Part I
Introduction – Tech, Digital Tech and LawTech

Chapter 1
What is Electronic Digital Technology?

1.1 Introduction

As we will be using many technical technological terms, this section will define and explain these terms in what is hopefully easy to understand language. However, we should note from the beginning that there are problems with definitions and explanations of technological terms, especially those to do with digital electronic technology. In researching for this book, the author found that many experts in technology and in law seem to have forgotten a remark that is often ascribed to Albert Einstein, although he probably did not say this, "If you can't explain it simply, you don't understand it well enough." The author is not sure that the problem is that these experts do not understand their subject, it is that they assume that everyone else is an expert as well and thus do not bother to explain things simply. This problem is made worse for the explanations of technical terms because digital electronic technology is still a relatively new field, or at least new in its popular application. Therefore, the terms are not always clearly defined by technologists yet. Further, terms often are used interchangeably. Finally, most confusingly, the same term will be used to refer to different things. For example, we will consider the terms digital assets, virtual assets and cryptoassets, which are often used interchangeably. However, they have distinct meanings even if they are related. Cryptoassets are a specific type of virtual asset, and virtual assets are digital assets – therefore, all cryptoassets are virtual and digital assets but not all digital or virtual assets are cryptoassets. We will consider these terms in more depth later.

The terms used for digital electronic technology are still being developed, expanded and sometimes clarified. One cannot help but suspect that language is used in this field to confuse and exclude as well as communicate – the language maintains a mystery. Most professions maintain such mystery. They emphasise their exclusivity and profitability by using their own language, even using everyday words and terms in specific ways that are different to common usage. Lawyers at least should not be upset by this, as using an elite language to exclude and maintain mystery is something lawyers are familiar with in respect of the language of law.

http://www.pbookshop.com

If we begin with the most used term, we begin with a problem. The experts in this field refer to technology or tech, when they really mean electronic digital technology.

1.2 Electronic Digital Technology

Electronic digital technology is all about data, its collection, storage, distribution and processing. The term data refers to facts, such as numbers, words, measurements, observations or just descriptions of things, collected for reference or analysis. Humans have always accumulated and used data. Traditionally this data was recorded in hard copy in many ways. For example, by impressing on wet clay tablets in ancient Mesopotamia, or writing on papyrus and eventually paper in ancient Egypt and China. More recently we have accumulated our handwritten and then machine typed data in files and folders in filing cabinets and card indexes. Communication of this data would be by making and sending hard copies – handwritten, typed or printed. Processing of this data was by human analysis – humans would organise the data and search for the records they wanted. Today, we store, access, process and share this data using electronic digital technology.

The terms tech and digital technology are now almost overused. The technology that we are usually considering today when we use these terms is electronic digital technology. It refers to technology that is or relies on electronics and digitalisation (the conversion of data into digital form). Experts in this field often forget to explain what this means, so we will consider the meaning of these words individually and together as the phrase electronic digital technology. Electricity powers most of the technology we use in our daily lives, from the heating or air-conditioning in our homes to our smartphones and our cars. Therefore, an electric device is one powered by electricity. Some of these devices are also electronic devices, which have, or operate by using components such as microchips and transistors that control and direct electric current. The word digital refers to recording, storing and representing information as digits or pictorial representations of numbers. The term digital is usually contrasted with the term analogue. Thus, a digital clock shows the time in digital form as numbers from 0-9. If the time is one o'clock, the clock will display the numbers "01.00", "1.00" or "13.00", the last if it is using a 24-hour representation and it is one o'clock in the afternoon. An electronic digital clock represents time by displaying electronically generated numerals (see Figure 1.1). Digital technology is usually contrasted with and is now often replacing analogue technology. The term analogue or analog shares roots with the word "analogy" meaning it is similar or comparable to something else. Thus, analogue refers to recording, storing and representing information in a way that has variables comparable to each other. Therefore, we usually say that analogue data is recorded, stored and represented in a physical way. Therefore, analogue data is stored in physical

http://www.pbookshop.com

media or by comparing generated electronic signals with a constant signal. Examples include sound recorded in the surface grooves on a vinyl record, the magnetic tape of a four-track audio or videotape recording (VCR) cassette, or the variable density on photographic film which records images as still photographs, or moving images, and the variable density light recordings on the edge of movie films which record audio as the "soundtrack" accompanying the movie. An example of the analogue representation of data would include an analogue clock face. An analogue clock represents time by rotating hands on the dial or face of the clock against figures representing hours which are evenly spaced around the face of the clock (see Figure 1.2).

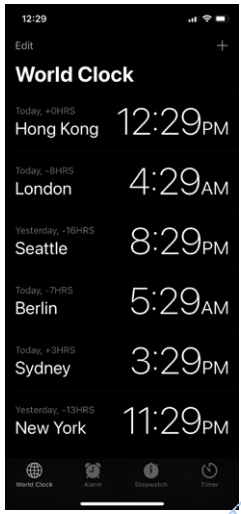

Fig. 1.1 An electronic digital clock face displays time by electronically producing and displaying digits representing the time

Fig. 1.2 An analogue clockwork clock displays time by rotating hands against a clock face with hour representations

http://www.pbookshop.com

Analogue technology uses reference between things to represent, store and transmit data. Therefore, electronic analogue technology transmits data as electronic signals of varying frequency or amplitude that are added to carrier waves of a given frequency. The transmitted signals are compared to the constant given signal to signify a value.

Of course, to complicate matters, clockwork clocks are produced with digital displays (see Figure 1.3), and an electronic digital clock may represent time by electronically generating an analogue representation (see Figure 1.4).

Fig. 1.3 A clockwork digital clock

Fig. 1.4 An electronic digital watch displays an analogue watch face

http://www.pbookshop.com

Although digital clocks represent time using the digits 0-9, in electronic digital technology, the term digital when referring to electronic digital technology usually refers to a series of the numbers 1 (one) and 0 (zero). These two digits, 1 and 0, the binary system, are used to represent the presence or absence of a signal. This signal may be a voltage or magnetic polarisation. Usually, a 1 (one) would represent a signal being present and a 0 (zero) would represent no signal. In electronics this is often referred to as positive and non-positive electronic charge. When the two numbers are put in a linear series, for example "101110010", this is referred to as a string of digits. Electronic digital data is stored as strings of positive and non-positive electronic charges.

The word technology is now often associated with and explained in scientific terms. For example, "technology is a particular method by which science is used for practical purposes".[1] However, a more general meaning of technology is anything created by humans that makes life easier or solves a problem. For example, using this definition, a hammer is technology, as it makes driving a nail into wood easier. Similarly, it may be argued that the law is technology,

[1] Cambridge Dictionary Online. https://dictionary.cambridge.org/dictionary/english/technology. Viewed 23 January 2023.

as, contrary to popular opinion, law is intended to make life easier for us all, to prevent or solve problems.

Therefore, the term electronic digital technology refers to tools, systems, devices and resources having or operating with components such as microchips and transistors that control and direct electric currents, which generate, store or process data in terms of two states: positive and non-positive. Positive is expressed or represented by the number 1 (one) and non-positive by the number 0 (zero). Thus, data transmitted or stored with digital technology is expressed as a series or string of zeros and ones. As there are so many forms of electronic digital technology today, we usually refer to digital technologies, which include all electronic tools, systems, devices and resources that generate, store or process data.

1.3 The Benefits of Electronic Digital Technology

There are many benefits with the use of electronic digital technology. One reason for the preference for electronic digital technology is the problem of deterioration of analogue data and its possible loss. This deterioration may occur because every time analogue data is retrieved, for example a vinyl record is played, damage can occur. This may eventually cause the content to become unusable. Further, every time analogue is copied, noise and other distortions will be added. Thus, there is just no way to make a "perfect" copy of analogue data. As digital data is recorded and stored only as a series of positive or non-positive charges, as long as the devices storing the data are maintained, the data remains as recorded until deliberately changed and limitless numbers of identical copies of the data may be made and distributed.

Electronic digital technology has revolutionised our ability to store, access, process and communicate data. This electronic processing of data stored in an electronic digital form is central to many of the greatest technological developments in recent times. The most important example is, of course, the computer. It is often claimed that data is now our greatest asset. Today, the storage of data is usually in electronic digital form. The electronically stored data can be accessed using computer programmes to cross-reference and classify. The retrieved data can be analysed by computer programmes. The programme usually will contain an algorithm or algorithms which process the data to provide information in the form required by the programme. All these processes are carried out far more quickly than the time it would take for humans to make written records, retrieve written records, analyse the data in these records, and share the original data and analyses. Another benefit is that, as these processes are often repetitive, there has always been an issue with humans getting bored, tired, and distracted, and consequently making errors. Machines do not get tired or bored, they do not make errors. Of course, that does not mean that all machine data in storage or analysis is without error, as humans still predominantly input

http://www.pbookshop.com

data and design the programme for analysis. Thus, there may be, and often are, human errors in the inputting and programming.

1.4 Computers and Hardware

Everyone is assumed to be familiar with computers today, but it is worth refreshing our memories about some of the basics and computer jargon. The term computer is generally used to refer to an electronic device that can store, retrieve, and process data. The data is stored in bits. A bit (binary digit) is the smallest unit of data that a computer can process and store. A bit is always in one of two physical states, similar to an on/off light switch. It is either a positive or non-positive electrical charge. The state is represented by a single binary value, usually a 0 or 1. Computers range in size and computing power, from mega computers with huge computational powers, through desktops and laptops for business, gaming and domestic use, to handheld devices, such as tablets and mobile telephones, and smartwatches.

The term hardware is used to refer to physical devices upon which software runs. These include computers, smartphones, and any device which has computational powers and a physical presence. These also include accessory devices such as a printer, which is a hardware output device, as it prints out the computed data output of the computer when you instruct the computer to print, and a web camera (webcam) which is a hardware input device, as it captures data to input to the computer.

http://www.pbookshop.com

1.5 Software – Computer Programmes, Coding, Algorithms, Apps and Application Programming Interfaces (APIs)

Software is the term used for the computer programmes, codes, algorithms and applications (or apps) which are run on the hardware. Computer programmes, codes and algorithms are interrelated. A computer programme is a detailed plan or procedure for achieving a goal with a computer – the goal is solving a problem and achieving an answer or result. More specifically, the computer programme must be an unambiguous, ordered sequence of instructions, necessary to achieve a solution to a problem. A programme will often contain an algorithm or algorithms as part of these instructions.

An algorithm is a series of instructions for a computer on how to transform data into a useful form of information. It is a set of rules which must be followed in problem solving, for example calculation rules. The algorithm gives instructions as to what the computer must do, what data it must access, what factors are to be taken into account and what variables may affect the processing of the data.

The terms code and coding are often used interchangeably with computer programme and programming, although specifically coding means turning the instructions for the programme into a programming language or form the computer can follow – a computer code, for example the early programming codes such as FORTRAN and BASIC, and the more recently developed programming languages such as COBOL, Python and Java.

Therefore, programming is the implementation of the instructions to solve a problem. This usually involves including algorithms in the programme to process data into a useful form to be used by the programme to reach its goal. The whole programme including the algorithms must be put into code for the computer to be able to follow these instructions. Some programmes developed for artificial intelligence use natural language processing (NLP), which means the programme will convert your written or spoken natural human language instructions into a computer code which the artificial intelligence can process through its main programmes. (Natural language processing is discussed in the section on artificial intelligence).

A mobile or computer app, application or software application is a type of software that can be installed and run on an electronic device – most often a computer tablet or smartphone. An app is a computer programme which carries out a specific task other than one relating to the operation of the computer itself. An app is intended to be used by end-users. Thus an app for booking taxis will be a programme for a computer user, often using a smartphone, which processes all necessary information to find the most convenient and efficient taxi available for the smartphone user. The app accesses data which is used by algorithms to work out if there is an available taxi near you, how long it will take them to get to you, how long the journey will take, consequent costs, prevailing traffic conditions and, often, the maximum fare you will accept based on your previous usage. The app solves the problem of finding you a taxi – hopefully.

An application programming interface (API) is a set of routines, protocols, and tools for building apps. It is a useful tool for building apps as it allows a programme to access another programme and use that to perform a task or tasks. An application programming interface specifies how software components should interact. This is very useful as it means a programmer does not have to spend time programing for all tasks within their programme. They can use existing programmes to perform simple or complex functions within their programme by sending data to this programme for it to perform its task or tasks. The application programming interface allows the programmes to communicate with each other. Application programming interfaces are vital for the development of smart technology, for example accessing apps. Of course, relying on other programmes and sending data to them does raise issues of privacy, security and liability.

Smart technology is any device which uses big data analysis, machine learning, and artificial intelligence to make objects interactive. Examples include smartphones and smartwatches.

http://www.pbookshop.com

1.6 Connecting Computers – The Internet, Cyber, Nodes and Clouds

Computers are usually linked via various networks, sometimes internal networks, but usually external via telecommunications. An internal network is referred to as an intranet. An intranet is a computer network which is used by a particular group of users. Many organisations, public and private, have intranets to internally communicate, share information, collaborate, and for other computing services. An intranet is usually protected by password access. If you are not a member of this group or organisation, usually you should not be able to access this intranet. The most used external network today is the internet. The internet is a global computer network which links billions of computers and other electronic devices. The internet provides a variety of information and communication facilities, consisting of interconnected networks using standardised communication protocols. When our device accesses the internet, it is said to be online. The communication and information sharing of the internet enabled the creation of the World Wide Web, also known as the web or simply WWW. The web, is an information system where information is stored on webpages, often grouped together to form a website. The webpages and websites may contain digital documents, images, audio and/or video recordings etc.

A commonly used prefix in technology is cyber. If a word includes "cyber" or is joined to the word "cyber" by a hyphen, this indicates that it involves computers or computer networks, including the internet, and virtual reality. For example, cybersecurity is the protection of systems, networks, programmes, devices and data from cyberattacks by hackers who access these systems and devices to steal data, take control of the system or device, or just to crash the system or device.

A hacker is someone who can use their technological skills to overcome a problem in electronic digital technology. However, the term is now often used as a shortened form of security hacker, which is someone who uses their technological skills to access computers or systems in cyberattacks, stealing data, running their own programmes and/or crashing the device or system.

Each device linked on a system, whether on an intranet or the internet, is a node. A node is a mathematical term which refers to a point in a network or diagram at which lines or pathways intersect or branch. In computer science and digital technology, a node is a device or data point in a larger network. Nodes may be a connection point, a redistribution point, or a communication endpoint. These include devices such as a personal computer (PC), telephone, or a printer. A modern usage of the term node is for each device on a blockchain. Nodes may also be referred to as peers in peer-to-peer systems.

Computers often store data in the cloud. The cloud is a term for computer servers that are accessed over the internet. These cloud servers store information and may run software remotely. Therefore, the cloud is a data storage centre. The most useful aspect of cloud servers is that users may access the same files and applications from any device, anywhere at any time. This makes access

http://www.pbookshop.com

to information more convenient and more efficient, which should save money. Although the users of cloud storage pay fees for this use, the efficiency and cost saving, combined with not having to provide and maintain your own servers and data storage, may make the cloud an attractive option for many users. The main issue with the cloud is access, as access will depend on a node being able to connect to the cloud, and concern about security of data. Hackers may hack information from cloud servers. Also, it is worth remembering that, although we use the term cloud as some sort of nebulous non-fixed facility, a cloud is a data centre, which is a physical facility. Although that facility may be shared on a network of computing and storage resources, it has physical presence and a geographic location in the real world (IRW). This physical location and the computers storing the cloud information may be subject to failure, as with any machine, or susceptible to accidental or deliberate damage and destruction.

1.7 Web 3.0 and the Internet of Things (IoT)

The term Web 3.0 or Web3 is often used to describe our present age of connectivity on the internet. Also known as the third-generation internet, Web 3.0 is the next evolution of the World Wide Web.

- Web 1.0 was all searching for, retrieving and reading information.
- Web 2.0, our present iteration of the World Wide Web, also known as "the participative social web". It facilitates reading, writing and creating data, and interacting with the end user.
- Web 3.0 is the third generation of the World Wide Web, which is currently a work in progress. This is a vision of a decentralised web with interactive reading, writing, and owning of information. The decentralisation and owning is often facilitated by blockchain technology and the interaction is facilitated by artificial intelligence handling data.

http://www.pbookshop.com

The original idea of Web 3.0 was a development of data analysing using artificial intelligence. Tim Berners-Lee, one of the creators of the World Wide Web, originally referred to Web 3.0 as the "Semantic Web".[2] This would be a data-driven web operating on artificial intelligence. Berners-Lee envisaged an intelligent, self-sufficient, and open internet that employed artificial intelligence and machine learning to function as a "global brain", which could interpret content conceptually and contextually. The present version of the internet, Web 3.0, which is in development, falls short of this "global brain". The focus on the use of technologies like machine learning and artificial intelligence to provide relevant content for each user has been achieved through narrow

[2] Shyamli Jha. Simplilearn.com. 18 November 2022. What Is Web 3.0? Everything You Need to Know About Web 3.0. Viewed 31 January 2023.

artificial intelligence like Siri (Speech Interpretation and Recognition Interface) on iPhones. This uses natural language processing and tailors its responses to the user's questions. Web 3.0 requires more data than ever. This focus of Web 3.0 has changed since the global interest in cryptocurrencies and blockchain technology was sparked by bitcoin and ether. The interest in blockchain technology has added the element of decentralisation to Web 3.0 – the idea that all users will control the internet and assist in the provision of information and its management, but there will be no government or institutional control.

As more data is gathered and processing speeds are increased, electronic digital technology becomes more powerful and is incorporated into many devices. These range from communication, business and commercial tools, our cars, phones, televisions, washing machines, cookers, vacuum cleaners, to exercise devices, such as Fitbit, and multifunctional devices such as Apple watches. These are all now connected through the internet as the Internet of Things (IoT). These devices also provide data to the Internet of Things. Thus, electronic digital technology affects most aspects of our personal and working lives, and we are increasingly reliant upon it, often without understanding how it works, its capabilities, limits, benefits and problems.

http://www.pbookshop.com

1.8 Law and Electronic Digital Technology

Law is a profession which many see as hidebound and loathe to change. However, lawyers often embrace technology, especially if it is perceived to improve efficiency and consequently make lawyers' services more efficient for their clients and more profitable for the lawyers. For example, lawyers' offices were often the first to make use of advances in communication such as the telephone, the telex, and the fax machine. Law offices welcomed the typewriter, the word processor and eventually the computer.

LegalTech or LawTech are terms used for technology used in the practice of law. LegalTech is the use of digital electronic technologies, including artificial intelligence, to assist in the practice of law. These technologies include the computer, basic electronic databases, through e-Discovery, e-Contract drafting and management systems, to artificial intelligence systems which can give assistance to lawyers in giving legal advice or even provide independent legal advice.

LegalTech at its most basic involved the computer. The computer revolutionised the practice of law by making it far more convenient to store and share information. The internet has also made it far easier for lawyers to find information, particularly with open access databases and electronic law reports. It has also made it easier for those seeking assistance with legal issues to have access to lawyers. However, there are a number of legal issues that arise with the use of electronic digital technology for storing and sharing data, for all, but particularly for lawyers. The storing and processing of data, which is what this

technology is all about, brings possible issues with confidentiality, privacy and security. This may be because of simple mistakes and data leaks or cyberattacks by hackers attempting to steal data and either distribute it openly or blackmail those who should have protected the data or those whose data it is. These issues are possible problems that face lawyers utilising this technology in their practice of law. For example, lawyers may wish to use the cloud to take advantage of the ability to access data at anytime and anywhere, particularly firms which have an international practice and which may have offices in different time zones. However, some have expressed concern about the security of data in the cloud and question whether the security of the providers would satisfy professional confidentiality commitments and standards.

1.9 Cybercrime

Cybercrime is crime which involves a computer and/or a computer network. The computer and/or the network may have been used in committing the crime, or the computer and/or the network may be the targets of the crime. Cybercrime often involves cyberattacks. A cyberattack is the accessing of a computer and/or computer system by a hacker to steal data, take control of the device or system, or just to crash the device or system. Cybercrimes raise issues of cybersecurity. Cybersecurity is the protection of systems, networks, programmes, devices and data from cyberattacks. The cybercrime and cyberattacks come in many different forms, and new forms are being developed all the time. At present, the commonest forms of cybercrimes include unauthorised data access or modification, social engineering attacks including phishing, denial-of-service (DoS[3]) attacks, malware, viruses, ransomware, and Internet of Things hacking.

http://www.pbookshop.com

1.9.1 Unauthorised Data Access or Modification

Computers and their linked systems have access to vast amounts of data, much of which is personal and private information of individuals, whether humans or non-living legal entities, such as companies. This data is vulnerable to various forms of cybercrime including attacks by hackers, both human and machine. The risks are heightened because computer systems are linked to the internet, and they may be using cloud storage systems. Data may be accessed by legitimate users of the system in breach of privacy rules and laws. It may also be accessed by illicit users – hackers. Authorised users may inadvertently or deliberately disseminate or otherwise misuse data to which they have legitimate access. Hackers may

[3] The abbreviation DoS is also used for disk operating system. This is an operating system that runs from a disk drive. These operating systems are becoming less common.

access the data illicitly because of compromised passwords. Passwords may be compromised because they are shared with others or because hackers use software or other hacking techniques to identify common and reused passwords, which they can exploit to gain access. Hackers may also be able to eavesdrop on unsecured network traffic or redirect or interrupt traffic as a result of failure to encrypt messages within and outside an organisation's firewall. These are referred to as "network-related and man-in-the-middle attacks." There are also attacks known as "supply chain attacks", which involve linked business or systems which have become compromised, and which permit a hacker a route into a system to attack it or recover data. The information obtained may be used to commit crimes such as blackmail or theft. Personal data used to access banks and other services may involve identity theft.

1.9.2 Social Engineering Attacks and Phishing

Social engineering attacks are a broad range of malicious activities accomplished through interactions with victims, usually online. These attacks use psychological manipulation to trick users into making security mistakes or giving away sensitive information. This may include the wrongdoer posing as a bank, employer or cybersecurity worker and tricking a user into disclosing passwords. These attacks usually happen by the wrongdoer finding out details of the intended victim, often from social media and other online sources. The wrongdoer then has personal information from which to launch their attack, masking themselves as a trusted friend, colleague or financial institution. Wrongdoers may even use such information to guess a password or security protocol, for example by noting a pet's name or a date of birth. Social engineering attacks include phishing, baiting, pretexting, scareware, business email compromise (BEC) and website spoofing.

Phishing involves the wrongdoer initiating communication with the intended victim. If you have ever received an unsolicited email which purports to be from your bank and which asks you to click on a link or reply urgently because your account has been comprised – Don't! These are methods that criminals use to try to trick you into giving them access to your devices and the data stored on them for "data exfiltration", so that they can remove this data. Often, they are trying to trick you into giving them your passwords for your devices and your online banking facilities. If the intent is the latter and they are successful, the data they extract may control your electronic funds.

Information may also be illicitly obtained by website spoofing (or web spoofing). This is where wrongdoers create a replica of a trusted site. Visitors to the site will now interact with the site providing their personal details and perhaps even passwords believing they are dealing with a trusted site. Spoof websites are often almost identical to the original sites.

http://www.pbookshop.com

1.9.3 Denial-of-Service (DoS) Attacks

A denial-of-service (DoS) attack is intended to shut down a computer or network, making it inaccessible to its intended users. A denial-of-service attack floods the target with information, this triggers a crash in the computer and/or system, which may cause a temporary shutdown or slowdown. A distributed denial-of-service (DDoS) attack also floods a system, but this is accomplished by a network of devices sending information to the targeted system. The purpose behind these malicious attacks is often to demand the payment of a ransom to stop the attacks and perhaps explain the victim's system vulnerabilities.

1.9.4 Malware, Viruses and Ransomware

Malware ("malicious software"), often referred to as a computer virus, is a programme that is introduced into a computer or system and which infects, explores, steals or conducts virtually any behaviour an attacker wants. Ransomware is a form of malware. It is a malicious software which is introduced into a system, and which then restricts access to encrypted data or systems until a ransom is paid to the wrongdoer. The ransom may be demanded to release the system, return data or by threats that sensitive data will be provided to others or publicly released if the ransom is not paid. Some attackers threaten to release data if the ransom is not paid. Often, the first many users know of a ransomware attack is their screen freezing, or perhaps a red flashing screen or a message warning the user of danger. They will usually then receive a message demanding payment. To avoid being traced and prosecuted, the criminals often demand payment in cryptocurrencies to take advantage of the confidentiality and anonymity they offer.

Ransomware is often delivered into a system by innocuous seeming emails which require the receiver to click on links or open attachments. These hidden threats are sometimes disguised as free software, videos or music, or seemingly legitimate advertisements. In such hidden form they may be referred to as Trojans, as they are deceptive programmes that appear to perform one function, but in fact perform another, malicious function.

Ransomware and other viruses may also be introduced by so-called "watering hole attacks". These are hackers who observe that their target victim uses a particular website regularly and so introduce their virus to that website. When their victim next visits the website, they access the virus and allow it into their system. The idea is of a lion or other predator watching a watering hole for prey coming to drink.

http://www.pbookshop.com

Demanding money by threatening harm or causing harm and demanding money to stop the harm may constitute the crime of blackmail,[4] for which a convicted person may be imprisoned for a maximum term of 14 years.

1.9.5 Internet of Things (IoT) Hacking

The Internet of Things (IoT) envisages the world where all our electronic devices can communicate with one another. Internet of Things (IoT) hacking exploits insecure interfaces between devices and the internet. The hackers analyse code used to link devices to the internet to find flaws and vulnerabilities in the systems. These vulnerabilities are then exploited to retrieve confidential information or access devices to allow Trojan and ransomware viruses to be implanted or denial-of-service attacks. Some breaches become feasible because of user carelessness. Other insecurities are caused by infrequent software updates and vulnerabilities in the hardware itself.

1.10 Cybersecurity

Cybersecurity is the process of protecting computers and computer systems from accidental damage to the system and loss of data, or from deliberate cyberattack by cybercriminals. Cybersecurity is sometimes referred to as computer security or information technology security. Cybersecurity may vary from the basics of not disclosing your passwords to others, to the spending of millions of dollars on advanced anti-virus and other technology. Concerns about cybersecurity, especially on computer systems linked to the internet, mean that many corporations have closed systems which restrict users from downloading data, for example by not allowing USB and other data storage devices from being linked to the system, and even running on an intranet to prevent access and vulnerability to external internet attack. In July 2022, it was proposed to Hong Kong's Legislative Council that new criminal offences should be introduced to help deal with cybercrime.[5] These would be – illegal access to a programme or data, computer data interception and interference, computer system interference, and provision or possession of devices or data for criminal purposes. However, even if these laws are introduced there may be issues in enforcing them, as the perpetrators may be difficult to identify, given the anonymity possible on the internet, and they may be anywhere in the world, which raises issues of jurisdiction.

http://www.pbookshop.com

[4] Theft Ordinance, section 23.

[5] Tony Cheung. South China Morning Post. 7 November 2022. Proposed cybercrime law needs long reach to cover offences outside Hong Kong, compel tech giants to cooperate: legislators.

1.11 Summary

Possibly the most complex part of understanding technology today is the language used. The term technology itself is used most often to refer to electronic digital technology. Electronic digital technology refers to tools, systems, devices and resources having or operating with components such as microchips and transistors that control and direct electric currents, which generate, store or process data in terms of two states, which are usually represented by the numbers 1 (one) and 0 (zero). Data stored, processed and transmitted with digital technology is expressed as a series or string of zeros and ones, which in electronic form is a series of positive and non-positive electronic charges. As there are so many forms of electronic digital technology today, we usually refer to digital technologies.

Computers use electronic digital technology to store, retrieve, and process data. Computer technology is often referred to as cyber-technology. Computers are usually referred to as hardware, whereas the programmes they run are referred to as software.

Software is the term used for the computer programmes, codes, algorithms and applications (or apps) which are run on the hardware. A computer programme is a detailed plan or procedure for achieving a goal with a computer. This may consist of an algorithm or algorithms which are a series of instructions for a computer on how to transform data into a useful form of information to be used by the programme to solve the problem. The programme has to be turned into code for the computer to follow the instructions. A computer programme which carries out a specific task for our everyday lives may be turned into an app. Sometimes, to make programming easier and more efficient, the programmer will set up the programme to access other programmes which have already been set up to perform particular functions through an application programming interface. This allows the programme to send data to other programmes for them to perform their task or tasks and then receives the processed data back and incorporates it into the next step of its instructions.

Computers are linked via internal networks, called intranets, and external networks via telecommunications. The most popular external network is the internet, which is a global network connecting all sorts of computers. Each computer device linked on a system is a node. The World Wide Web is an information system which exists on the internet. As information storage is often the most limiting factor in computer processing, many now use cloud data storage, where large computer servers, or storage devices, are accessed for storage and processing data via the internet. However, there is one major problem with storing data in electronic form – it deteriorates and may be lost. The average lifespan of a digital hard drive is three to five years. This applies to your digital hard drive in your laptop and the digital hard drives in cloud storage facilities. Hard drives fail for several reasons, whether magnetic or solid state. They may suffer from mechanical failure, format obsolescence, dust and heat. There is even a form of decay at the microscopic level that computer scientists call “BitRot”,

http://www.pbookshop.com

where the bits lose or flip their magnetic charge. Although cloud storage providers can guard against this and provide more backups and checks on data, there is still a risk of data loss and corruption.

Computers and their connecting systems, including the internet, are vulnerable to cybercrime including various forms of cyberattack. These cybercrimes may involve theft of data, attacks on the computers or systems themselves to close them down, and demands of money from cybercriminals. Cybersecurity is something we should all be concerned about, especially lawyers, as cybercrime not only forms a major area of practice today, but lawyers are often targets of cybercrime because of the confidential and sensitive data they manage.

Further issues arise with the products derived from electronic digital technology, this includes, at present, artificial intelligence, blockchains, cryptocurrencies, non-fungible tokens, smart contracts, and the metaverse.

http://www.pbookshop.com