrorist offences. More indirect use of such evidence can establish an alibi by locating an individual at a specific time and place in the same way as indicated above. In child custody cases, social media data has been used to demonstrate that a child was regularly left unsupervised late at night during schooldays, and social media information has provided evidence of spousal infidelity in divorce proceedings.[1] An individual's social network contributions may also help to determine political or social prejudices that in turn shed light on the character of a trial witness. The evidence may be recovered from the witness's contributions to social networking sites, depending on their availability and accessibility. If an individual has made such contributions under an alias, a digital evidence professional may be able to establish his true identity by matching his online contributions to the same content that is found on the individual's storage media.

1 By way of example, see *Lachaux v Lachaux* [2017] EWHC 385 (Fam), [2017] 4 WLR 57, [2017] 3 WLUK 67, [2018] 1 FLR 380, [2017] 2 FCR 678, [2017] CLY 984.

1.64 Finally, in addition to the content of individual contributions, the social network of a person can itself be of evidential value, for instance in investigations of terrorist organizations, criminal networks or any other situation where the law requires evidence of membership of a group or participation in a form of coordinated action. In such cases, it is increasingly common to use network analysis or similar artificial intelligence tools to identify structures within social media networks.[1]

1 Michael Chau and Jennifer Jie Xu, 'Mining communities and their relationships in blogs: a study of online hate groups' (2007) 65(1) International Journal of Human-Computer Studies 57; Stephen Kelley, Mark Goldberg, Malik Magdon-Ismail, Konstantin Mertsalov and Al Wallace, 'Defining and discovering communities in social networks', https://core.ac.uk/download/pdf/209214163.pdf.

Types of evidence available on a digital device

1.65 A digital evidence professional can make a range of evidence available from a digital device. This section provides an outline of some of the types of evidence that can be gleaned.

Files

1.66 A wide range of application software is used on computers, laptops, tablets and mobile telephones, including programs that enable a user to send messages, prepare spreadsheets, databases and text documents, take digital photographs, and create multimedia and presentations. This data, referred to as files on the digital device or on networks, will store messages, spreadsheets, databases, texts, photographs,

multimedia and presentations, and may themselves be electronic evidence. A great deal of data can be retrieved, depending on the method of storage, the media on which it is stored and the manner in which the device manages data storage.

Metadata

1.67 Metadata is, essentially, data about data. For instance, the metadata in relation to a piece of paper as a physical document may be:

> Explicit from perusing the paper itself, such as the title of the document, the date, the purported name of the person(s) who wrote it, who received it and the location of the document.
>
> Implicit, which includes such characteristics as the types of type (font) used, such as bold, underline or italic, the location of the document such as a coloured file to denote a particular type of document, and document labels that also act as pointers to allow the person using the document to deal with it in a particular manner, such as a confidential file, for instance.

1.68 All files, including email communications, spreadsheets, websites and word processing documents, will contain metadata in one form or another. In fact, a file has to have metadata to help the interpretation of the purpose of the digital document. Such data can be taken automatically from the originating application software, or can be supplied by the person who originally created the record. The list of information that is available includes, but is not limited to: when and how a document was created (purported time and date), the file type, the name of the purported author (although this will not necessarily be reliable information, because the person whom the document metadata names as 'author' might be someone entirely different from the person who actually wrote the document[1]), the location from which the file was opened or where it was stored, when the file was last opened (purported time and date), when it was last modified, last saved and last printed, the identity of the purported previous authors, the location of the file on each occasion it was stored, the details of who else may be able to obtain access to it, and, in the case of email, blind carbon copy (bcc) addresses.

1 For instance, where a document is revised on a number of occasions, on different computers and by different people, the name of the author will probably bear no resemblance to the authorship of the document. In *IG Markets v Crinion* [2013] EWCA Civ 587, [2013] 5 WLUK 621, [2013] CP Rep 41, Times, 31 July 2013, [2013] CLY 387, also known as *Crinion v IG Markets Ltd*, the judgment of the trial judge, HH Judge Simon Brown QC, was taken word-for-word from the closing submissions of Mr Chirnside, counsel for the claimant, written in a Word file. The trial judge adjusted the text, and the 'properties' file in the Word version of the judgment indicated that the 'author' was 'SChirnside'. Also, the person originating a document may not use a new file, but may create the document by opening an old file, deleting the majority of the text, then creating the genesis of the new text; further, the name of the author may not be accurate if the person creating the document had logged onto the computer using somebody else's account, and there may be occasions when a person uses software on their own computer that has been installed and registered in another name – although if the metadata is correct, it can directly lead to a killer that has murdered a number of people over a long period of time: https://en.wikipedia.org/wiki/Dennis_Rader.

1.69 Because metadata is generally created automatically by the software and without the knowledge of the user, it is therefore also more difficult to alter, manipulate or delete. Imagine that Alice writes a document on a computer. The software will add metadata that is associated with this document, for instance the time when the document was created. The file where this information is stored is the metadata that

records the time of the event of writing. Since it is not an intentional creation by the author, but an automatic, software-generated artefact that is often invisible to the user, she may not know about this data, and even if she did, she may not know how to alter or delete it.

1.70 However, it must be said that metadata is not infallible. Its interpretation requires making assumptions about the environment in which it was created. If the real-time clock on the device was not accurate (for instance, the clock in a laptop that has crossed time zones without being adjusted for this, or if the clock is slow, or has been deliberately changed), the metadata as recorded will be false. Since the environment can in this sense 'lie', informed criminals can intentionally manipulate the data. For instance, experienced phishing attackers who use email may not only forge the sender's address in the emails they send, but may also manipulate the entire header to conceal the place from which the email originates. Finally, since metadata is the unintentional creation of information by the environment, examiners or other third parties who are operating in the same environment will also create metadata, and so potentially contaminate the evidence. A careless digital evidence professional, or an IT administrator of a company who is alerted to potentially illegal activity by an employee, can by the very act of opening and looking at the file create new metadata and overwrite the old (a new time when the document was created, according to the computer), thereby erasing potentially useful metadata about the illegal activity such as the actual date and time it was committed.

Types of metadata

1.71 In broad terms, there are three main types of metadata:[1]

> (1) Descriptive metadata describe a resource for a particular purpose, such as a disclosure or discovery exercise. The metadata may include such information as title, key words, abstract and the name of the person purporting to be the author. To understand the history of the document more fully, it would be necessary to obtain information about how and when the system recorded the name of the purported author.
>
> (2) Structural metadata describe how a number of objects are brought together. Some examples of structural metadata include 'file identification' (e.g. to identify an individual chapter that forms part of a book or report); 'file encoding' (to identify the codes that were used in relation to the file, including the data encoding standard used (ASCII, for instance)); the method used to compress the file and the method of encryption, if used; 'file rendering' (to identify how the file was created, including such information as the software application, operating system and hardware dependencies); 'content structure' (to define the structure of the content of the record, such as a definition of the data set, the data dictionary, files setting out authority codes and such like); and 'source' (to identify the relevant circumstances that led to the capture of the data).
>
> (3) Administrative metadata, which provides information to help with the management of a resource. Administrative data is further divided into rights management metadata and preservation or record-keeping metadata.

1 For more information on metadata, see Dublin Core Metadata Initiative, http://dublincore.org/; National Information Standards Organization, 'Understanding Metadata' (NISO Press 2004), http://www.niso.org/standards/resources/UnderstandingMetadata.pdf; Michael Day, 'DCC Digital Curation Manual Instalment on Metadata' (UKOLN v1.1 2005), https://www.dcc.ac.uk/sites/default/files/documents/resource/curation-manual/chapters/metadata/metadata.pdf.

1.72 The metadata can be fundamentally linked to and be a part of the electronic document, be included in the systems used to produce the document, or be linked to it from a separate system. Metadata can be viewed in a variety of ways, one of which is to look at the 'properties' link in the application that created the document, or by using software specifically written for this purpose. Some metadata can also be removed with specialist software. This can be useful when sending files to third parties, but can attract additional expense if a court orders the data to be delivered up in its original format, as in the case of *Williams v Sprint/United Management Company*.[1] Before passing electronic spreadsheet documents in Excel form to the plaintiffs, Sprint modified the electronic files by, among other things, deleting metadata from the electronic files that included the spreadsheets, and preventing the recipients from viewing certain data contained in the spreadsheets by locking the value of certain cells. Sprint was ordered to produce the unlocked versions of the spreadsheets in the manner in which they were maintained, including their metadata. In his judgment, the judge discussed metadata and whether it formed a sufficient part of a document in electronic form for it to be given up to the other party.[2]

1 230 F.R.D. 640 (D.Kan. 2005).
2 230 F.R.D. 640 at 646–48 (D.Kan. 2005).

1.73 A further illustration of the importance of metadata is the case of *Campaign Against Arms Trade v BAE Systems PLC*.[1] On 29 December 2006, a senior officer of the Campaign Against Arms Trade (CAAT), Ms Feltham, sent an email containing privileged legal advice to the members of the CAAT steering committee using a private and internal email distribution list to 12 members of the steering committee and 7 members of CAAT's staff. A copy of the email was somehow sent to BAE Systems PLC (BAE). By a letter dated 9 January 2007 and received the next day, solicitors for BAE returned a printed paper copy of the email to CAAT's solicitors. This was the first time that CAAT came to know of the leak. CAAT sought and obtained a *Norwich Pharmacal* order against BAE. In giving judgment, Mr Justice King noted that the printed email returned to CAAT was incomplete (because the email metadata were missing). As described by Mr Justice King:[2]

> It was a redacted version of that which had come into the possession of the Respondent and/or its own solicitors. All the routing information, the header address and so forth, which would give details of the email accounts through which the email had been received and sent before arriving at the Respondent and its solicitors, had been removed. Such removal must have been done either by the Respondent or by its solicitors acting on its instructions.

1 [2007] EWHC 330 (QB), [2007] 2 WLUK 617.
2 [2007] EWHC 330 (QB) at [31].

1.74 The source of the leak could be the result of only two possibilities – one of the authorized recipients of the email or an unauthorized interception of the email. BAE had objected to the order, arguing that CAAT should have investigated the authorized recipients and their personal electronic data to trace the source before seeking the order. Mr Justice King rejected this argument:

> 46. … Ms Feltham … explains that there was a major practical and logistical problem as regards access to the computers used by members of the steering committee. Unlike the staff they are not employees of the Applicant but volunteers who do not work in the office or use computer systems belonging to

> the Applicant. Some are members of other organizations who access emails from accounts and equipment owned by their employers. Some are based outside London. This all means that to have investigated further on the lines suggested by the Respondent, the Applicant would have needed access to computers to which the Applicant has no right of access and in any event the Applicant would have needed the 'costly services of a computer expert to go on a fishing expedition for emails which might or might not have been sent which moreover would have been very time consuming.'

1.75 The unrealistic claim by BAE that CAAT ought physically to examine every computer to trace the route of the email fails to grasp the fundamental issue that electronic data knows no geographical or physical bounds. Returning the email without the metadata is similar to returning a letter received through the post in an envelope, yet refusing to deliver up the envelope. That the routing and other technical data available in relation to an email is 'similar' to the data included on an envelope is an understatement, because the email metadata is far more extensive than the metadata contained on an envelope. In this instance, Mr Justice King concluded that the order sought ought to be granted, although not in the terms requested.

1.76 This application illustrates the importance of the metadata associated with an electronic object. Documents in electronic form include metadata as a matter of course, and it seems unrealistic for the recipient to refuse to deliver up the full document, including the associated metadata, in such circumstances.

1.77 A case from the US serves to highlight how concerns relating to the preservation of data are viewed, as well as the relevance of metadata. In the case of *Armstrong v Executive Office of the President, Office of Administration*,[1] the Executive Office of the President and related White House departments intended to require all federal employees to print out their electronic communications on paper to discharge their obligations under the provisions of the Federal Records Act. This was challenged by researchers and non-profit organizations on the grounds that this amounted to a destruction of federal records. The United States Court of Appeals, District of Columbia Circuit upheld the challenge, noting that the hard copy printed version 'may omit fundamental pieces of information which are an integral part of the original electronic records, such as the identity of the sender and/or recipient and the time of receipt'.[2]

1 1 F.3d 1274 (D.C. Cir. 1993).
2 1 F.3d 1274 (D.C. Cir. 1993) at 1277.

Social context and metadata

1.78 A significant amount of electronic data is created through communication between people separated by geographical, political, social and cultural boundaries. While the Internet has brought people previously separated by distance into interaction, it also creates a new form of 'distance' between the communicators. Some communication practices do not translate well to this new medium, such as facial expressions and tone of voice. Evidence is not created in a vacuum, however. It has meaning, and can be interpreted only with knowledge of the context in which it was created. The exchange 'I hate you all and wish you were dead' in a dispute between a teenager and his parents about cleaning a room will be interpreted by most people acquainted with a similar cultural background as insignificant and not serious. The

same words found on a carefully written letter will carry a different meaning. Therefore, consideration has to be given to whether an email, a Twitter post or an exchange on a discussion forum is more similar to a letter or to a direct verbal exchange.

1.79 Consider the case of *Chambers v Director of Public Prosecutions*.[1] Paul Chambers was a registered Twitter user with the handle '@PaulJChambers'. He was due to fly to Belfast from Doncaster Robin Hood Airport to meet another Twitter user, identified as '@Crazycolours', on 15 January 2010.[2] On 6 January 2010, Chambers became aware of problems at Doncaster Robin Hood Airport because of adverse weather conditions, and he and Crazycolours subsequently entered into the following exchange on Twitter:

> @Crazycolours: I [Chambers] was thinking that if it does then I had decided to resort to terrorism
>
> @Crazycolours: That's the plan! I am sure the pilots will be expecting me to demand a more exotic location than NI

1 [2012] EWHC 2157 (Admin), [2013] 1 WLR 1833, [2013] 1 All ER 149, [2012] 7 WLUK 933, [2013] 1 Cr App. R 1, (2012) 176 JP 737, [2012] Info TLR 193, [2012] ACD 114, [2013] CLY 625.

2 The facts are taken from the judgment of Lord Judge LCJ in *Chambers v Director of Public Prosecutions* [2012] EWHC 2157 (Admin); Lilian Edwards, 'Section 127 of the Communications Act 2003: threat or menace?' (2012) 23(4) Computers & Law 21.

1.80 The court noted that in the context of the bad weather, these comments from Chambers seemed to be a reference to the possibility of the airport closing. No reply from Crazycolours was produced in court. Two hours later, when Chambers found out that the airport had closed, he posted the following message, available to the 600 or so followers of his Twitter postings:

> Crap! Robin Hood Airport is closed. You've got a week and a bit to get your shit together otherwise I am blowing the airport sky high!!

1.81 On 11 January 2010, five days after the comments were posted, the managers at Robin Hood Airport found the comments and passed what was regarded as a 'non-credible' threat (because the tweet featured Chambers' name and because he was due to fly from the airport in the near future) to the airport police, who in turn referred the matter on to the South Yorkshire police.

1.82 The South Yorkshire police arrested Chambers on 13 January on suspicion of involvement in a bomb hoax while he was at work, seven days after the offending message was tweeted. Interviewed under caution, Chambers repeatedly asserted that this Tweet was a joke, or meant to be a joke and not intended to be menacing. He said that he did not see any risk at all that it would be regarded as menacing, and that if he had, he would not have posted it. In interview he was asked whether some people might get a bit jumpy and responded 'yah. Hmm mmm'. Chambers was charged with the offence of sending by a public electronic communication network a message of a 'menacing character' contrary to s 127(1)(a) and (3) of the Communications Act 2003 and was found guilty. His appeal to the Crown Court in Doncaster was dismissed, and on further appeal the question was whether the words he used were a 'menacing message sent through a public communication medium' and thus in violation of s 127(1)(a) and (3) of the Communications Act 2003.

1.83 The ensuing prosecution showed just how difficult this determination can be. Some security officers at the airport were willing to dismiss it outright as 'venting', while others were concerned enough to inform the police. The court of first instance, applying an abstract, decontextualized dictionary definition of 'menace', convicted Chambers. On appeal, the members of the Court of Appeal noted, however, that '[b]efore concluding that a message is criminal on the basis that it represents a menace, its precise terms, and any inferences to be drawn from its precise terms, need to be examined in the context in and the means by which the message was sent'.[1] The Court of Appeal reversed the decision of the lower court and allowed the appeal against conviction because it was posted as a conversation piece for Chambers' followers, drawing attention to himself and his predicament. It was not addressed to anyone at the airport or anyone responsible for public security. The communication was airing the grievance that the airport was closed when the writer wanted it to be open, and identified the person making the 'threat' in ample time for it to be reported and extinguished.

1 *Chambers v Director of Public Prosecutions* [2012] EWHC 2157 (Admin) at [31].

1.84 For the Court of Appeal to consider the social context in which the electronic evidence was to be understood must be correct. The visual form in which this evidence appears may not be a true account of the social meaning that informed the users when the evidence was created. For instance, a Tweet may look like a warning, but it is certainly not understood as such by the participants. Since judges and jurors will often have very different technological experiences, it is tempting to lead sociological or psychological evidence on these issues, but procedural rules on admissibility may well prevent this.

Imaging

1.85 Any digital forensic investigation will begin by 'imaging' the device on which electronic evidence may reside. The imaging process is a non-destructive process that creates an exact external digital copy of any data on the device. Subsequently, all data investigation should be performed on the imaged copy and not on data stored on the original device.

System and program logs

1.86 As previously noted, many services and devices keep records or logs of activity for business and operational purposes. In most modern operating systems such as Windows and Linux, virtually anything and everything happening on and to the system is recorded in the form of logs in some manner. This includes information about system events, including the startup of applications and various classes of error messages. Information in the logs may help to determine, for instance, how an unauthorized computer user obtained access to a system with the intent of stealing information from the computer. It may also be possible to configure the systems log (syslog) such that the log messages can be sent to another networked system while retaining a local copy. As a result, if a hacker acquires system adminstrator privileges on a networked UNIX operating system,[1] for instance, and wants to erase something from the local logs, he would not be able to erase the data from the remote logs to remove all traces of his intrusion unless he also has the appropriate privileges on the remote machine.

1 In UNIX-type systems, the 'superuser', that is the account for the system administrator, is known as 'root'. This account has all rights or permissions to all files and programs in all modes.

1.87 Unlike UNIX-type operating systems such as Linux and macOS, the Windows operating system also includes a 'registry'. This is a store of data that contains a great deal of information, including a comprehensive database containing information on every program that is compatible with Windows that has been installed on the computer. It also includes information about the purported user of the computer, the preferences exercised by the user, information about the hardware components and information about the network (if it is connected to a network). The values stored in the registry are designed primarily to be processed by the computer, but can be converted to a human-readable form. An example of the type of information that the registry can provide to an investigator is the AutoComplete data for a user of Internet Explorer visiting a particular website, such as her name, address, telephone number, email address and passwords. In addition, it is possible to establish when the user last downloaded a file from the Internet, together with the first page she visited from the registry.[1]

1 Although it does not follow that a user clicked on a website address that has been recorded in a temporary cache file, for which see the case of *State of Connecticut v Julie Amero* (Docket number CR-04-93292; Superior Court, New London Judicial District at Norwich, GA 21; 3, 4 and 5 January 2007). For an exhaustive analysis of this case, see Stephen Mason (ed.), *International Electronic Evidence*, xxxvi–lxxv.

Temporary files and cache files

1.88 When a digital device connects to the Internet, a range of information about its activities may be recorded and retained locally, including the websites and any newsgroups that have been visited, and the content that was viewed. For the purpose of enabling the browser to improve user experience and speed up browsing, temporary copies of websites that have been visited are stored in cache folders. These folders contain fragments of the web page, including images and text. Some browsers will retain more than one local file containing location information about the websites visited.

1.89 It is important to understand the legal consequences of temporary files and cache files. This is exemplified in the case of *Atkins v Director of Public Prosecutions*.[1] In this case, Dr Atkins, a university lecturer at the University of Bristol, Department of English, had browsed the Internet for indecent photographs of children and had saved a number of such photographs as files in the J directory of his computer. He was convicted of one offence of having in his possession indecent photographs of children on the J directory of his computer and nine other offences for the temporary files that his browser had placed in the cache folder. In allowing an appeal, Simon Brown LJ and Blofeld J held that Dr Atkins should not have been convicted of possession in respect of the photographs stored in the cache, because he was not aware of its existence or what it did, and therefore could not be said to have knowingly had possession of these particular photographs. The court ordered that the case be remitted with a direction to convict Dr Atkins of the offences where he deliberately saved photographs in the J directory.[2]

1 *Atkins v DPP* [2000] 1 WLR 1427 (QB), [2000] 2 All ER 425, [2000] 3 WLUK 213, [2000] 2 Cr App R 248, (2000) 97(13) LSG 42, (2000) 144 SJLB 148, Times, 16 March 2000, Independent, 17 April 2000, [2000] CLY 993, also known as *DPP v Atkins*; for a US case based on similar facts with an identical outcome, see *United States v Kuchinski* 469 F.3d 853 (9th Cir. 2006).
2 In *Clifford v Chief Constable of the Hertfordshire Constabulary* [2011] EWHC 815 (QB), [2011] 4 WLUK 7, Mr Justice Mackay observed that the prosecution were fully aware of this issue, but prosecuted Mr Clifford in any event: a prosecution that was eventually determined to be malicious; see also *Clifford v Chief Constable of the Hertfordshire Constabulary* [2008] EWHC 3154 (QB), [2008] 12 WLUK 568 and *Clifford v Chief Constable of the Hertfordshire Constabulary* [2009] EWCA Civ 1259, [2009] 12 WLUK 16.

1.90 In addition to browser caches, Windows and UNIX systems also have paging file or swap space. This is an area of non-volatile storage space that is used as virtual memory. In the event that the applications being run on the system require more RAM than the system has available, low-priority applications are copied to the virtual memory and the RAM they are using is thereby freed for use by applications with a higher priority. Swap space is rarely cleaned during the normal operation of the system. This means that when a system needs to be forensically analysed, it is often the case that useful data associated with applications, which may not even be running at the time, can be found by analysing the content of the swap space. This can also apply to data that is normally stored on the standard file system in an encrypted form. Depending on the application and the precise circumstances, some applications may allow unencrypted copies of the data to be stored in the swap file.

Deleted or 'lost' files

1.91 File systems keep a record of where data are located on a storage medium. The way data are stored will differ, depending on the software and the architecture of the method used to allocate blocks of storage for files (the file system architecture). In simple terms, the location of data on a storage medium is controlled by a file system. For instance, the storage medium can be divided into partitions and media blocks, and where this is the case, the file will be stored in a particular location in a partition. When a file is deleted, only the system's pointers in the filing system are deleted: the instruction to delete removes the pointer to the location of the file, but does not actually delete the file. Even where part of a file has been overwritten, it is often possible to recover part of the deleted file if the set of media blocks containing that file has not been completely overwritten. For this reason, in the majority of cases it is possible to recover data that has been deleted, depending on the amount of medium-writing activity that has been performed between the deletion of the file and the recovery process.[1]

1 Andy Jones and Christopher Meyler, 'What evidence is left after disk cleaners?' (2004) 1(3) Digital Investigation 183; 'Deleted File Recovery' (NIST), https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cftt/cftt-technical/deleted.

1.92 File systems also keep a record of those parts of the medium that are unusable or 'bad', so that no data will be written there. But a user may intentionally mark portions of the medium as 'bad' to hide substantial amounts of data in those portions. Such data could not be seen without the use of an appropriate media diagnostic or examination tool (since the operating system will automatically avoid making any use of these 'bad sectors'). Alternatively, when a device that is claimed to be non-functional is forensically restored or unlocked, it may be possible to discover or infer evidence of

wrongdoing on the device. This is illustrated by the case of *Sectrack NV v Satamatics Ltd*[1] concerning the misuse of confidential information. One of the defendants was in possession of a Blackberry device, which he claimed was frozen or locked. When the device was 'unlocked', it automatically downloaded various emails that the defendant had received, which implicated him in the misuse of confidential information.[2] Since this case, manufacturers of hand-held devices have developed extensive backup systems that permit the backing up of device data to other devices and storage facilities. In the future, without the use of encryption, it will be relatively difficult to delete data sufficiently for it to be beyond recovery.

1 [2007] EWHC 3003 (Comm), [2007] 12 WLUK 558.
2 [2007] EWHC 3003 (Comm) at [7].

1.93 However, it does not follow that the recovered data is genuine or trustworthy evidence just because it is found. There are numerous contexts in which data may be lost or damaged, and this will affect the credibility of any resulting data that is recovered. Examples include the corruption or loss of original or deleted data because of errors in the program, and interference with the data from extrinsic sources.[1] Further, it should be observed that the reliability of the recovered data as evidence would also be affected by the way in which a digital evidence professional carries out the examination and recovery process. If the process of investigation affects the evidence, it will be less reliable.

1 Peter Sommer, 'Downloads, logs and captures: Evidence from cyberspace' [2002] CTLR 33; Eoghan Casey, 'Error, uncertainty, and loss in digital evidence' (2002) 1(2) Intl J of Digital Evidence; Caroline Allinson, 'Audit trails in evidence – a Queensland case study' (2001) 1 JILT; and 'Audit trails in evidence: analysis of a Queensland case study' (2003) 2 JILT.

Simulations, data visualizations, augmented and virtual reality

1.94 There is an increasing use of computer-generated sequences as a method of presenting evidence in legal proceedings. Often these are designed to predict the behaviour or outcome of an incident, based on mathematical models that are built on the well-known behaviour of natural systems in chemistry, biology, physics and engineering.[1]

1 Computer simulation (Wikipedia), https://en.wikipedia.org/wiki/Computer_simulation; see 'Computer generated animations and simulations' in Chapter 2 for a more detailed discussion of the legal issues and citation of relevant authorities, legal and non-legal.

Encryption and obfuscated data

1.95 Encryption has been known and used since ancient times, especially to protect military communications.[1] But the advent of computers and the Internet has intensified the use of cryptography to secure information and communications. The underlying concept remains the same, however: since sensitive information in its unencrypted form may be read by people with unscrupulous motives or be exposed to interceptors, encryption converts the information in its unencrypted form (referred to as plaintext) into a form which is non-readable by unauthorized parties (referred to as ciphertext). Only authorized parties can decrypt the ciphertext back into its readable form. Encryption is classically combined with authentication, allowing the recipient to

verify who created the information and that it has not been tampered with in transit. The data that allows a recipient to verify the authenticity of a message is known as a digital signature, but this is quite separate from the legal concept of a signature.

1 John F. Dooley, *History of Cryptography and Cryptanalysis: Codes, Ciphers, and Their Algorithms* (Springer 2018), 13–18.

1.96 Encryption and authenticity verification are achieved through the use of a third piece of information known as a key. There are two main types of keys in cryptographic systems: symmetric key and asymmetric (or public) key schemes. In symmetric key schemes, the key that is used to encrypt and/or authenticate the plaintext is the same key used to decrypt and/or verify the ciphertext. In other words, both the sender and recipient must share the same key in order to achieve secure communication. In asymmetric key schemes, the private part of the key is used to decrypt information or create a digital signature, and the public part of the key is used to encrypt the information or verify the authenticity of a message with a corresponding digital signature. Asymmetric and symmetric cryptographic systems are often combined to take advantage of the efficiency of symmetric cryptography and the flexibility of asymmetric cryptography.

1.97 For instance, the Hypertext Transfer Protocol Secure (HTTPS), an extension of the Hypertext Transfer Protocol (HTTP), is used to secure communications over the Internet by authenticating a website, protecting the privacy of the sender and the recipient, and preserving the privacy and authenticity of the data exchanged while the data is in transit.[1] The authentication aspect of HTTPS is achieved by a trusted third party digitally signing a server-side document (known as a digital certificate) that certifies that the public key is owned by the sender responsible for the website, while the privacy aspect of HTTPS is achieved by the encryption of the data transmitted between the sender and recipient using symmetric cryptography keys that are unique to each connection.[2]

1 HTTPS (Wikipedia), https://en.wikipedia.org/wiki/HTTPS.
2 Transport Layer Security (Wikipedia), https://en.wikipedia.org/wiki/Transport_Layer_Security.

Artificial intelligence and machine learning

1.98 Using a definition dating back to the 1970s, artificial intelligence (AI) can, in a suitably technology-neutral way, be defined as '[The automation of] activities that we associate with human thinking, activities such as decision-making, problem solving, and learning'.[1] While the term first appeared in the 1950s, interaction between law and AI entered the academic mainstream in the 1980s and 1990s through organizations such as JURIX[2] and the International Association for Artificial Intelligence and Law.[3] These were the halcyon days of the 'symbolic manipulation' approach to AI, exemplified through the quest for 'expert systems' that contained symbolic representations of expert knowledge in their knowledge base, usually in the form of 'If/Then' rules, and that were able to perform logical operations on it. Systems of that type (which are still around today and continue to be developed and refined) include programs that help crime investigators to structure the evidence they collect as part of an investigation,

evaluate its probative weight and turn it into logically compelling arguments.[4] More complex systems combine rule-based knowledge representation with statistical or probabilistic reasoners, for instance Bayesian networks, to analyse and evaluate a broader range of evidence types.[5] While these systems help investigators to analyse and structure evidence, they do not generate new types of digital evidence. As a result, they are outside the scope of this chapter.

1 Richard Bellman, *An Introduction to Artificial Intelligence: Can Computers Think?* (Boyd & Fraser Publishing Company 1978), 3–4.
2 http://jurix.nl/.
3 http://www.iaail.org/.
4 Ephraim Nissan, *Computer Applications for Handling Legal Evidence, Police Investigation and Case Argumentation* Volume 5 (Springer Science & Business Media 2012); Jeroen Keppens and Burkhard Schafer, 'Knowledge based crime scenario modelling' (2006) 30(2) Expert Systems with Applications 203.
5 Floris Bex, Peter J. van Koppen, Henry Prakken and Bart Verheij, 'A hybrid formal theory of arguments, stories and criminal evidence' (2010) 18(2) Artificial Intelligence and Law 123, DOI: 10.1007/s10506-010-9092-x.

1.99 The results of approaches that started to emerge in the mid-1990s to enable a way of knowledge representation and knowledge sharing that preserved more of the meaning, or semantics, of our knowledge are closer to being digital evidence generated by AI. This became of particular importance with the emergence of the semantic Web and its aim to establish 'a common framework that allows data to be shared and reused across application, enterprise, and community boundaries',[1] one of the significant technologies underpinning the World Wide Web. Ontology-based legal AI would then try to represent the knowledge of an investigator, or the knowledge we have about a particular crime, by building taxonomies and classification networks. Such a formal ontology would, for instance, allow the software to reason about the information it finds on a website to determine if the text falls under the category of 'committing incitement', which in turn falls under the category of 'committing a criminal offence'. Ontology-based AI systems have been used, for instance, to enable search engine indexing services to autonomously identify websites that host content that violates banking regulations or are in other ways fraudulent, or to identify whether a set of digital VAT receipts are likely to support a claim for VAT fraud.[2] This part-automation of the investigative process can raise issues for the law of evidence, for instance how rules on searches can be analogized: whether it makes sense to attribute 'reasonable suspicion' to the software agent, or whether this resides with its human (police) operators, for instance. However, more recent developments in AI have moved beyond these 'symbolic' approaches to knowledge representation and reasoning to probabilistic or statistic approaches, using machine learning as a way to implement them.

1 https://www.w3.org/2001/sw/SW-FAQ.
2 John Kingston, Burkhard Schafer and Wim Vandenberghe, 'No model behaviour: ontologies for fraud detection' in V. Richard Benjamins, Pompeu Casanovas, Joost Breuker and Aldo Gangemi (eds.) *Law and the Semantic Web* (Springer 2005), 233–247; Dimitris Kanellopoulos, Sotiris Kotsiantis and Vasilis Tampakas, 'Towards an ontology-based system for intelligent prediction of firms with fraudulent financial statements', *2007 IEEE Conference on Emerging Technologies and Factory Automation (EFTA 2007)* (IEEE 2007).

1.100 Before examining machine learning in more detail, it should be noted that many forensic subdisciplines have relied for a long time on complex statistics software programs for data analysis that can no longer be verified by human experts, thus already creating the problem of 'black box' algorithms that are a main concern for current AI systems. Forensic DNA analysis, and in particular advanced methods such as low copy number DNA testing, requires complex statistical analysis that is carried out by computer programs.[1] Similarly, forensic use of neuroimaging such as FMRI scans rely on complex statistical software tools that mediate between the 'raw data' collected by sensors and the visual representation of a brain for the human analyst. Even though, especially in the latter case, significant parts of the evidence are computer-generated, new evidential requirements for electronic evidence have not normally been applied to the use of computer technology within established forensic disciplines. To the extent that the accuracy and reliability of these programs has been discussed at all, they have been dealt with through certification and standardization, rather than a forensic computing analysis of individual machines and their use in an individual case.

1 Wing K. Fung, Yue-Qing Hu and Yuk-Ka Chung, 'On statistical analysis of forensic DNA: theory, methods and computer programs' (2006) 162(1–3) Forensic Science International 17, DOI: 10.1016/j.forsciint.2006.06.025.

1.101 Machine learning (ML) refers to the broad category of computational approaches to solving problems through applying statistical techniques to identify patterns in data, rather than having a developer explicitly specify detailed steps to follow. In this way, machine learning systems can be said to demonstrate artificial intelligence; that is, their approach contains some characteristics of the approach a human would take to carry out such a task. Machine learning works by 'allow[ing] systems to learn directly from examples, data, and experience'.[1]

1 Royal Society, 'Machine learning: the power and promise of computers that learn by example' (April 2017) 19, https://royalsociety.org/~/media/policy/projects/machine-learning/publications/machine-learning-report.pdf.

1.102 There are three main permutations of ML. First, in supervised machine learning the machine system is trained with data items that each have an associated label. The ML system learns the relationship between data items and labels and is then able to estimate the most likely label that should be associated with data items it has not encountered. For example, a ML system could be provided with many photographs of street signs that each have been transcribed by a human, then be tasked with identifying photographs of street signs encountered by a self-driving car. Second, in unsupervised machine learning data is not labelled. The ML system identifies patterns within the data items in order to group items that are similar or to summarise the important characteristics of the data. For example, supermarket customers could be grouped into categories based on their shopping habits, so as to direct advertising more effectively. Third, with reinforcement learning the ML system interacts with the physical world or a system of rules and develops a strategy that achieves a specified objective. For example, a robot could be given the task of reaching a point as quickly as possible, given access to a collection of motors and sensors.[1]

1 Royal Society, 'Machine Learning', 20.

1.103 Because ML is a general technique for automating useful tasks that require human intelligence for successful completion, the range of applications possible with ML are wide and varied. Law enforcement authorities such as police officers may be equipped with body-worn video cameras that record crucial evidence in real time[1] and can execute automated facial recognition.[2] Patrol cars are equipped with in-car cameras that automatically read number plates to find matches for vehicles and their owners.[3] The gathering of criminal intelligence and predictive policing are also being helped by advancements in ML.[4] In banking, logistics, medicine, electronic commerce and other industries, ML systems are used in applications that range from fraud and accident detection to productivity improvement, from diagnostics and safety assurances to customization of goods and services, to enable rapid and accurate decision making.[5] For this reason, the range of evidence that is generated by ML devices is practically limitless. This in turn engenders a careful review of the nature of such evidence, including an examination of the authentication of such evidence and whether the admission of it in legal proceedings breaches the rule against hearsay.[6]

1 Ben Bowling and Shruti Iyer, 'Automated policing: the case of body-worn video' (2019) 15(2) Int JLC 140; *DPP v Young* [2018] EWHC 3616 (Admin), [2018] 12 WLUK 67 (accepting body-worn video as evidence).

2 See *R. (on the application of Bridges) v Chief Constable of South Wales* [2019] EWHC 2341 (Admin), [2020] 1 WLR 672, [2020] 1 All ER 864, [2019] 9 WLUK 9, [2020] 1 Cr App R 3, [2019] HRLR 16, [2019] ACD 122, Times, 9 December 2019, Times, 11 December 2019, [2019] 11 CLY 1389, regarding a challenge to privacy and data protection from police use of automated facial recognition technologies on body-worn videos.

3 For instance, see *R. v Doyle (Hugh), R v Wood (Carl), R. v Lincoln (William)* [2017] EWCA Crim 340, [2017] 2 WLUK 194, admitting automatic number plate recognition evidence as part of the evidence of the movement of accused's cars; *R. v Brown (Nico)* [2019] EWCA Crim 1143, [2019] 1 WLR 6721, [2019] 7 WLUK 41, [2019] 2 Cr App R 25, [2020] Crim LR 71, [2019] CLY 647, admitting automatic number plate recognition evidence.

4 Walter L. Perry, Brian McInnis, Carter C. Price, Susan C. Smith and John S. Hollywood, 'Predictive policing: the role of crime forecasting in law enforcement operations' (Rand Corporation 2013), https://www.rand.org/content/dam/rand/pubs/research_reports/RR200/RR233/RAND_RR233.pdf; Patrick Perrot, Gendarmerie Nationale, Ministry of Interior, Paris, France, 'What about AI in criminal intelligence? From predictive policing to AI perspectives', European Police Science and Research Bulletin, Issue 16, Summer 2017, 65–76, https://bulletin.cepol.europa.eu/index.php/bulletin/article/download/244/208/; Albert Meijer and Martijn Wessels, 'Predictive policing: review of benefits and drawbacks' (2019) 42(12) International Journal of Public Administration 1031, https://www.tandfonline.com/doi/full/10.1080/01900692.2019.1575664.

5 Artificial intelligence in industry (Wikipedia), https://en.wikipedia.org/wiki/Artificial_intelligence_in_industry.

6 See Daniel Seng and Stephen Mason, 'Artificial intelligence and evidence' (2021) 33 SAcLJ 241.

Simulations, data visualizations, augmented and virtual reality

1.104 In addition to collecting and evaluating evidence, an important role of AI and related technologies is to help communicate complex data to the trier of facts. This can range from data visualization tools that, for instance, make channels of email communication within an alleged criminal network visible, to visual recreation of crime scenes or dynamic reconstructions of putative events.[1] This technology is described using a variety of terms, including 'computer simulations', 'computer animation' and 'data visualization'. Where the simulation allows for the creation of a three-dimensional sequence in which the viewer can participate, move around the computer-simulated environment and look at the incidents from different viewpoints, the technology is

described as 'virtual reality' or 'augmented reality', the distinction being that in augmented reality the virtual representations of objects is also overlaid with real-world objects and items to alter one's perception of the real-world environment.[2] This can be achieved through the use of virtual reality headsets, which offer a particularly radical way to enable judges or jurors to 'relive' putative events in 3D space.[3]

1 The reader should read the text in this part in combination with the detailed discussion of the legal issues in 'Computer-generated animations and simulations', Chapter 2. Minhua Ma, Huiru Zheng and Harjinder Lallie, 'Virtual reality and 3D animation in forensic visualization' (2010) 55(5) Journal of Forensic Sciences 1227; Isabella Aquila MD, Ph.D., Matteo A. Sacco MD, Giuseppe Aquila MS, Roberto Raffaele MS Alfredo Manca, Giuseppe Capoccia, Fabrizio Cordasco MD and Pietrantonio Ricci MD, Ph.D., 'The reconstruction of the dynamic of a murder using 3D motion capture and 3D model buildings: the investigation of a dubious forensic case' (2019) 64(5) Journal of Forensic Sciences 1540; see 'Computer-generated animations and simulations' in Chapter 2 for a more detailed discussion of the legal issues and citation of relevant authorities, legal and non-legal.

2 Augmented reality (Wikipedia), https://en.wikipedia.org/wiki/Augmented_reality.

3 Till Sieberth, Akos Dobay, Raffael Affolter and Lars C. Ebert, 'Applying virtual reality in forensics – a virtual scene walkthrough' (2019) 15(1) Forensic Science, Medicine and Pathology 41.

1.105 Factual data from an investigation is input into a forensic computer simulation software, which then associates the data with the 'generic world knowledge' in the knowledge base of the AI. This can then reproduce crime scenes and demonstrate how an alleged activity at various points in time could have taken place, while observing physical constraints such as gravity and other considerations.[1] The jurors may then 'see' how a car collided with a wall after swerving around an animal,[2] or how a person killed the victim, so that the reconstruction matches the pathologist report about, for example, the trajectories of bullets and our general knowledge of human anatomy, behaviour of firearms or the law of optics when taking aim.[3] These reproductions usually combine computer graphics, natural language processing, computer vision, motion tracking and forensic computing to turn defence and prosecution hypotheses into 'observable' stories that can then be tested.

1 G. D. Sloan and J. Talbott, 'Forensic application of computer simulation of falls' (1996) 41(5) Journal of Forensic Sciences 782.

2 Kristin L. Fulcher, 'The jury as witness: forensic computer animation transports jurors to the scene of a crime or automobile accident' (1996) 22 U Dayton L Rev 55.

3 Lars C. Ebert, Tuan T. Nguyen, Robert Breitbeck, Marcel Braun, Michael J. Thali and Steffen Ross, 'The forensic holodeck: an immersive display for forensic crime scene reconstructions' (2014) 10(4) Forensic Sci Med Pathol 623.

1.106 While these technologies can help to communicate complex facts to laypeople during a trial, there are concerns about their 'authenticity' for evidential purposes, and also their potential prejudicial effect, even in cases where the reconstructions are as faithful as possible.[1] Computer simulations do not fall easily within any of the existing categories of evidence because they are synthetic evidence: they are not contemporaneous records of the facts but are produced after the relevant events have occurred.[2] One problem that can arise is that the reconstruction will add details that are neither supported by eyewitness evidence, nor by universal scientific facts from the AI's knowledge base, but are default design choices made by the programmers. For instance, this can include choosing a colour scheme when visualizing brain activity from a scan, or having an intact headlight on a car directly before a crash, even though there is no direct witness statement to substantiate such an assertion. Sometimes these

design choices are salient for evaluation of the event; at others they subtly influence juror perception.[3] Therefore, computer simulations should be seen for what they are – representations of opinions about facts. They should be treated as expert evidence and should be admitted only when reasonably required and with the judge's permission to resolve the proceedings.[4] While computer simulations have been admitted in both criminal and civil cases,[5] their limited use has been permitted only as mechanisms to enable the disputed issues to be refined, and only when the raw data that serve as the source of simulations are of sufficiently high quality.[6]

1 The legal issues are discussed in more detail in 'Computer-generated animations and simulation', Chapter 2.

2 Moya Clifford and Katie Kinloch, 'The use of computer simulation evidence in court' (2007) 24 Computer Law and Security Report 169.

3 See 'Computer-generated animations and simulation', Chapter 2 for relevant citations.

4 The foundational legal issues are discussed in more detail in 'Computer-generated animations and simulation', Chapter 2.

5 For example, see *R. v Maloney (Gerald)* [2003] EWCA Crim 1373, [2003] 5 WLUK 565; *The Owners of the Ship Pelopidas v The Owners of the Ship TRSL Concord* [1999] 2 All ER 737 (Comm), [1999] 2 Lloyd's Rep 675, [1999] 10 WLUK 259, [2000] CLY 4677; *Owners of the Global Mariner v Owners of the Atlantic Crusader, sub nom. Global Mariner, The, Atlantic Crusader, The* [2005] EWHC 380 (Admlty), [2005] 2 All ER (Comm) 389, [2005] 1 Lloyd's Rep 699, [2005] 3 WLUK 782, [2005] 1 CLC 413, (2005) 155 NLJ 594, [2005] CLY 3794.

6 Clifford and Kinloch, 'The use of computer simulation evidence in court', 173.

Transparency and explainability

1.107 Machine learning systems apply probabilistic reasoning and statistical techniques to solve problems. They therefore introduce the same types of error as in more traditional applications of statistics.[1] For example, the data on which they are trained might not be representative of reality, and so any conclusions drawn may not be accurate, or the uncertainty present in the output of the system might not be properly interpreted. Furthermore, the complexity of machine learning systems introduces sources of error. With the advent of machine learning and its implementation in 'artificial intelligence' systems, concerns have been rightly raised as to whether autonomous or intelligent detection systems are 'traceable, explicable and interpretable'[2] – often referred to in short as 'explainability'. The requirement for explainable autonomous or intelligent systems, reflected as the Principle of Transparency in the IEEE (Institute of Electrical and Electronic Engineers) rulebook on Ethically Aligned Design, ensures that the operation of such systems is transparent to a wide range of users.[3] In addition, depending on the type of machine learning algorithms used and implemented, the degree and extent of the explainability of the results from such algorithms may vary greatly. Statistical multivariate regression or random forest models built on existing data may be more traceable, explicable and interpretable by virtue of their algorithmic design,[4] but they may lack the requisite accuracy and prediction power.[5] On the other hand, deep learning neural network models, with their higher dimensionality architectures, may produce models that have the necessary prediction power,[6] but may suffer from issues of explicability from their relative opacity and an inability to generalize or deal with corner cases.[7] The requisite level of transparency and explainability that is required to provide the foundational substantiation for admitting evidence produced by such systems in legal proceedings will depend on the purposes for which the evidence is adduced.

1 Colin Aitken, Paul Roberts and Graham Jackson, 'Communicating and interpreting statistical evidence in the administration of criminal justice: 1. Fundamentals of probability and statistical evidence in criminal proceedings' (Royal Statistical Society), https://www.maths.ed.ac.uk/~cgga/Guide-1-WEB.pdf.
2 IEEE, Ethically Aligned Design, Principle 4 – Transparency (March 2018), 29, https://standards.ieee.org/content/dam/ieee-standards/standards/web/documents/other/ead_v2.pdf.
3 IEEE, Ethically Aligned Design, Principle 4 – Transparency.
4 For instance, see Rich Caruana and Alexandru Niculescu-Mizil, 'An empirical comparison of supervised learning algorithms' in *ICML 2006, Proceedings of 23rd International Conference on Machine Learning* (Association for Computing Machinery 2006), 161–168, https://www.cs.cornell.edu/~caruana/ctp/ct.papers/caruana.icml06.pdf; Vijay Khadse, Parikshit N. Mahalle and Swapnil V. Biraris, 'An empirical comparison of supervised machine learning algorithms for Internet of Things data' in *2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA)* (IEEE 2018), https://ieeexplore.ieee.org/document/8697476.
5 For example, see Michal Hrabia, 'Deep learning vs. machine learning', 8 February 2020, https://towardsdatascience.com/deep-learning-vs-machine-learning-e0a9cb2f288.
6 Decision tree learning (Wikipedia), https://en.wikipedia.org/wiki/Decision_tree_learning.
7 But see Geoffrey Hinton, Oriol Vinyals and Jeff Dean, 'Distilling the knowledge in a neural network', in NIPS Deep Learning Workshop (2015), https://arxiv.org/pdf/1503.02531.pdf; Minsuk Kahng, Pierre Y. Andrews, Aditya Kalro and Duen Horng Chau, 'ActiVis: visual exploration of industry-scale deep neural network models' (2018) 24(1) IEEE Transactions on Visualization and Computer Graphics http://arxiv.org/abs/1704.01942.

AI adversarial attacks

1.108 As AI systems are increasingly used, there is a need to verify that they work reliably and appropriately, especially when they are used in open environments which may expose the systems to real-world data on which they have not been previously trained. When this happens, a system may produce unexpected results or behave in an unexpected way. Where AI systems are being set to continue to 'learn' from their new environment and update their models, this may also cause a system to 'unlearn' its models and crystallize the unexpected results or behaviour as correct or expected responses.[1]

1 Royal Society, 'Machine learning', 112.

1.109 Considerable research is being undertaken to investigate AI systems for such weaknesses. Known as 'adversarial attacks', these generally attempt to expose AI systems to novel environments and track their unexpected behaviour. While 'good' adversarial attacks attempt to detect such weaknesses to increase the robustness of AI systems, 'bad' adversarial attacks may exploit such weaknesses for gain or to cause disruption. When evidence is generated from AI systems that have or could have been compromised, questions regarding the robustness, transparency and explainability of AI systems will be valid when authenticating or evaluating such evidence.

Defining electronic evidence

1.110 Defining what we mean by 'electronic' evidence is not an easy task. The type of evidence that we are dealing with has also been variously described as 'digital evidence' or 'computer evidence'. All three terms express some aspects of our pre-theoretical intuition that this type of evidence has some distinctive features that

set it apart from other means of proof. However, defining what these distinguishing features are is far from straightforward. The rapid technological change in the field of information technology means that any definition narrowly tailored to the current state of technology faces the risk of becoming obsolete rapidly. Definitions that are suitably future-proof by contrast tend to be too abstract and will cut across traditional divisions and categories in the law of evidence. For our purpose, we will take as our approach the need of the lawyer to turn certain artefacts – digital objects – into evidence that can be used as proof in legal proceedings. Based on this, we can develop a workable definition that will suit most applications and purposes.

1.111 Various definitions of electronic evidence exist. These include 'information of probative value that is stored or transmitted in binary form'[1] and 'information stored or transmitted in binary form that may be relied on in court'.[2] In his treatise, Casey defines digital evidence as:

> any data stored or transmitted using a computer that support or refute a theory of how an offense occurred or that address critical elements of the offense such as intent or alibi.[3]

1 Scientific Working Groups on Digital Evidence and Imaging Technology, 'Model Quality Assurance Manual for Digital Evidence Laboratories' (v3, 13 September 2012), https://www.swgde.org/documents/published.

2 International Organisation on Computer Evidence, 'G8 proposed principles for the procedures relating to digital evidence' (2000), http://web.archive.org/web/20030207173420/http://ioce.org/G8_proposed_principles_for_forensic_evidence.html. This definition was adopted by the US Department of Justice Office of Justice Programs, National Institute of Justice, in *Electronic Crime Scene Investigation: A Guide for First Responders* (US Department of Justice 2001) and *Forensic examination of digital evidence: A guide for law enforcement* (US Department of Justice 2004).

3 Eoghan Casey, *Digital Evidence and Computer Crime* (3rd edn, Elsevier 2011), 7.

1.112 Although the emphasis of this definition is on criminal investigations, it is a wider definition than the previous definitions, and it usefully explicates certain important aspects of electronic evidence. For instance, the reference to 'data' is to information that is held in electronic form, such as text, images, audio and video files. Also, the word 'computer' must be understood in its widest possible sense, and incorporates any device that stores, manipulates or transmits data. In addition, the definition implies that the evidence must be relevant and admissible, a question that can only be answered after we know what the electronic evidence, whether admissible or inadmissible, actually is. A project funded by the EU entitled 'European Informatics Data Exchange Framework for Court and Evidence' (March 2014 – October 2016)[1] set out a number of definitions of electronic evidence in 'D2.1 – EVIDENCE Semantic Structure', 1.2, and offered a definition at 1.6.1 that is strikingly similar to the one set out below:

> Electronic evidence is any data resulting from the output of an analogue device and/or a digital device of potential probative value that are generated by, processed by, stored on or transmitted by any electronic device. Digital evidence is that Electronic evidence which is generated or converted to a numerical format.

1 http://www.evidenceproject.eu/.

1.113 With the aim of offering a wider-ranging definition that includes civil and criminal cases, we propose the following definition:

> Electronic evidence: data (comprising the output of analogue devices or data in digital form) that is generated, processed, stored or communicated by any digital device, computer or computer system or conveyed over a digital transmission system that has the potential to make the factual account of either party more probable or less probable than it would be without the evidence.

1.114 This definition has three elements. First, the reference to 'data' includes all forms of evidence created, processed or stored in a device that can, in its widest meaning, be considered a computer.[1] It is used here in a non-technical sense, meaning roughly 'a gathered body of facts'. While computer scientists often distinguish between 'data' and 'programs', this distinction is not helpful for our purposes. For instance, in a copyright case, if a defendant has allegedly installed an unauthorized operating system, the presence of the system on his computer is electronic data for our purposes.[2] Second, the definition includes the various devices by which data can be stored or transmitted, including analogue devices that produce an output. Ideally, this definition will include any form of a digital device, whether it is a computer (as we presently understand the meaning of a computer), telephone systems, wireless telecommunications systems and networks such as the Internet, and mobile devices and embedded systems such as smart cards and navigation systems. Third, the definition restricts the data to information that is relevant to the process by which a dispute, whatever the nature of the disagreement, is to be decided by an adjudicator, whatever the form and level the adjudication takes. This part of the definition includes one aspect of admissibility – relevance only – but does not use 'admissibility' in itself as a defining criterion, because some evidence will be admissible but excluded by the adjudicator within the remit of their authority, or inadmissible for reasons that have nothing to do with the nature of the evidence. This could be, for instance, because of the way it was collected, such as in violation of privacy or in breach of legal professional privilege. However, the definition is limited to those items of evidence offered by the parties as part of the fact-finding process. This contextual, teleological aspect of the definition excludes, for instance, electronic documents that are created during a trial in a purely administrative capacity, such as email reminders of the date of the hearing sent to the parties by the court administrators. Of course, the very same data can become 'electronic evidence' if offered in an appeal to show that the information was not sent out in a timely fashion, if this is part of the complaint.

1 Excluding the human brain, which has also been compared to a computer, though this line is becoming increasingly difficult to maintain, especially with the increasing feasibility of human–computer interfaces.

2 Obviously, we also do not use 'data' in the way it is sometimes understood in telecommunications, where only digital, but not analogue, information is sometimes referred to as data.

1.115 A particularly important form of evidence in all developed legal systems is proof by document. Consequently, electronic documents are a particularly important form of electronic evidence.[1] They are also a particularly good example to illustrate some of the pertinent characteristics of electronic evidence. Because of the importance of documents for our daily life, and the way we handle them as folders, documents and photocopies, many of the most important software applications intentionally mimic the 'look and feel' of traditional, paper-based stationery when dealing with electronic documents. We therefore create digital objects that are called documents and have the same visual appearance as documents typed on paper. We 'turn' their

'pages' (as with some electronic readers for ebooks and ejournals), 'put' them in files and folders, and discard them in digital 'waste paper' baskets or trash bins. Email also intentionally mimics the traditional letter, from the letter icon on the inbox to the pencil icon for 'writing' a new message. This inauthentic familiarity can create the misleading impression that the electronic document exists somewhere on the computer as a single, complete whole, and maintains its structural integrity even when the file is closed or the computer is switched off, in the same way a paper document continues to exist when it is put out of sight into a folder. This overly naive view underestimates the differences between electronic and paper-based documents, and potentially also overestimates their reliability. The converse, however, can equally happen, where a more sophisticated user sees through the processes that intentionally create the appearance of a paper document and dismisses all electronic evidence as essentially deceptive, spurious and unreliable, rather than as a new kind of document. This becomes a particular problem for those jurisdictions whose evidence law has formal definitions of 'document' and proof by document, for instance the German *Urkundenbeweis*. In these jurisdictions, legal rather than factual issues can increase the chasm between electronic and traditional documents and bridging legislation is required to make electronic documents also 'documents-in-law'.

1 William Kent, *Data and Reality* (2nd edn, 1stBooks 2000) for an interesting discussion of how humans perceive and process information, and how humans impose this outlook on data processing machines.

1.116 A better and more realistic approach is to acknowledge that documents in electronic form have particular characteristics that affect both the test for authenticity (or provenance), should authenticity be in issue, and the way the electronic evidence is secured and handled at the pre-trial stage. It is the thesis of this text that evidence in electronic form ought to be subject to a more rigorous mechanism than would normally be associated with a document extant on physical media. John D. Gregory has observed that the integrity of physical documents is 'often protected fairly casually',[1] yet the same could not be said of documents that are created, modified, communicated, stored and deleted in electronic form. For instance, a forensic document examiner can analyse the chemical properties of the ink on a paper document to determine if more than one writing utensil was used, or if the composition of the ink is consistent with the time at which the document was allegedly created, or the material properties of the paper. Once the document is written, changes or alterations will also leave physical traces. With paper documents, we therefore have a clear understanding, routinely recognized in evidence law, that the original document[2] and copies of it are objects with different physical properties. This crucial distinction becomes problematic in the electronic medium, where not only are copy and original indistinguishable, but the very act of working on 'a' document will also automatically and routinely create numerous copies on the computer without the knowledge of the author, copies that can persist and override earlier drafts even when the document is completed. As outlined above in the discussion about metadata, documents in electronic form have a number of features that present particular challenges that a paper carrier in the physical world does not.

1 John D. Gregory, 'Authentication rules and electronic records' (2002) 81 Can Bar Rev 529, 533.

2 For the meaning of 'original', see Steven W. Teppler, 'Digital data as hearsay' (2009) 6 Digital Evidence and Electronic Signature Law Review 7, 9 n 18; Stephen Mason, 'Electronic evidence and the meaning of "original" ' (2009) 79 Amicus Curiae 26, http://sas-space.sas.ac.uk/2565/; Luciana Duranti

and Corinne Rogers, 'Trust in digital records: an increasingly cloudy legal area' (2012) 28(5) Computer Law and Security Review 522, 527 with further references.

The dependency on machinery and software

1.117 The reader can easily read the content of a traditional document long after it was created with little or no additional costs; the only things necessary are good eyesight and a knowledge of the language in which the document is written. Data in electronic form by contrast is dependent on hardware and software. The data requires an interpreter to enable it to be rendered into human-readable form. A user cannot create or manipulate electronic data without appropriate hardware. Therefore, an electronic document should not be treated as an object 'somewhere there' on the digital device, in the same way as a paper book is in a library. Instead, the electronic document is better understood as a process by which otherwise unintelligible pieces of data that are distributed over the storage medium are assembled, processed and rendered legible for a human user. In this sense, the electronic document is nowhere: it does not exist independently from the process (software) that recreates it on the device (hardware) every time a user opens it on screen. If those electronic documents were produced in the 1990s, many thousands of the programs used to create them are now no longer available commercially, and even if such software were available, it might be impossible to load it on a modern operating system. An additional problem for older data is that it might be necessary to have a specific machine with specific software loaded in order to read the data.[1] This can cause additional expense to a party, as in the case of *PHE, Incorporated dba Adam & Eve v Department of Justice*,[2] where PHE was ordered to review information contained in a database, even though no program existed to enable it to obtain the information requested by the Department of Justice.

1 For instance, the jazz club Ronnie Scott's, based in Soho, London, was refurbished in 2005–2006. As each part of the club was renovated, so large numbers of recordings of jazz musicians and singers, such as Dizzy Gillespie, Ella Fitzgerald, Chet Baker, Sarah Vaughan and Buddy Rich, that had been recorded during live performances were discovered. Some of the recordings were made on tapes that could only be played on machines that were no longer in the possession of the club. Report by Bob Sherwood, 'Ronnie Scott's jazz club to release archive of the greats' *Financial Times* (London, 28 June 2006) 1.

2 139 F.R.D. 249 (D.D.C. 1991); a similar problem was considered by Vinelott J in *Derby & Co Ltd v Weldon (No. 9)* [1991] 1 WLR 652, [1991] 2 All ER 901, [1990] 7 WLUK 300, [1992] CLY 3472.

The mediation of technology

1.118 Data in electronic form must be rendered into human-readable form through the mediation of a set of technologies. This means differences occur in how the same source object is displayed in different situations. A good example common to all users of the Internet is that a website can look very different depending on what type of screen and what browser is used, among other things. As a result, there can be no concept of a single, definitive representation of a particular source digital object. This can have obvious legal repercussions. An electronic contract document carelessly drafted may informally refer to the 'paragraphs' of the document without enumerating them since the formatting on the author's computer makes them plainly visible through line breaks in the text. Sent by email to the buyer and opened on her

machine with a different software program, this formatting data may be unreadable and the paragraphs no longer apparent. Another example can be found in the changed representations of emojis (ideograms used in an electronic message similar to older ASCII emoticons). For instance, in 2016 Apple controversially changed a 'hand gun' emoji into a 'water pistol' emoji. However, when a message containing this emoji is sent to a non-Apple device, it could appear on the recipient's machine as a cartoon image of a real gun.[1] If a message such as 'bring <gun emoji> to our meeting' or 'retract that or I come with my <gun emoji>' is sent, what was intended by the sender as a light-hearted joke may look like a threat for some recipients, depending on what device they are using.

1 Bonnie Malkin, 'Water pistol emoji replaces revolver as Apple enters gun violence debate' *The Guardian* (London, 2 August 2016), https://www.theguardian.com/technology/2016/aug/02/apple-replaces-gun-emoji-water-pistol-revolver-violence-debate.

1.119 With traditional evidence, the act of observing or analysing a crime scene should not be allowed to alter it – a problem commonly known as 'contamination'. In contrast, with electronic evidence the mere act of starting a computer and opening a document changes it, for instance by altering its metadata. Different observers using only marginally different machinery may recreate different versions of the object in question, and it is not an easy issue to decide which one of them should be regarded as 'more authentic'.

1.120 To manage this issue, we can adopt the approach taken with eyewitness evidence. We know that different observers of the same event will always provide subtly different accounts as to what happened. Furthermore, an observer will unintentionally and inevitably alter his memory of the events every time he tries to remember them. In the same way in which we try to minimise these effects through appropriate protocols and procedures – for instance, processes for an identification line-up or the interviewing of witnesses – protocols and procedures used by the digital evidence professional can minimize, but not eliminate, the distortion that the investigation creates. This means that it is crucial to identify appropriate standards, protocols, benchmarks and procedures, and the relevant hardware and software to be used, in relation to the management and use of any item of electronic evidence.

Speed of change

1.121 Technology in operating systems, application software and hardware changes rapidly. As a result, data in digital form may reach a point when they cannot be read, understood or used with new software or hardware. For instance, a software company may no longer produce software that is backward compatible or 'downward compatible' (where new versions of software are able to operate with older products). Technical obsolescence is a major problem that affects every aspect of the legal process, especially because the rate of change has now become so rapid.

1.122 The incessant speed of change has another consequence, again best explained by contrasting electronic evidence with traditional evidence. Eyewitness identification evidence is one of the oldest, if not the oldest, form of evidence used in trial. Despite this, the way we elicit and interpret eyewitness evidence in legal proceedings has changed

little over the centuries, and legal systems regularly keep culturally obsolete concepts such as the oath or dock identification for their ritual value. Fingerprint evidence is younger, with little over a hundred years of forensic use. But since its inception, while the basics of the discipline have remained the same, important changes in the way in which we interpret fingerprint evidence have been made, as have the features that we look for when establishing a match. A fingerprint expert trained 90 years ago would probably need at least a refresher course. DNA evidence is younger still, but in its 30-year history there have been considerable changes in the way in which DNA is collected, analysed and interpreted. An expert trained in the 1980s would require considerable retraining to be able to deal with current technology and equipment. For electronic evidence, the pace of change is faster still. This makes it all the more difficult to keep lawyers and other non-experts briefed of the relevant developments, and increases reliance on experts. It also means that it is essential that an expert has up-to-date knowledge and receives constant training, which may be more important than 'experience' in this field. A problem related to the rapid changes witnessed is the horizontal diversification of software and hardware. If a DNA expert analyses a blood sample, she need not know in advance the age, nationality or gender of the donor. By contrast, the digital evidence professional needs to know, and be trained for, the specific type of device and software that she is asked to analyse.

1.123 The ability of those investigating crimes is also hampered, for instance, by the speed at which the technology changes. In particular, obtaining relevant electronic tools to analyse a device forensically can be difficult for two reasons: first, the tools needed have yet to be devised, and second because, even if they are available, such tools can be expensive. In the case of *R. v Hallam (Sam)*,[1] Sam Hallam's conviction for three offences of murder, conspiracy to commit grievous bodily harm and violent disorder was quashed. One of the grounds of appeal was that Hallam was in possession of two mobile telephones, both of which were seized by the police. One of the telephones, a 3G telephone, contained evidence that suggested that Hallam's alibi was probably correct, and that the memories of both Hallam and his alibi witness as to the date they were together were defective. Neither telephone was the subject of forensic analysis. The observations by Hallett LJ, delivering the judgment of the court, illustrate the lawyers' naivety in the forensic investigation of the data.[2] She said:

> 65. … For reasons which escape us [the mobile phones] do not seem to have been interrogated by either the investigating officers or the defence team. We can understand why cell site evidence in relation to the use of the phones may have been of limited value given the close proximity of the masts, the various scenes, and the homes of those involved. However, given the attachment of young and old to their mobile phones, we cannot understand why someone from either the investigating team or the defence team did not think to examine the phones attributable to the appellant. An analysis of mobile phone evidence played a part in the investigation …
>
> 67. One reason proffered for the failure to examine the phone was that in 2004 the Metropolitan Police did not have the technology in-house to examine 3G telephones. However, given our limited knowledge, we would have thought that even a cursory check might have produced some interesting results. Further, it might be thought that the appellant would have alerted his defence team to the fact that he had taken photographs on his new phone in the days before and after the murder which might have jogged his memory and helped establish his whereabouts.

1 [2012] EWCA Crim 1158, [2012] 5 WLUK 518.
2 This highlights the need for lawyers to ensure they are competent to practice, for which see in particular Denise H. Wong, 'Educating for the future: teaching evidence in the technological age' (2013) 10 Digital Evidence and Electronic Signature Law Review 16; and Deveral Capps, 'Fitting a quart into a pint pot: the legal curriculum and meeting the requirements of practice' (2013) 10 Digital Evidence and Electronic Signature Law Review 23.

1.124 Because the electronic evidence in the telephone supported the defendant's alibi and contradicted the eyewitness testimony, which Hallett LJ had described as 'rock solid', the court concluded that this was a case of mistaken identity and acquitted the defendant.[1]

1 [2012] EWCA Crim 1158 at [77].

Volume and replication

1.125 Electronic documents are easy to manipulate: they can be copied,[1] altered, updated, or deleted (and deleted in the electronic environment does not mean expunged). The integration of telecommunications and computers to form computer networks (such as wide area networks and the Internet) further allows for data to be created and exchanged in far greater volumes than had previously been possible, and across physical and geographical boundaries. In essence, email, instant messaging and Internet communications are a 'duplicate and distribute' technology.[2] Once computers are networked together in this fashion, an electronic document may be transmitted and numerous copies distributed around the world very rapidly. By way of example, in *AMP v Persons Unknown*[3] the claimant's mobile telephone was stolen or lost. It was not protected with a password. A number of photographs were stored on the telephone, some of which were of an explicit sexual nature. Shortly after the telephone went missing or was stolen, digital images were uploaded on various social media websites, enabling others to download and share the images. Some of the social media sites removed the images when requested, but the images were seeded onto a Swedish BitTorrent node and continued to circulate. Ramsey J decided that the claimant was entitled to an interim injunction to prevent the distribution of the digital images, either by conventional downloading from a site or by downloading using the BitTorrent protocol. To reflect the ease with which the images could be obtained and distributed, the injunction was granted in the following terms:

> 50. I therefore grant an interim injunction in the following terms against persons unknown being those people in possession or control of any part or parts of the files listed in Schedule C to the order who are served with this order:
>
> (1) shall immediately cease seeding any BitTorrent containing any part or parts of the files listed in Schedule C of this Order.
>
> (2) must not upload or transmit to any other person any part or parts of the files listed in Schedule C of this Order.
>
> (3) must not create any derivatives of any of the files listed in Schedule C of this Order.
>
> (4) must not disclose the name of Claimant (or any other information which might lead to her identification) or the names of any of the files listed in Schedule C of this Order.

1 The copying of large numbers of electronic documents (around 56,000) formed part of the allegations in *Vestergaard Frandsen A/S v Bestnet Europe Limited* [2007] EWHC 2455 (Ch), [2007] 10 WLUK 659, (2008) 31(1) IPD 31005, which is a judgment in relation to an application by the defendants to strike out the action on the grounds that it was vexatious and an abuse of the process; George L. Paul and Jason R. Baron, 'Information inflation: can the legal system adapt?' (2007) 13(3) Rich J L & Tech 1.
2 Social media websites and text messages sent on mobile telephones and other devices were used to foment rioting in the UK in 2011: *R. v Blackshaw (Jordan Philip)* [2011] EWCA Crim 2312, [2012] 1 WLR 1126, [2011] 10 WLUK 465, [2012] 1 Cr App R (S) 114, [2012] Crim LR 57, (2011) 108(42) LSG 19, Times, 25 October 25, 2011, [2011] CLY 3030.
3 [2011] EWHC 3454 (TCC), [2011] 12 WLUK 641, [2011] Info TLR 25, (2012) 156(2) SJLB 31.

1.126 The ease of communication and replication of electronic documents has increased the potential volume of data that need to be identified to obtain relevant documents pertaining to litigation or the prosecution of a criminal offence. For instance, as part of the Enron investigation, the Federal Energy Regulatory Commission made public a dataset corpus containing 500MB of electronic messages.[1] Yet 'traditional' messages like these are a minuscule minority of all the electronic data (and potential evidence) that is routinely created by machines, such as monitoring and routing Internet traffic. In addition to the sheer volume of this data, it poses the additional problem that in its raw form it is not intelligible to humans – most of the data are instructions sent between and for use by machines. To turn them into evidence for legal proceedings requires a significant amount of translation or 'sense making' by a suitably qualified expert.

1 Available at the Library of Congress website: https://www.loc.gov/item/2018487913/.

1.127 To deal effectively with this amount of data, other computer tools such as data-mining software will routinely be required. These methods of analysis carry their own problems of accuracy, reliability, prejudicial effects and so on. Link analysis software, for instance, can create from this data a picture of a network that shows how people in the company formed communication circles that can be interpreted as the core of a conspiracy, simply as a result of the way in which the software arranges and visualises the information or other design choices not supported by the actual evidence.[1] On the other hand, other forensic disciplines routinely use scientifically validated sampling techniques.[2] At present, there is still a tendency not to use the same sampling protocols for at least some types of electronic evidence, in particular the type of data that can in principle be assessed directly by humans. This can force witnesses, such as police officers, to visually inspect potentially large amounts of disturbing illegal material. However, some jurisdictions have begun to use statistical methods of (electronic) evidence collection more systematically. 'Predictive coding' or 'technology assisted review' uses Bayesian probability theory and ML to scan electronic documents for data relevant to the case, and automatically identifies 'good candidates' for further examination by humans. Used mainly in civil electronic disclosure or discovery, it acquired approval from the courts in 2016.[3] And prosecutors, lawyers and judges have likewise started to use ML-driven case-tracking and management systems to manage case filing, information and caseloads.[4]

1 Cathleen McGrath, Jim Blythe and David Krackhardt, 'Seeing groups in graph layouts' (1996) 19(2) Connections 22.
2 If 300,000 suspicious pills are seized, only a small sample of them will be tested to determine if they are illegal drugs, and a statistical confidence value reported. Colin G. G. Aitken and David Lucy,

'Estimation of the quantity of a drug in a consignment from measurements on a sample' (2002) 47(5) J Forensic Sci 968.

3 *Pyrrho Investments Ltd v MWB Property Ltd* [2016] EWHC 256 (Ch), [2016] 2 WLUK 413; *Brown v BCA Trading Ltd* [2016] EWHC 1464 (Ch), [2016] 5 WLUK 371; Clive Freedman, 'Technology assisted review approved for use in English High Court litigation' (2016) 13 Digital Evidence and Electronic Signature Law Review 139.

4 For instance, see Joint Technology Committee – National Center for State Courts, Introduction to AI for Courts, 7–8, 27 March 2020, https://www.ncsc.org/__data/assets/pdf_file/0013/20830/2020-04-02-intro-to-ai-for-courts_final.pdf.

1.128 The ability to transfer evidence rapidly can also create issues relating to jurisdiction. Many computer users now routinely upload all their files for backup purposes to Internet-based providers. Business data may be processed using cloud computing technology. On the other hand, the automatic uploading of data also means that the user of a device loses control over the information she has created. It can become increasingly difficult to delete or rid oneself of information once it has been created on a device and the information is uploaded onto the cloud.

Storage and disclosure

1.129 Generally, the media upon which electronic data are stored is fragile. Electronic storage media is inherently unstable, and unless the media is stored correctly, it can deteriorate quickly without showing external signs of deterioration. It is also at risk from accidental or deliberate damage and accidental or deliberate deletion.

1.130 Computers, systems and digital devices now operate largely in a networked environment. Devices such as smartphones, computers, laptop computers, mobile telephones, personal digital assistants (PDAs) and tablets are linked by applications (facsimile transmissions, voice over Internet protocol (VoIP), email, peer-to-peer software and instant messaging) that run over networks (the Internet, intranets, wireless networking, cellular networks and dial-up). It follows that almost everything anybody does on a device that is connected to a network is capable of being distributed and duplicated with consummate ease. As a result, the same item of digital data can reside almost anywhere. The ramifications for lawyers and law enforcement authorities are obvious. The relevant document may be available, but it might not be clear where it resides. This affects how a criminal investigation is conducted, and how much effort a party to a civil case will have to devote to finding relevant documents for discovery or disclosure.

1.131 An early example from the US, *Zubulake v UBS Warburg LLC*, serves to illustrate some of the problems faced by a large organization in locating relevant documents in electronic form, especially historical email correspondence. Zubulake, a director and senior salesperson with UBS Warburg LLC, commenced legal proceedings for gender discrimination when she was dismissed from her job. Among other things, she alleged that her manager Chapin treated her differently. She sought disclosure of UBS email communications to support her action.[1] The parties disagreed about the extent of the disclosure of emails, although it was not in dispute that email was an important means of communicating since each salesperson received approximately 200 emails each day. Securities and Exchange Commission Regulations required UBS to store emails. UBS used two storage methods: backup tapes for disaster recovery and optical disks.

This meant that there were three possible places that relevant email communications could be found: in files that were in use by employees, emails archived on optical disks, and emails sent to and from a registered trader (internal emails were not recorded) that were stored on optical storage devices. Ninety-four backup tapes were identified as being relevant for the purposes of disclosure. UBS used a backup program that took a snapshot of all emails that existed on a given server at the time the backup was taken: namely, at the end of each day, every Friday night and on the last business day of the month. Because emails were backed up intermittently, some emails were not stored, in particular where a user received or sent an email and deleted it on the same day.

1 *Zubulake v UBS Warburg LLC* 217 F.R.D. 309 (S.D.N.Y. 2003); *Zubulake v UBS Warburg LLC* 216 F.R.D. 280 (S.D.N.Y. 2003).

1.132 Scheindlin J determined that Zubulake was entitled to disclosure of the emails because they were relevant to her claim, and ordered UBS to produce all relevant emails that existed on the optical disks or its servers at its own expense, and from five backup tapes selected by Zubulake. A consulting firm restored and searched the tapes for US$11,524.63. Additional expenses included the time it took lawyers to review the emails, which brought the total cost to US$19,003.43. Some 1,541 relevant emails were discovered. Fewer than 20 relevant emails were found on the optical disks. In July 2003, Zubulake made a further application for the remaining backup tapes to be restored and searched. UBS estimated that the cost would be US$273,649.39 and applied for the costs to be shifted to Zubulake. In considering the seven-factor test (which is not relevant for the purposes of this particular discussion), the judge noted that a significant number of relevant emails existed on backup tapes, and there was evidence that Chapin had deleted relevant emails. Scheindlin J decided that Zubulake should pay 25 per cent of the cost of restoring the backup tapes, but UBS were required to pay all other costs.

1.133 The purpose of describing this example is to illustrate the problems that multinational organizations have in locating relevant evidence in electronic form. The nature of the distributed environment means that a range of practical problems have begun to emerge in determining what material needs to be disclosed or discovered to the other side. First, it is necessary to prevent the destruction of evidence, and then it is necessary to establish where the evidence is likely to be, before undertaking the exercise of sifting through the various sources to identify relevant documents. This will invariably require a party to locate where all backup tapes are situated, whether held on the premises, with third parties in off-site remote storage or on individual computers, servers, in an archive or a disaster recovery system. The types of storage media that will need to be identified and located include tapes, disks, drives, USB sticks, tablets, laptops, PCs, PDAs, smartphones, mobile telephones, pagers and audio systems (including voicemail), to name but a few.[1] The fragility and the ubiquity of electronic storage has made the modern-day discovery exercise a formidable process.

1 Detective Inspector Simon Snell, Head of the High Tech Crime Unit in Devon and Cornwall, is reported to have indicated that criminals are using satellite navigation systems, games consoles and hand-held computers to try and hide their activities; see 'Abuse images "hidden on sat-navs"', BBC News, 22 January 2008, http://news.bbc.co.uk/1/hi/england/devon/7201785.stm.

Concluding remarks

1.134 This chapter provides an overview of the nature of digital evidence, and introduces the most important concepts and terms that are needed to understand the discussion in the chapters to follow. It also introduces the main components and aspects of digital devices that a forensic investigator has to consider. The chapter also reveals a tension that is inherent in technologically mediated evidence. If we describe digital evidence on a sufficiently high level of abstraction, the continuity with other, older forms of evidence becomes apparent, thereby permitting analogies with the existing common law rules on evidence. For instance, memory, in this sense, is memory, whether gathered from an eyewitness and stored in a biological medium or from a digital device and stored in silicon. From a legal and regulatory perspective, these high-level abstractions fulfil an important role – they create legal stability and predictability for businesses and citizens alike. However, as soon as we move to a higher level of detail, these similarities all but disappear. Electronic evidence is always technologically mediated and technology dependent. We can get data from a book written centuries ago needing nothing more than knowledge of the language. By contrast, acquiring data from an electronic storage device requires appropriate tools and procedures, and can therefore fail, even for systems that are but a few years old. This can mean that laws quickly fail to understand the nature of the technology they try to regulate, and therefore quickly become obsolete. This can create the impression that the law is constantly behind technological developments, and where parliaments or courts try to respond, they more often than not exacerbate the situation with poorly drafted laws or ill-considered rules. The challenge for lawyers and policy makers is to find a middle ground between stable and technology-neutral, but overly abstract and imprecise laws, and highly specific rules that try, but often fail, to be responsive to the latest technological development and therefore risk obsolescence. This first chapter tries to help find such a middle ground by combining high-level and abstract definitions and discussions of historical continuities with more technology-specific discussions, and demonstrating both the similarities as well as the differences between traditional evidence and electronic evidence.