THOMSON REUTERS
SWEET & MAXWELL™

# The Digital Estate

## Second Edition

Leigh Sagar
Jack Burroughs



THOMSON REUTERS®

# TABLE OF CONTENTS

## PART II: INFORMATION

# TABLE OF CASES

and distil information from it. The interpretation is subjective to the viewer, covering his life experiences, cultural background, present state of mind and purpose. Information is context-sensitive; looking at a page of text, the information received by the viewer will depend on his focus. He might concentrate on the weight, quality and colour of the paper; the colour and typeface of the printed text; the tidiness of letters and numbers written in manuscript across the page; the ideas expressed in the written or printed words; or the people represented in an image printed on the page. An object does not itself constitute information, although it may be the subject of an item of information. Take a tree in a field. As an object it is not information, but a description of it as a coconut tree, that it is starting to bloom or that it exists and is situated in that field, is.

**1-02** These terms have a wide range of meanings. For instance, the UK General Data Protection Regulation[2] ("UK GDPR") reg.4(1), defines "personal data" in terms of information relating to an identified or identifiable natural person; there is no definition of "information". In the Freedom of Information Act 2000 s.84, "information" is defined as meaning "information recorded in any form", although ss.75(2) and 51(8) of the Act provide that for certain purposes it includes unrecorded information. The definitions of "information" provided by *The Shorter Oxford English Dictionary* (2007) are in terms of communication of knowledge of facts and occurrences and subjects, events, intelligence and news. Wikipedia describes "information" as "processed, organized and structured data".

**1-03** This book is concerned with the application of legal and equitable rules and principles to property rights and interests associated with information; particularly information that exists in a form that can be manipulated by machines, referred to as "digital information".[3] The inquiry is made from the point of view of fiduciaries and their interactions with the information. One of the central themes of this book, however, is that information is not property,[4] to be directly owned and administered by fiduciaries such as trustees and personal representatives. Their ownership is of rights and interests that are associated with the information, such as intellectual property rights,[5] contractual rights[6] and digital cryptographic token interests.[7]

## II. DIGITAL INFORMATION

**1-04** Imagine a car travelling at 43.5 miles per hour. The driver can check his speed by looking at his speedometer.

(a) Some cars have analog speedometers, on which the speed is represented by a needle pointing at different angles depending on the speed of the car. Various numbers are painted on a gauge so that the speed can be determined according to the numbers underneath the pointing needle. If the car is travelling at 43.5 mph, the needle might indicate a speed between 40 and 50. An

2 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (as introduced to UK domestic law and amended).
3 See section II of this chapter.
4 See Ch.4.
5 See Ch.6.
6 See Ch.5.
7 See Chs 8 and 9.



increase (or decrease) in speed produces a smooth increase (or decrease) in the angle of the needle. Reading the gauge involves the driver exercising judgment as to what is the actual speed.

(b) Some modern cars have digital speedometers, which show the speed as a number (a digit). If the car is travelling at 43.5 mph and the calculations used by the car's systems to update the numbering are accurate, the digital speedometer will display that precise number. Increases and decreases in speed will likewise be shown with similar accuracy. The digital speedometer shows the speed according to the decimal system, or number base 10. As a number increases beyond 9, it returns to 0 and the number to the left of it increases by one: a zero in a column needs to increase 10 times before it returns to zero.

Another example is a clock. An analogue clock uses hands moving smoothly around the clock face to show the time, again to be determined as an exercise in judgment. A digital clock shows the time as a series of numbers, which is easier to read and, depending on the calibration, more accurate. With the clock, there are various number bases: the hour column works in either base 12 or 24, depending on whether it is a 12- or 24-hour clock; both the minute and second columns work in base 60. **1-05**

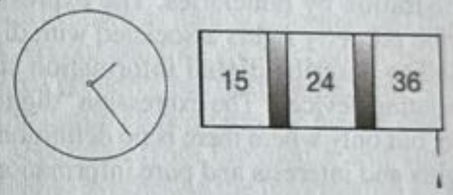


**Figure 1: Analog and digital clocks**

**1-06** Computing devices generally operate using number base 2, known as a binary system, in which the only numbers are 0 and 1. As a column of numbers increases beyond 1 it returns to 0 and the value in the column to the left increases by 1. A binary system is ideal for computer operations as it allows for simplicity: if only two values are needed, one of them (the "1") can represent an "on" position and the other (the "0") an "off" position, or where logic is involved, "1" can represent "yes" and "0" can represent "no". When a voltage passes through the system that would read as 1 and, where no (or lower) voltage passes through, it would read as 0. Similarly, a card with a series of holes could be used for 0's and 1's, as could a magnetic tape or disc with the magnetic particles aligned one way or another.

**1-07** The decimal number 11 is represented by the binary number 1011: adding (decimal) 1 for the "1" in the fourth column, (decimal) 2 for the "1" in the third column, (decimal) 0 for the "0" in the second column and (decimal) 8 for the "1" in the first column (1 + 2 + 0 + 8 = 11).[8] The following table shows the binary translations for the decimal numbers 0 to 9.

**Table 1: Binary translations**

| Decimal number | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|

8 If there had also been a "1" in the third column (1111), that would represent the decimal number 16 (1 + 2 + 4 + 8 = 16).

| | | | | | |
|---|---|---|---|---|---|
| Binary number | 0000 | 0001 | 0010 | 0011 | 0100 |
| Decimal number | 5 | 6 | 7 | 8 | 9 |
| Binary number | 0101 | 0110 | 0111 | 1000 | 1001 |

1-08 An example of a non-electronic digital binary system is a bonfire communication system: if there is danger the fire is lit, otherwise it remains unlit, so that on (1) might mean war and off (0) peace.

## III. NOMENCLATURE

1-09 Certain expressions will be used throughout the book and they are discussed next. They are "digital assets", "digital records", "digital property rights", "digital property interests", "cryptoassets" and "crypto-tokens".

### 1. Digital assets

1-10 In books, articles and some will precedents, writers use the expression "digital assets",[9] without distinguishing between proprietary rights and interests and non-proprietary items. In this book, the use of that expression is limited, because it is not sufficiently precise for the purposes of describing the functions and activities associated with administration by fiduciaries. The expression "digital property rights" is used to describe property rights associated with digital information, and "digital records" is used to describe digital information stored in electronic or magnetic form in a computing device.[10] The expression "digital assets" may be used for general convenience, but only where there is no definitional need to distinguish between proprietary rights and interests and pure information.[11]

#### (a) The Revised Uniform Fiduciary Access to Digital Assets Act

1-11 The Revised Uniform Fiduciary Access to Digital Assets Act (2015), which is known as "RUFADAA", is draft legislation prepared by the National Conference of Commissioners on Uniform State Laws in the US and recommended for adoption by individual states for uniformity of state law.[12] Amongst other things, RUFADAA is designed to deal with the problem of fiduciaries obtaining access to information relating to cloud services, although the jurisdiction is limited to local applicants.[13] Apart from the terms and conditions of the various cloud services, in the US, electronic communications are subject to the privacy protections of content "when used with respect to any wire, oral or electronic communication", including email, text messages, instant messages and any other electronic communication between private parties[14]; in addition, content stored with a service provider cannot be divulged without authorisation.[15]



1-12 RUFADAA defines a "digital asset" in terms of electronic records in which an individual has a right or interest, but not including any underlying asset or liability.[16]

#### (b) The Uniform Access to Digital Assets by Fiduciaries Act

1-13 A similar enactment has been prepared by the Uniform Law Conference of Canada, known as the Uniform Access to Digital Assets by Fiduciaries Act (2016), in which "digital asset" is defined in terms of a digital or intangible record. No specific equivalent legislation has been enacted in England and Wales.[17]

### 2. Digital records

1-14 The contents of a printed book, a phonographic disc and a cinematic film are examples of information (known as analog information) that is part of the containing medium. The book, record and film are all chattels that devolve on the personal representative as personal property, but the information—represented by the words printed on the paper, the music etched onto the plastic disc and the images printed on the film—can be separated from the media and stored in a different way: processes can be applied to synthesise the information so that it is represented by numbers (generally in binary format), which can be stored electronically or magnetically as records, sometimes known as "files", and the numbers can be reconverted back into analog form for the enjoyment or utility of the user. Digital information need not have been converted from an original analog format; a substantial proportion of all documents, images, music and videos are now created directly in digital form by computer programs and applications.[18]

1-15 The information represented by these numbers is digital information and the

---

9 See, for instance, R. Dew and K. Shannon, *Parker's Will Precedents*, 8th edn (London: Bloomsbury Professional, 2014), Ch.15; *Butterworths Wills Probate and Administration Service* (London: LexisNexis), para.[4.7]; Withers LLP, Practical Will Precedents (London: Sweet & Maxwell, 2022), para.F5-1359 ("... so far as such asset or right may be lawfully transmissible or transferable ..."); D. McCallig, "Facebook after death: an evolving policy in a social network" (2014) 22(2) *Int. J. Law Info. Tech.* 107; K. Davies, "We are living in a virtual world" (2014) S.J. 2014, 158(22), 38; C. Currie, "Can a 'digital buddy' bring solace to our loved ones?" S.J. 2015, 159(2), 38; J. Yves, "£17bn of digital assets could be left in cyber space" (2015) *Solicitors Journal* 6 March 2015; Murray, "Digital life after death", (2014) *Solicitors Journal* 24 September 2014; S. Walsh and C. Teitell, "Protecting Clients' Digital Assets" 153 *Trusts & Estates* 32.

10 See Ch.4, section V.

11 The expression "digital asset management" has for more than 15 years been used to refer to "management tasks and decisions surrounding the ingestion, annotation, cataloguing, storage, retrieval and distribution of digital assets", where what is being managed comprises audio, video and other media content, in a digital format (see the Wikipedia article at *https://en.wikipedia.org/ wiki/Digital_asset_management*). Digital asset management systems are generally used by persons or organisations that need to catalogue and manipulate these electronic records, such as advertising agencies, libraries, museums and universities; in this book, these "digital assets" are described as "digital records"; see Ch.4, section V.

12 At the time of writing it has been adopted by 47 US jurisdictions and introduced by one other, although California has not yet introduced it.

13 In its unamended form, the Act applies where the user of a digital service resides in the state, or if he did so at the time of his death: RUFADAA s.3(b).

14 See the Electronic Communications Privacy Act 18 US Code §§2510–2522.

15 See the Stored Communications Act 18 US Code §§2701–2712.

16 RUFADAA s.2(10).

17 See M. Walters, "Digital legacies need legal protection say lawyers" *Law Society Gazette*, 7 June 2017, *https://www.lawgazette.co.uk/law/digital-legacies-need-legal-protection-say-lawyers-/5061412.article*. The Digital Devices (Access of Next of Kin) Bill was introduced as a Private Member's Bill on 18 January 2022 "to grant a right of access to the digital devices of a dead or incapacitated person to their next of kin"; see *https://www.step.org/industry-news/uk-private-members-bill-would-open-deceaseds-records-family*.

18 For instance, few cameras still use rolls of film that need to be processed before the images can be seen—most now use an image sensor to collect light signals that are processed by computer software running in the device; most documents are created using some type of electronic software designed to process words, graphics and images, and sounds. For a discussion about electronic documents, see Ch.3, section IV.

stored information is contained in "digital records". The numbers can be referred to, generally, as data, which are manipulated by computing devices.

### 3. Digital property rights and interests

-16 The ownership of the physical material in which information, whether digital or analog, is stored or held, must be distinguished from any rights and interests that are associated with the information. These rights might be intellectual property rights, subsisting in literary, musical, artistic and dramatic works. The use of digital information might be controlled by a contract made by internet communications using a web browser.[19] The information might exist within the bitcoin protocol as a digital cryptographic token.[20] Such rights and interests are referred to in this chapter as "digital property rights" and "digital property interests". The expressions "cryptoassets" and "crypto-tokens" have up until now been used largely interchangeably. However, the Law Commission have proposed the use of crypto-tokens in the case of what we refer to as "cryptoassets", but with a particular meaning. We have retained the existing use of the words "cryptocurrencies" and "cryptoassets".[21] Broadly, the Law Commission use the expression "crypto-token" in this context as a reference to the particular data structure constituted by the protocol rules of a particular crypto-token system (for example, a bitcoin), whereas a "cryptoasset" is a "composite of a crypto-token and any associated or linked property or other legal rights that are recognised in law as existing as a consequence of having legal rights in relation to that crypto-token"[22] (for example, a non-fungible token linked to particular legal rights).

### 4. Communication

1-17 Information is framed in language, which can be communicated to others, ready to be absorbed and assimilated by them as raw data, to be interpreted, with other data and knowledge, as information.[23] Humans have developed devices that assist in the manipulation and communication of information in a variety of formats; for instance, cameras can capture images, which can be represented by altering chemicals imprinted on paper or film (analogue) for physical distribution or by converting the images into electronic signals (digital) that can be processed by computing devices and reconstructed on demand for utility or enjoyment, or transmitted to other devices for further processing and reproduction. Similarly, a microphone can capture sound, which can be represented by scratching or stamping grooves into a plastic platter (analogue) for physical distribution or by converting them into electronic form for further processing and manipulation (digital).

---

[19] See S. Mason, *Electronic Signatures in Law*, 4th edn (London: University of London, Institute of Advanced Legal Studies, 2017) for a discussion about electronic and digital contracts; see also Electronic Communications Act 2000 and Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [2014] OJ L257/73 (known as the e-IDAS Regulation); see also the Law Society, "Execution of a document using an electronic signature" 21 July 2016: *https://www.lawsociety.org.uk/topics/business-management/execution-of-a-document-using-and-electronic-signature*. Electronic documents and signatures are discussed in Ch.3.

[20] Bitcoin and other cryptographic digital tokens are discussed in Chs 7 to 9.

[21] See Law Commission, *Digital Assets: Consultation paper* (HMSO, 2022), Law Com. No.256). A short-form description of a crypto-token is given in Appendix 4 (pp.504–505).

[22] Law Commission, *Digital Assets: Consultation paper* at 10.4.

[23] See para.1-01.



Communication of information between humans can be achieved in many ways. Historically, a fire beacon might have been used, or talking drums, or paper, or the air around us. The technologies of the communication would have been decided by the media to which they were applied; in the examples given above, it would have been lighting a pile of inflammable materials; striking a stretched skin with a stick; applying coloured ink in shapes with a sharpened object; and uttering sounds using the mouth. A message was communicated by the communicator to the recipient using a language capable of being understood by both, be it English, Mandarin or Ndebele. The words of the language were converted to a form that could be utilised by the relevant technology in performing its function; for instance: a series of bonfires on hilltops each within sight of the next, reporting the landing of the ships of the enemy; the beating of rhythmic and tonal sounds, announcing the birth of a child; written characters and pictures, describing the course of a battle; and the spoken word, commenting on the weather. 1-18

A communication can be divided into at least six components: 1-19

(1) the original item or event; this is not information but gives rise to raw data. In the above examples, the information element might be the landing of the ships, the birth, the battle and the weather;
(2) an interpretation of the raw data. This is information;
(3) an expression of the information, in some language, which might not be a spoken language;
(4) the conversion of the expressed information into usable portions that are compatible with the communication technology; in the above examples, the landing is converted into an instruction to light the bonfire, the birth into a series of drumbeats, and the battle and the weather into words;
(5) the operation of the communication technology to transmit the expressed information; in the above examples, lighting the bonfire, hitting the drums, and writing and speaking the words; and
(6) after the transmission has been received, the expressed information is analysed and reconverted into language that can be understood by the recipient.

Modern communication of information takes place largely between computing devices.[24] Digital information is input into a device from an analog source, such as a keyboard, microphone or camera, or by conversion of existing analog information into digital records. If a record is to be sent over a network, such as the internet,[25] it is divided into packets, or blocks, that are addressed to the receiving device, which reassembles the received packets and stores the resulting data as a digital record identical to the original that was sent.[26] The receiving device can then convert the record into an intelligible form, such as text displayed on a computer monitor or printed onto a sheet of paper. 1-20

## IV. COMPUTER SYSTEMS

### 1. Introduction

There are several types of computer system, including the personal computer 1-21

---

[24] Computing systems are discussed in section IV of this chapter.

[25] The internet is discussed in section VII of this chapter.

[26] This process is known as "packet switching".

(including laptops and notebooks), smartphone, tablet and game console. There is also wearable technology, examples of which are smartwatches and fitness trackers that absorb information from their surroundings, including the human body, and communicate it for analysis to some other device, like a smartphone. Embedded computers might control cars, televisions, central heating and cooling, automatic lighting, microwave ovens and washing machines (known as the internet of things). All these systems have the same basic structural architecture but the smaller the system, the greater its integration into less powerful and less flexible units.

## 2. Structure

### (a) Conductivity

1-22 Certain substances, such as copper, are made up of atoms that are not electrically stable. The instability is caused by electrons randomly moving between atoms. If the exchange of electrons moves in the same direction, the result is an electric current. An electron from one atom moves to another and is replaced by an electron from a third atom, and so on, all moving in the same direction. Each electron moves relatively slowly but, because all of the electrons in the copper wire are moving together in the same direction, the resulting current appears to move extremely quickly. That is why toggling a light switch causes a light some distance away to illuminate almost immediately. The current and the resulting movement of the electrons is caused by applying voltage, or electric energy, to the cable, for instance by connecting a battery to the two ends of the cable.

1-23 On the other hand, an insulating material is electrically stable, in that its electrons do not move between atoms and do not carry an electric charge. Examples of this are rubber and wood.

1-24 One of the challenges in the use of electric current is to control its flow. Varying the strength of a signal can be useful, for instance, to produce radio waves for transmission, or to amplify weak signals received from an antenna to make them ready for processing to provide output to a television screen or radio loudspeaker or from a WiFi antenna to a computer processor. If the flow of current is switched on and off, or with high and low energy, that will produce a binary signal.

### (b) Semiconductors

1-25 There is another type of material, whose electrical properties lie between those of conductors and insulators. This material is known as a semiconductor and examples are silicon and germanium. The flow of current through a semiconductor can be changed. The electrical properties of semiconductors are flexible and can be altered to change the direction of the passing current or to stop the flow of current altogether and then start it again.

1-26 The most flexible of semiconductor devices is the transistor and the modern age of electronic computing began with its invention. It was first demonstrated in 1947 and can be compared with the invention of the wheel in bringing about a dramatic shift in our way of life. Modern computers and telephone devices use components, known as integrated circuits, microprocessors or chips, that are made up of billions of transistors and other elements,[27] all fashioned (or grown) from a single piece

[27] The latest Apple A15 microprocessor driving its iPhone contains over fifteen billion transistors. A 64Gb memory chip has over 64 billion transistors—see *https://en.wikipedia.org/wiki/Transistor_count*.



of silicon and often smaller than a credit card. These so-called "solid-state" chips,[28] manufactured with different configurations, are used for computer memory, data processing and storage.

### (c) Magnetic binary signals

Magnetic discs (known as hard drives) are also commonly used to store data.[29] 1-27

### (d) Organisation

A basic computing device is made up of the Central Processing Unit ("CPU"), main memory and storage, which might be magnetic or silicon based. It will also have some kind of output, such as a monitor (screen) or printer, or a connection to the internet. All of these components send, receive and/or process binary data; they are connected by a bus, which is a collection of wires used to send information amongst the connected components. Figure 2 shows the organisation of a simple computing device, with the CPU, memory, storage and output all connected by the bus.[30] 1-28

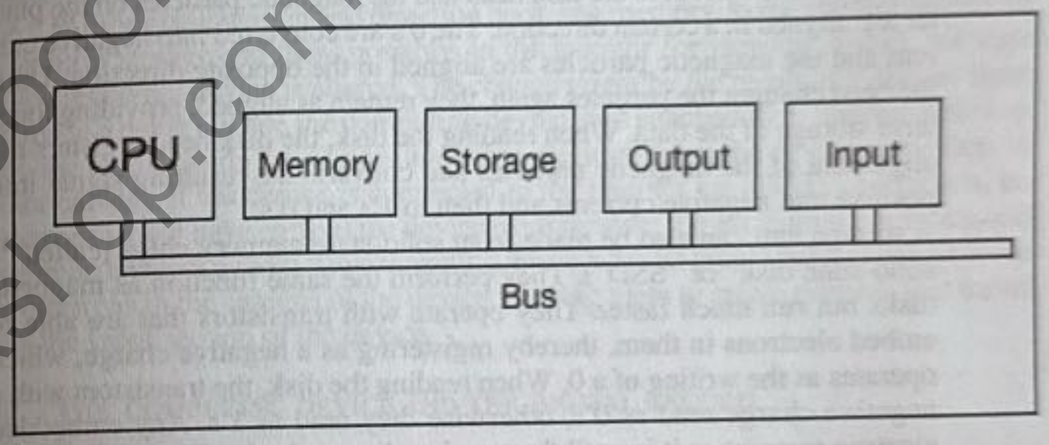


**Figure 2: Schema of a simple computing device**

#### *(i) Processor*

The CPU is the "brain" of the device and executes a series of instructions provided by a program (or application). It is a complex component and, amongst other things, has a control unit, which fetches the instructions from memory, and an arithmetic logic unit, which performs operations (such as addition and subtraction) that are needed to carry out the instructions. Data are manipulated in a logical manner to produce a result that can be further manipulated or sent through an output process to storage or display. The device will also have other processing units that are used for specific tasks, such as interpreting non-binary information that is inputted into the device; converting binary data into colours and shapes that are sent out to the display unit; converting binary data into electric signals to drive a 1-29

[28] If it is sophisticated enough, it is known as a "computer-on-a-chip".

[29] These are discussed in section IV.2(d)(iii) of this chapter.

[30] See generally, A. Tanenbaum and T. Austin, *Structured Computer Organisation*, 6th edn (Harlow: Pearson, 2013).

loudspeaker; and converting electrical signals coming in from the WiFi or bluetooth antenna into binary data (and the other way around).

*(ii) Memory*

1-30 Memory is stored on solid-state chips and comprises instructions to be processed by the CPU, the data that is used in the execution of the instructions and the results of the execution of those instructions. They are stored as a series of 0's and 1's.

*(iii) Storage*

1-31 Long-term storage is generally on magnetic disk drives or (more commonly today) solid-state disk drives.[31]

(1) Magnetic disk drives consist of a series of platters each coated with a substance that can be magnetised and having a disk head floating on a cushion of air over it. Binary data are written onto the disk from memory and read from it to be transferred to memory ready for manipulation. When data are to be written on the disk, the 1's making up the data are converted into a positive current in the disk head and the magnetic particles on the platter are aligned in a certain direction. The 0's are converted into negative current and the magnetic particles are aligned in the opposite direction. Until the head changes the particles again, they remain as aligned, providing long-term storage of the data. When reading the disk, the disk head registers the alignment of the magnetic particles and converts the resulting signal into positive and negative currents and then to 1's and 0's.

(2) A storage unit can also be made from solid-state memory chips (called "a solid-state disk" or "SSD"). They perform the same function as magnetic disks but run much faster. They operate with transistors that are able to embed electrons in them, thereby registering as a negative charge, which operates as the writing of a 0. When reading the disk, the transistors with a negative charge read as 0's, otherwise they read as 1's. Any embedded electron remains as it is until the transistor's state is altered.

*(iv) The bus*

1-32 The bus carries all the signals and data to and from the various components and to the input/output (known as "I/O") facilities available to it. It can output to the disk storage unit, to a monitor or screen for viewing by the operator, to a printer for reading later or to a network connection for transmission to another computer. Input can come from a storage unit, a network transmission, a keyboard or the touch-sensitive glass of a smartphone or tablet. These operate in the same way, passing electrons through the bus to the system ready for manipulation as appropriate.

*John Richardson Computers Ltd v Flanders*

1-33 In *John Richardson Computers Ltd v Flanders*,[32] Ferris J discussed the operation of a computer as a machine that processes numerical data. Non-numerical data, such as text, needs translation into binary numbers for processing by the computer. The computer operates on simple processes very quickly, thereby achieving the effect of processing complex operations more quickly and more accurately than the human mind. On the other hand, the computer needs instructions, provided by a computer program, for these operations.

[31] The solid-state disk is a collection of chips and is not a disk at all. Its name is historical.

[32] [1993] F.S.R. 497 at 502.



## 3. Operation

It can therefore be seen that the electronic operations of a computing device occur at a sub-atomic level. To that extent there are no moving parts and the passage of information through the system occurs by the movement and injection or passage of electrons through and into various components of the device. Similar changes occur with the magnetic materials making up magnetic hard disks: the magnetic material alters according to the binary value of the information. A tap of an "x" key on a keyboard alters the device in a subtle but definite way. The binary code representing the pressed key is sent using electronic transmission through the bus into memory then to the CPU, which manipulates it and directs it through the bus into memory. Then it is processed through the output to the monitor and an "x" magically appears on the glass of the screen. That keypress altered the state of the device at an atomic level. 1-34

If, for instance, an email is received from the internet, the binary information passes through input into the bus and on to the memory for temporary storage, to the CPU for manipulation and direction back into memory, to the storage device for long term storage and then, possibly, to the monitor for viewing. Again, the state of the receiving device is altered. The change might be the result of electrons from atoms in a cable outside the computing device, and attached to it, finding their way into the atoms inside the device (and other electrons from the device into atoms in other cables). If the device is connected to the internet via a WiFi connection, no electrons would have entered the device from outside; the oscillating electronic and magnetic fields of a radio wave travelling through the air would have exerted a force on electrons in the antenna of the device, causing them to create currents that travel into the input section of the device. 1-35

## 4. The computing device and the digital record

When a photograph is taken by a digital camera,[33] the electrical signals from the image sensor are converted by a processor in the camera into a binary file, which is transferred by the CPU in the camera to the memory section and then to the transistors in the storage section of the camera, for which a secure digital ("SD") card is commonly used. The transfer of the 1's and 0's of the binary image file onto the SD storage is a transfer of electrons through the system, altering the state of the device at an atomic level: the transistors in the CPU are altered many times while it manipulates the digital record to send it to the transistors in the memory chip, some of which change from 0's to 1's and others change from 1's to 0's.[34] The question to consider here is whether the image captured by the image sensor, or the digital record that results from the manipulation of the 1's and 0's of the file have any proprietary character: can the person who snapped the picture claim ownership of anything that results from that action? 1-36

Ownership of the information making up the image that passed through the lens of the camera is impossible; it disappeared immediately after the picture was taken, 1-37

[33] Modern digital cameras have a functional computing system that has a similar architecture to the system in a personal computer. Many digital camera components are incorporated into mobile phones, tablets and laptops.

[34] Depending on the image resolution (or pixel density), there might be millions of transistors involved.

to be replaced by a stream of electrons. The camera is a chattel and can therefore be owned. The atoms, electrons and transistors that operate to manipulate, transfer and store the digital record within the camera are part of it and belong to its owner. There is nothing else to own and it must be the case that the digital record is not capable of ownership apart from the transistors in which it is stored.

1-38 Once the digital record is passed out of the camera to a computing device, or from a computing device through internet connections to another one, it becomes even more difficult to say that the person who snapped the picture retains any ownership in the image's digital record. Consider a transfer across the internet. The initial journey of the image's digital record will be by electrons along the bus[35] to the point at which the system processes the signal to send it off to the internet. That might be along a new cable or into the air to be carried on a WiFi signal. At that point, the original electrons cease to have any function in the journey and the conveyance of the 1's and 0's is taken up by the passage of new electrons and atoms. This might happen many times throughout the journey, through the devices on which the internet is built, ending with its entry into the receiving device, the 1's and 0's being transported to the CPU for processing.

1-39 In this way, there can be no physical correspondence between the original existence of the image's digital record in the sending device and its existence on the receiving device. The journey is accomplished by the processes that occur in those two devices and all the intermediate internet devices. Furthermore, even if it could be shown that the transfer of the digital record was somehow a physical matter, it would have been submerged into the receiving computer, which would remain in the ownership of its original owner and the person taking the picture or sending the email would not have any title to any part of the computer. Bricks used to build a wall become part of the resulting house; thread used to repair a coat becomes a part of the coat; and planks, nails and pitch used to repair a ship become part of the ship.[36]

## V. THE CYBERSPACE METAPHOR

1-40 Although working with computing devices and the internet is an interaction of humans with coded logic operating in a context of metal, silicon and plastic, there is a tendency for users to imagine that they are in a virtual world with experiences that can be aligned to those of the real world. Software was often designed so that users could imagine that they were operating familiar items, such as clicking a mouse so that an image appeared to act as if it were a button, or tapping the screen of a digital reading device, such as a smart phone, to look as if the user is turning a page. This skeuomorphic ornamentation was used to simulate the way that the task had been done without a machine, making the user feel at ease.

1-41 Now that people have become accustomed to operating computing devices and have no need to imagine that they are in a three-dimensional space, rather than the two-dimensional screen of the monitor, there is a tendency to move away from skeuomorphism and operating systems are being designed in more efficient and less ornamental ways. The metaphor remains in the language of internet use, however, with users talking of cyberspace, the world-wide-web, surfing and internet addresses; "spiders" crawl through web pages; a cyberbusiness is one that is carried

---

35 The bus is described in section IV.2(d)(iv) of this chapter.

36 See M. Bridge, L. Gullifer, G. McMeel and K. Worthington, *The Law of Personal Property*, 3rd edn (London: Sweet & Maxwell, 2022), para.17-033.



on using the internet or in cyberspace; a cyberattack is the transfer of code over the internet designed to cause a malfunction of some kind on a computer connected to the internet; and cybercommunication is communication in cyberspace.

What of the content of an email message sent to the receiving device: the words and pictures are transferred across the internet to the receiving device, displayed on its monitor, screen or other viewing facility and stored in its storage device. The idea of a transfer of words and pictures across the internet is, however, no more than a metaphor. The words and pictures move in cyberspace, a representation of reality that facilitates understanding but misrepresents the true facts. The true position is that those words and pictures were converted by the sender's computing device into binary data, which set up a series of moving electrons across the internet to the receiving device. It was not even a continuous movement of electrons; at each exchange point a computing device received the electron signal and sent a fresh electron signal onto the next exchange point. 1-42

## VI. TRESPASS

### 1. Introduction

1-43 If the words and pictures of an email or some other transmission sent to a computing device are not welcomed by the user of the receiving device, there might be a trespass. In the case of land, a trespass is committed by an unjustifiable intrusion by one person upon land in the possession of another; placing a part of one's foot unlawfully on someone else's land is as much a trespass as walking on it.[37]

1-44 The tort of trespass to goods involves direct, immediate interference with a person's possession of a chattel. It is not necessary in England for there to be any resulting damage, but there is no trespass where the action does not go beyond generally acceptable standards of conduct. There is no liability without some intention to the act complained of, even if it is not known that the act constitutes wrongful interference. If an email passes into the circuitry of a computing device, electrons are moving between the atoms making up the receiving device[38]; the device is altered, even if only at an atomic level. As such, there has been interference.[39] Normal email activity could be defended as being within generally acceptable standards of conduct unless it is commercial spam, carries a virus or is part of some other attack on the machine, such as a denial of service attack. The same principles would apply if someone gained access to a device belonging to another but did not transfer any data to storage; even accessing the device would have caused a subtle change by altering the transistors making up the CPU.[40]

---

37 Per Coleridge CJ in *Ellis v Loftus Iron Co* (1874-75) L.R. 10 C.P. 10 at 12.

38 See section IV.2 of this chapter.

39 See M. Jones, A. Dugdale, M. Simpson, *Clerk and Lindsell on Torts*, 21st edn (London: Sweet & Maxwell, 2014) ("*Clerk and Lindsell*") paras 17-135 and 17-136.

40 In para.17-136 of *Clerk and Lindsell* it is argued that such an activity is defensible as "not having gone beyond generally acceptable standards of conduct". This might be true of a search engine or spider (a program, also known as a "search robot", designed methodically to search through the storage of a device and analyse its contents for later use—search engines, such as Google, use spiders to search and analyse the contents of websites) accessing a server on which a website is hosted and the public are invited to access the site, but it cannot be the same if unauthorised access is made to the data on a personal computer. Such activity would be, at the least, equivalent to infection by a computer virus, worm or Trojan horse (see also the discussion about the US decision in *Ticketmaster Corp v Tickets.com Inc* 2003 U.S. Dist. Lexis 6483 (C.D. CA., 7 March 2003) at para.1-45(2)).

1-45 There has been no directly relevant litigation about this in England. The position is different in the US.

*Thrifty-Tel v Bezenek*

(1) In *Thrifty-Tel v Bezenek*,[41] the plaintiff, Thrifty-Tel Inc, provided long-distance telephone services. A subscriber needed to enter both a confidential access code and a six-digit authorisation code in order to use the services. The defendants' children knew their access code but not the authorisation code and they made many attempts to guess that code over an extended period, using their parents' home computer and modem, at times overburdening the company's system and denying some subscribers access to the phone lines. The plaintiff company brought proceedings against Mr and Mrs Bezenek for trespass. The Californian court found for the plaintiff and awarded damages and costs. It was held that trespass to a chattel lay where "intentional interference with the possession of personal property has proximately caused injury". It was noted that, although historically at common law, trespass required a physical touching of another's chattel, the modern rule recognised an indirect touching, such as dust particles from a cement plant migrating onto another's personal property; the requirement of a tangible contact had been relaxed almost to the point of being discarded, so that microscopic particles or smoke could give rise to trespass.[42] Even migrating intangibles, such as sound waves, could result in trespass, provided they caused damage and did not simply impede the owner's use or enjoyment of property.

*Ticketmaster Corp v Tickets.com Inc*

(2) In *Ticketmaster Corp v Tickets.com Inc*,[43] the plaintiff and the defendant were competitors. They used websites to offer tickets for entertainment events for sale to the public. Each website had individual pages for each event for which tickets were being sold, with information about the event and a method of purchasing tickets for it. Each of the event pages had its own URL, so that it was possible to point the web browser directly to the web page, by-passing the home page, which contained advertisements for which payment had been made. The defendant also displayed pages showing information about events for which it was not selling tickets. Tickets.com used a computer program known as a "spider" or "crawler" to search through Ticketmaster's web pages. The court held the use of a spider was not a trespass without tangible interference with the use or operation of the computer being invaded by the spider or actual dispossession of it for a substantial time.

*Register.com Inc v Verio Inc*

(3) In *Register.com Inc v Verio Inc*,[44] the defendant used a spider without authority to search and analyse the plaintiff's database and extract information from it for the purposes of its business. The defendant argued that its conduct did not harm the plaintiff's computer but the court held, distinguishing the *Ticketmaster* decision, that if the defendant was permitted to continue to access the database with the spider it was "highly probable" that others would devise similar programs to access the plaintiff's data, and that its system would be overtaxed and crash.

[41] (1996) 46 Cal. App. 4th 1559.
[42] *Ream v Keen* (Or. 1992) 314 Ore. 370, 838 P.2d 1073 at 1075.
[43] 2003 U.S. Dist. Lexis 6483 (C.D. CA., 7 March 2003).
[44] 356 F.3d 393; 2004 U.S. App. LEXIS 1074; 69 U.S.P.Q.2D (BNA) 1545.



## VII. THE INTERNET

### 1. INTRODUCTION

1-46 In the 1960s the United States Department of Defence developed a system of communication between military bases that could survive a nuclear attack. The result was a variety of connections between different bases so that if one base or one line of communication was destroyed, connection between the bases was not lost. Universities became involved in research for the project and a flexible and survivable system was built connecting many more computers using various methods, including standard telephone systems and radio waves. Businesses started to see possibilities for the transfer of their data between sites and organisations. Private networks using similar principles were developed and became the modern, fast and ubiquitous internet.

1-47 Each computing device connected to the internet has a unique address, known as its IP address,[45] which can be used to identify it and to connect to it. An example of an IP address is 74.125.224.72, which belongs to Google; typing the expression "*http://74.125.224.72/*" (without the quotation marks) into the URL bar of a web browser may bring up the Google search page.[46] The system goes further, by associating these numeric addresses with names, such as google.co.uk, or gov.uk. These are known as domain names and when a person enters a domain name into the URL bar of a web browser, that name is checked against the Domain Name System server to discover the numerical IP address it is seeking.

### 2. THE DOMAIN NAME SYSTEM ("DNS")

1-48 Domain names are used to identify computers and networks connected to the internet, enabling a person, with certainty, to access a particular web page, out of the millions in existence, and to send an email to another person. Domain names can qualify as trademarks.[47] A non-profit organisation known as "ICANN" is responsible for the co-ordination of the Domain Name System.[48] The .uk name registry in the UK is Nominet UK.

1-49 The domain name system is referred to as the "DNS". A domain name is unique and the addition or substitution of even one character will alter the name: for instance, "thedigitalestate.co.uk" is not the same as "digitalestate.co.uk" or even "thedigital.estate". The name is divided into a number of labels, each separated, or delimited, by a dot. The label to the right, such as ".com" is the top-level domain

[45] "IP" stands for "internet protocol".
[46] Google uses many IP addresses and only certain of them work at any given time. The above address therefore may or may not work when typed into the URL bar.
[47] See, for instance, *Prince Plc v Prince Sports Group Inc* [1998] F.S.R. 21 (prince.com). The protection of domain names is discussed in more detail in Ch.6, section IV.4.
[48] The acronym stands for "Internet Corporation for Assigned Names and Numbers".