Singapore Journal of Legal Studies
[1994] 263 – 331

OFFENCES CREATED BY THE COMPUTER MISUSE ACT 1993[1]

This article analyses the terminology used in defining the offences created by the Computer Misuse Act 1993. Comparison is made with similar legislation from other jurisdictions which influenced its drafting, particularly the United Kingdom Computer Misuse Act 1990. It appears that the guiding principle behind the drafting of this Act is comprehensiveness – the offences are framed so as to cover every conceivable misuse of computers, but this has been achieved only at the cost of ease of interpretation.

I. INTRODUCTION

IN Singapore, debate about the criminality of 'computer hacking'[2] and the need for criminal legislation to deal with computer misuse[3] ended with the passage of the Computer Misuse Act (the Act). In fact, there was perhaps never really any question in the minds of Singapore's legislators since, of the five Members of Parliament who spoke at the Second Reading of the Computer Misuse Bill in Parliament, none questioned the desirability of

1 No 19 of 1993. The Act was passed by Parliament on 28 May 1993 and assented to by the President on 9 July 1993. It came into force on 30 August 1993 (GN No 348/93).

2 The term 'hacking' is not a term of art, though it is commonly used to describe the conduct of 'hackers'. That latter term originally referred simply to a person with a great deal of knowledge and expertise in computer technology. Of late, however, the term has taken on a negative connotation. A recent definition is of "an unauthorised person with expertise who uses this knowledge to gain illegal access to [c]omputers and [d]ata [c]ommunication [s]ystems, often for the purposes of sabotage, interference or gain" – Lynch, *The Concise Dictionary of Computing and Information Technology* (1991). The term 'hacker' will be used throughout this article in this narrower, negative sense of a person who seeks access to computer networks or services provided by a network without permission, usually from some remote location through a telephone link with that computer system, and who may in the process by-pass security features of that system. It was this type of activity which the UK Computer Misuse Act was meant to deter. The term 'hacking' will be similarly used to denote the activity of seeking unauthorised access to computer systems.

3 Terence Tan, "Computer Crime Legislation – More Bite Needed for Byte Law" [1990] 3 MLJ lxxxvi and KT Lim, "Information Technology and the Law – Protection against Computer-Related Crimes" [1990] 1 MLJ xcviii. *Cf* SK Toh, "Computer Crime in Singapore – Should We Legislate" [1991] 2 MLJ xvii.

imposing criminal penalties for computer misuse.[4] Perhaps any doubts in the minds of the Members of Parliament were overcome by the passage in the United Kingdom (UK) three years earlier, of similar (and similarly named) legislation (the 'UK Act').[5] If this was indeed the case, it was ironic that the passage of the Singapore Act was preceded just days earlier by newspaper reports celebrating the acquittal of an English teenager of charges brought against him under the UK Act.[6] This article will not consider that debate about the criminality or otherwise of computer misuse but will instead analyse the terminology used in the offences under the Act.

In his speech to Parliament to introduce the Second Reading of the Computer Misuse Bill, the then Minister for Home Affairs, Professor S Jayakumar, stated[7] that existing legislation[8] was inadequate because:

1. Difficulties arose in applying rules of criminal law dating from the 18th century to computer-assisted crimes;[9] and

2. Existing penalties were sometimes insufficient to deter computer-assisted or related crime.[10]

The Act was intended to deal with these concerns by introducing new offences modelled largely on those created by its UK counterpart. No changes were made to the then existing rules of criminal law (which are largely contained in the Penal Code)[11] to make them more appropriate in dealing with the new technology, so the burden of addressing shortcomings in the

4 *Parliamentary Debates, Singapore Official Reports*, 28 May 1993, cols 304 to 316.

5 The Computer Misuse Act 1990 (1990, c 18).

6 *R* v *Bedworth and others* (unreported). The result in that case was reported in The Straits Times, 22 May 1993 and is considered in Charlesworth, "Legislating Against Computer Misuse: The Trials and Tribulations of the UK Computer Misuse Act 1990" (1993) 4 JILS 80. That article also notes other cases where convictions under the UK Act were successfully obtained.

7 *Supra*, note 4, at cols 300 and 301.

8 Some rules of law that might have been called into service against computer misuse were considered in KT Lim, "Information Technology and the Law – Protection against Computer-Related Crimes" *supra*, note 3.

9 *Ibid*. It is not clear from this speech exactly what difficulties were contemplated. Some general discussion of the problems that could arise in attempting to apply the law prior to the Computer Misuse Act can be found in the English Law Commission Working Paper on Computer Misuse (Working Paper No 110) and in the articles cited at note 3, *supra*.

10 Although not expressed in the Minister's speech, the likely reasoning why more severe penalties were felt necessary to deter this type of crime is the extreme difficulty of detection and prosecution. Potential criminals would only be deterred from committing such offences if the consequences were so serious as to outweigh the probability of avoiding successful prosecution.

11 Cap 224, 1985 Rev Ed.

law fell entirely on the Act. It is submitted that the Act is not entirely successful. While the new offences criminalise hacking and other computer-specific forms of computer misuse that were the major concerns behind the Act, the offences are drafted in terms that make them difficult to understand and apply. Dealing as they do with new types of offences and interests arising from new technology, the legal concepts used as the basis for the new offences are not sufficiently clear for their scope to be properly understood. It would appear that the main lesson to be drawn from this Act is the importance of conceptual clarity in statutory intervention in an area of law where practice and technology have overtaken the existing legal regime.

The UK Act and other provisions of law on which much of our Act is based have already been the subject of a number of books and articles,[12] so issues already discussed in relation to their UK equivalents will be given only cursory treatment.

II. Drafting of the Act

A. *Scheme of the Act*

Part I of the Act sets out definitions and explanations of various terminology used in the Act. Given that the subject-matter is conduct associated with and new interests created by computers, technical terms such as 'access' to a program or data,[13] 'unauthorised access' to a program or data,[14] 'modification' of the contents of a computer[15] and 'unauthorised modification' of such contents[16] are used to describe the offences, and are the subject of explanations in this part. All of these explanations adopt the terms used in the UK Act. One significant term not defined in the UK Act but which is defined here is 'computer'.[17]

[12] On the substantive offences, see, for instance, Wasik, *Crime and the Computer* (1991); Wotherspoon, "The Computer Misuse Act 1990" [1991] LMCLQ 391; and Wasik, "The Computer Misuse Act 1990" [1990] Crim LR 767. Reference may also usefully be had to the Report of the English Law Commission (*Criminal Law: Computer Misuse*, Law Commission No 186, Cmnd 819 (1989)) around whose recommendations the UK Act was drafted. The Singapore Act has been discussed in Leong, "The Computer Misuse Act 1993" (1993) 15 EIPR 381.

[13] S 2(2).

[14] S 2(5).

[15] S 2(7).

[16] S 2(8).

[17] S 2(1). A discussion of this definition and its implications is to be found at the main text accompanying notes 22 to 27, *infra*.

The crux of this legislation and the focus of this article lies in Part II of the Act comprising sections 3 to 7 which set out the new criminal offences. Sections 3, 4 and 5 correspond to sections 1, 2 and 3 of the UK Act and the similarities between the two sets of provisions are obvious, though subtle changes in the words used to define the offences call for some comment.

Sections 3 and 4 were drafted with hacking in mind. Section 3 creates the basic offence of using a computer to obtain access to programs or data without authorization. It is couched in such wide terms as to criminalise all conduct that could amount to hacking as well as some conduct that would not be considered to be hacking. The section 4 offence involves essentially the same conduct as section 3, but imposes a heavier punishment where the motive behind the conduct is the commission of some further criminal offence. Like the corresponding UK provisions, section 3 and 4 are meant between them to provide a two-tier approach to the punishment of hacking, recognising that a distinction is to be made between persons who hack without criminal intent and those who hack with an ulterior criminal purpose in mind. The very act of hacking is considered serious enough to warrant at least the penal consequences in section 3, while section 4 provides more severe punishment for the latter.

Section 5 is concerned with a different type of misconduct; it creates criminal liability where a person modifies the contents of a computer without authority. Such conduct can be compared to that covered by the Penal Code offence of mischief,[18] except that the offence here is directed at 'damage' to information rather than corporeal property.

Section 6 stands out for separate consideration because it introduces three offences which are not drawn from the UK Act. The offences of unauthorised use of a 'computer service', unauthorised interception of any 'function' of a computer and use of a computer to commit the first two offences are adapted from the Canadian Criminal Code.[19] They represent a different approach to criminalising hacking from sections 3, 4 and 5. It will be argued that, with the exception of the offence of 'unauthorised interception', the offences created by section 6 are largely redundant, covering very much the same types of conduct as other offences in the Act and other criminal offences that pre-date the Act.[20]

Section 7 punishes abetment of and attempts to commit the offences outlined earlier. This provision also does not have an equivalent in the UK Act, and recites the formula for abetment and attempt used in section 12 of the Misuse of Drugs Act.[21]

[18] Defined at s 425 of the Penal Code.
[19] Chap C-46, Statutes of Canada.
[20] *Infra*, main text accompanying notes 134 to 158.
[21] Cap 185, 1985 Rev Ed.

Part III of the Act deals with ancillary matters to the enforcement of the Act: section 8 defines the extra-territorial application of the offences created by the Act; section 9 grants jurisdiction to District and Magistrate's Courts to hear cases under this Act and section 10 creates a power to issue compensation orders against persons convicted of offences under the Act. Sections 11 to 13 set out special provisions on evidence while sections 14 and 15 supplement police powers to investigate and arrest. These miscellaneous provisions will not be considered as they are outside the scope of this article.

B. *Part I – Interpretation*

1. *Definition of 'computer'*

Section 2(1) of the Act defines the term 'computer' as:

> an electronic, magnetic, optical, electrochemical, or other data processing device, or a group of such interconnected or related devices, performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device or group of such interconnected or related devices, but does not include an automated typewriter or typesetter, a portable hand held calculator or other similar device which is non-programmable or which does not contain any data storage facility.

This definition does not have an equivalent in the UK Act and is based on the definition in the US Federal Computer Fraud and Abuse Act 1984.[22] In fact, the English Law Commission in its report on computer misuse expressed the view that a statutory definition of this term was unnecessary and perhaps even undesirable.[23]

The proviso to the definition beginning with "but does not include..." shows that certain devices are not considered sufficiently computer-like (or the consequences of tampering with them are so trivial) that they fall outside the Act.[24] This proviso suggests that any other data processing devices that

[22] Title 18 USC, s 1030(e)(1).

[23] *Supra*, note 12, at para 3.39.

[24] Those words do give rise to practical difficulties in interpretation. For instance, the phrase "portable hand held calculator" is not at all clear. Devices that could be called "portable hand held calculators" vary enormously in sophistication and computing power, from the simplest of numerical calculators with only basic arithmetic functions to the most sophisticated scientific calculator (or perhaps digital diary or Personal Digital Assistant) with considerable memory capacity. The latter may deserve to be called a 'computer'. The

do not fall within that list are likely to be a 'computer' under the Act. It is not clear if the qualifying words "...which is non-programmable or which does not contain any data storage facility"[25] at the end of this phrase qualifies only the words "other devices", or the entire phrase. If the latter, then even a relatively simple hand held calculator which contains a limited 'memory' function is a 'computer' by virtue of that minimal data storage facility. The qualifying words also suggest that for devices other than those listed in the *proviso*, the ability to be 'programmed' or existence of a data storage facility strengthens the likelihood that they are 'computers' under the Act.

The definition which found its way into the Act was clearly intended to be sufficiently wide and flexible to cover future (and even unexpected) developments in computer technology. It is doubtless successful in applying the Act to devices like Automated Teller Machines (ATMs) and the implications of this will be considered later.[26] It is, however, the writer's view that the result of such drafting is to cast the net too wide. This definition applies the Act to devices that do not at this present time have the qualities that would bring them within the mischief at which the Act is directed.[27] Tampering with devices such as telefacsimile machines, electronic alarm clocks and electronic fuel injection systems in motor vehicles, to name a few, cannot be so serious a matter as to be worthy of special penal sanctions beyond those already contained in the Penal Code, if any criminal liability is called for at all. Technically, those acts are now capable of amounting to offences under the Act as a result of this definition.

Arguments based on the other terms by which the offences are described, and on general principles of criminal law, are available to suggest that acts such as resetting an alarm clock without permission or surreptitiously picking up a telephone extension to eavesdrop on a conversation do not constitute offences under the Act.[28] It is, nonetheless, submitted that a

terms of the definition leave us with the uncomfortable exercise of drawing a line between the two extremes.

25 These words do not appear in the definition in the US Act (*supra*, note 22 and accompanying main text), and that definition is perhaps better for it.

26 See the main text accompanying notes 178 to 186, *infra*.

27 It must, however, be borne in mind that advances in technology may (if they have not already done so) result in what are now trivial devices eventually playing so significant a role in commerce or society generally that tampering with a program or data in that device will have serious enough consequences to justify application of the Act.

28 For instance, see the discussion on s 79 of the Penal Code at the main text accompanying notes 65 to 67, *infra,* and the *de minimis principle* in the main text accompanying notes 174 and 176, *infra*. A more fundamental argument based on interpretation of this definition might be that notwithstanding the express words of the definition, there is a further implied limitation on the application of this Act based on a common sense understanding of what devices are 'computers' (*ie,* devices that should be singled out for special protection). Such

criminal provision should not be drafted so widely as to make criminal offences punishable with significant penalties out of such innocuous behaviour even if a defence is available. If it is clear to the public that some conduct which clearly falls within the terms of an offence under the Act is unlikely to be prosecuted because it amounts to a mere technical offence that results from an overwide drafting, then the persons at whom the Act was directed might form the conclusion that their conduct, too, was only technically an offence and the desired deterrent effect of this statute may be lost.

It may perhaps have been preferable to leave the courts to develop an understanding of what types of devices were meant to be covered by this Act in the knowledge that 'common law' definitions are capable of being adapted as circumstances change. In this regard, instead of attempting a statutory definition, express provision could have been made in the Act that the significance of consequences of misuse of a particular device (a factual matter to be determined by a court considering an offence under the Act) should be the test for whether that device comes within the Act. As things stand, the wide definition of 'computer' coupled with increasing use of microprocessors in everyday household items like vacuum cleaners, refrigerators and microwave ovens is likely to spread the reach of the Act well beyond what may have been the intention of the legislature.

For the purposes of this article, the term 'conventional computer' will be used to denote devices which a layman would consider to be a computer properly and so-called (that is, personal computers, mini-computers and mainframe computers), while devices falling within the statutory definition of computers which are not generally thought of by laymen to be 'computers' will be referred to as 'other electronic processing devices' where a distinction is to be made between them.

Difficulties raised by the other definitions and explanations in the Act will be considered later in the context of the provisions in which those defined expressions appear.

2. *'On-line computer systems'*

Although a large part of the Report of the English Law Commission[29] (whose recommendations formed the basis of the UK Act) was devoted to consideration of the special problems raised by on-line computer systems,[30]

a resort to extraneous considerations would defeat entirely the objective of expressly defining the term 'computer' in the Act.

29 *Supra*, note 12.

30 *Ibid*. A major area of concern was the obtaining of unauthorised access from a remote computer *via* telephone or other links. The discussion in that Report under the heading "The Threat Presented by Hacking" at paras 2.10 to 2.25 was almost entirely concerned with such practices.

neither the UK Act nor our local equivalent makes specific reference to this area of concern or distinguishes these computer systems from other types of computers. There was in fact no need to do so because the offences created by the Act are defined in such general terms that they are capable of dealing with misuse of on-line computer systems as well as other types of computers. Even so, it is desirable at this point to note that it is the combination of computer technology and modern telecommunications techniques that lies at the heart of the mischief against which the Act was directed. The manner in which remote users can obtain access to on-line computer systems is relevant to a proper understanding of the new offences and will thus be described briefly below. It is not possible in this article to explain the technological background in any great detail; readers who wish to pursue the technical background further may refer to other sources.[31]

The phrase 'on-line computer system' was not specifically defined or explained in the English Law Commission Report but the language used implies that 'computer systems' are a sub-class of 'computers'.[32] That term (and in particular, the words 'on-line') was probably used there (as it will be used here) to refer to groups of computers which are interconnected as networks and bulletin boards; that was probably meant to exclude from the discussion computers which operate in isolation from other computers (hereafter referred to as 'stand-alone computers').

The terms 'network' and 'bulletin board' will be used to denote two major types of implementation of on-line computer systems. Neither of these terms is used as a term of art or in a strict technical sense; they merely serve to indicate some characteristics of the two types of implementation which are significant for our purposes.

The term 'network' will be used here to denote a system consisting of two or more computers which are connected so as to be able to share information or resources. In practice, networks tend to be organised in such a way that communication between computers and other devices is routed through one or more machines ('servers') which are dedicated to facilitating this communication. Such an arrangement is called a 'client-server' relationship. The server may also store programs and data for use by all (or some) of the computers in the network. A hacker who hacks into a 'network' would necessarily obtain access to data or programs stored in

[31] Some explanation of the technical background to our discussion is set out in Part I of the English Law Commission Report, *ibid* at paras 1.14 to 1.36. Basic information about computers is also to be found in books such as Long, *Introduction to Computers and Information Processing* (4th ed, 1994), Corbitt, *Information Technology and Its Applications* (1990), Ron White, *How Computers Work* (1993) and *How Software Works* (1993), and Derfler & Freed, *How Networks Work* (1993).

[32] *Ibid*, para 1.1 and in particular at footnote 1.

one or more network servers even if his ultimate objective was to obtain access to the contents of a 'client' computer. Our analysis of offences of hacking into networks will thus focus on the process of gaining access to network servers and the interests of the person who owns or operates the server (the 'system provider') or the person who manages the network on his behalf (the 'system operator'). Of course, more complex arrangements are possible; there are networks where every computer connected to the network acts as both client and server; such an arrangement is called a 'peer-to-peer network' and analysis of hacking offences in relation to such networks would be correspondingly more complicated.

Networks tend to be set up within large organisations, although they are being used increasingly by smaller organisations as computers become cheaper and easier to use. Networks are also sometimes set up by groups of organisations and/or individuals who wish to be able to share information and programs. In either case, identification of the system provider is simple in the case of client-server networks: the party who provides the services of the network server would be the system provider for our purposes, while the system operator (if any) would be an employee of the system provider. In peer-to-peer networks, identification of a system provider may not be easy; reference may have to be had to the contractual or other arrangements between the parties.

The term 'bulletin board' is used in this article to indicate a centralized information source and message switching system run on one or several computers. For convenience, the computers which contain the software to run the system and store data in the form of messages and information will also be called 'servers' in this article. The system is 'on-line' in the sense that users of the bulletin board can get access to the server and its contents using a modem and a regular telephone line or other permanent telecommunications link. Once a connection is made with the server, users can write messages and send computer files to the server or download files or messages from the server to their own computers. Again, for the purposes of this article, the person providing the service (who need not be the owner of the server) will be called the 'system provider' and it will be around him that our analysis of the offences will be built.

The distinction between the terms 'bulletin board' and 'network' as used in this article lies not in the characteristics of the hardware or their interconnections, but in the tendency for networks to be a facility provided by an organization or group of organisations to facilitate interchange of data and communications between members of that organization, while bulletin boards here denote services provided by the system provider to members of the public or a sector of the public. Subscribers to a bulletin board are more in the nature of consumers of a service. References to bulletin boards will be confined to consideration of specific arrangements between

users and a service provider for occasional access to that particular service. Most networks actually have some bulletin board features that permit users to post messages for general information or direct messages to particular members of the organization, but these will be ignored for the purposes of this article.

Interactive on-line databases (such as Lexis) will be treated as a type of bulletin board. These databases involve the provision of data as well as computer-based services that facilitate access and reference to desired items of data. The user only obtains access when he chooses to and pays for these services on the basis of usage or by a fixed subscription fee. The different commercial and practical arrangements attaching to the implementation of on-line databases set them apart from traditional computer bulletin boards, but since their essential characteristics for the purpose of this article are those of a bulletin board (that is, the relationship between user and system provider is one between consumer of services and service provider, and access is occasional), references hereafter to bulletin boards will include such database services.

C. *Part II – The Offences*

1. *Section 3 – unauthorised access*

This provision creates what has been called the 'basic hacking offence',[33] a description which is somewhat misleading since the terms by which the offence is defined affects conduct that falls well outside the description of hacking mentioned earlier in this article.[34] The essence of the section 3 offence is that "any person who knowingly causes a computer to perform any function for the purpose of securing access without authority to any program or data held in any computer shall be guilty of an offence..."

This offence is clearly based on section 1(1) of the UK Act which reads as follows:

> A person is guilty of an offence if –
>
> (a) he causes a computer to perform any function with intent to secure access to any program or data held in any computer;

[33] That description was used, for instance, in Colvin, "Computer Misuse Act 1990" [1990] CL&P Nov/Dec 46. The author of that article was the Member of Parliament who moved the UK Act as a Private Member's measure. That description is also used extensively in the English Law Commission Report (*supra*, note 12).

[34] *Supra*, note 2.

(b) the access he intends to secure is unauthorised; and

(c) he knows at the time when he causes the computer to perform the function that that is the case.

The UK provision sets out the major elements of the offence with greater clarity than its Singapore counterpart. The mental elements of section 3 are particularly difficult to discern. It is clear enough under section 3 that a person must 'know' that his physical act would "cause a computer to perform a function" but it is less clear whether this knowledge requirement extends to the other matters set out in the provision; for instance, to the fact that he lacks authority. Similarly, it is not clear from the words of section 3 whether the requisite 'purpose' is simply the securing of access to program or data, or whether it is to secure access without authority.

In attempting to understand this provision, the traditional criminal law classification of the ingredients of an offence into the *actus reus* and *mens rea* is not particularly helpful, given the complexity of this provision.[35] It is proposed to ignore this traditional distinction in our discussion. We will consider instead three major elements of this offence in the following order:

(a) *the physical act element* – this is satisfied where the offender "causes a computer to perform [a] function"

(b) *the purpose element* – the physical act must have been performed "for the purpose of securing access without authority to any program or data held in [a] computer"; and

(c) *the knowledge element* – the words of section 3 make it clear the offence must be committed "knowingly".

The knowledge element is considered last because a major discussion arising here is the question of exactly what section 3 requires the potential offender to have knowledge of. Conclusions reached in relation to the other elements of this offence will be relevant to that discussion.

(i) *The physical act element – "causing a computer to perform a function"*

The marginal note to section 3 describes the offence as obtaining "unauthorised access to computer material". This can give rise to an incorrect

[35] It could for instance, be argued that the *actus reus* of this offence involved performing the physical acts 'with knowledge'; alternatively, the knowledge specified in s 3 could be taken to be part of the *mens rea*. Since it is not necessary to resolve this matter, no more will be said on this point.

impression of what the offence actually involves since it is clear from the words of section 3(1) that the physical act which triggers this provision is the "causing of a computer to perform any function". There is no requirement that access to the contents of the computer be obtained for the offence to be made out.

The term 'function' is given such a wide inclusive definition in section 2(1) that practically any act of operating a computer would fall within it.[36] Simply switching on a computer causes that computer to perform several 'functions' as the computer executes the logical operations involved in 'booting up'. The physical act element of this offence can therefore be easily satisfied, and this is likely to happen well before a potential offender even comes close to achieving his purpose.

The use of the phrase "causes a computer to perform any function" means that the physical act element may be performed by a person who does not physically operate a computer but who causes some third party to do so on his behalf.

Read thus with the extremely broad definition of 'computer',[37] the physical act element of this offence can be easily satisfied by conduct which would not ordinarily be considered to be 'use' or 'operation' of a 'computer'. For instance, inserting a forged Automated Teller Machine ('ATM') card in the machine would cause that machine (certainly a 'computer' under the wide definition in the Act) to perform a number of 'functions'.[38]

Since the physical act element is defined by reference to the potential wrongdoer's conduct (and conduct which is likely to occur well before an offender can achieve the desired result) rather than its consequences, damage or injury is not required for the offence of unauthorised access to be constituted.[39]

[36] S 2(1) states that this term includes "logic, control, arithmetic, deletion, storage and retrieval and communication or telecommunication to, from or within a computer".

[37] Discussed in the main text accompanying notes 22 to 27, *supra*.

[38] The operation of ATMs is described in A Arora, *Electronic Banking and the Law* (2nd ed, 1993), Ch 5. The use of the s 4 offence in relation to offences connected with ATM machines is considered, *infra*, in the main text accompanying notes 178 to 186.

[39] The English Law Commission in its Report, *supra*, note 12 at paras 1.29 to 1.35, pointed out that any incident of unauthorised access, whether or not accompanied by damage, leads to such costs as would justify deterrence. It further stated at paras 1.37 and 2.11 to 2.15 that the aim of UK equivalent to s 3 is "protection of the integrity and security of computer systems"; so the causing of physical damage is quite irrelevant to the thinking behind this offence.

Although damage is not necessary for the offence to be constituted, s 3(2) provides for an enhanced penalty if "any damage is caused by an offence under [s 3] which exceeds $10,000". This enhanced punishment and the term 'damage' is discussed in the main text accompanying notes 159 to 166, *infra*. There is no equivalent of this enhanced punishment provision in the UK Act.

(ii) *The purpose element: "for the purpose of securing access without authority to any program or data"*

(a) *'Purpose'*

The physical act element must be performed for a particular purpose: that of "securing access without authority to any program or data held in any computer".[40] The term 'purpose' in a criminal statute has been held to denote not simply the main object of the proscribed conduct but also "those objects which [the offender] knows will probably be achieved by the act, whether he wants them or not".[41] It is therefore not necessary for an offender to consciously seek unauthorised access to any program or data. If securing unauthorised access is a necessary incident of his broader objective, then one can say that his 'purpose' was to secure that access.

This interpretation of the term 'purpose' requires that the offender knows of certain consequences of his acts. In particular, he should know that his acts are likely to lead to his 'securing access' to the contents of a computer, and that this access is 'unauthorised'. The remainder of this discussion on the purpose element will only consider the meaning of these terms 'access' and 'authority', while the question of what it means for an offender to have 'knowledge' of these matters will be considered in the discussion of the knowledge element.[42]

(b) *'Access'*

'Access' is explained in sections 2(2) and 2(3) to cover a wide range of operations, including running a program, use of data in a computer or causing program or data to be output, modified, altered, copied, moved or otherwise manipulated. Simply switching on a computer and causing it to boot up will amount to obtaining 'access' to its contents since some basic instructions stored in a ROM chip in the computer would be executed in the process. This explanation, together with section 3(3) (which states that there is no need to show that the intention to 'secure access' was directed at any particular program or data or even a program or data held in any particular computer), means that any person who switches on a computer

[40] A recent English case, *Attorney-General's Reference (No 1 of 1991)* [1993] QB 94 held that the UK equivalent of our s 3 applies equally to unauthorised access to data or programs in the computer being operated by the offender just as much as it does to the classic hacking scenario, where the computer to which access is sought is a distinct device from the one being operated directly by the offender. Such a reading follows naturally from the use of the words 'any computer' in the quoted phrase.

[41] *Chandler* v *Director of Public Prosecutions* [1962] All ER 142 at 155 *per* Lord Devlin.

[42] *Infra*, main text accompanying notes 72 to 84.

in order to use it will inevitably have done so for the 'purpose'[43] of obtaining 'access' to its contents.

(c) *'Authority'*

Had the Act not contained a definition of the term 'authority', a court construing section 3 would probably have interpreted that term in the usual way – by reference to the type of mischief at which the Act was directed. Reference to the report of the English Law Commission on Computer Misuse[44] would have shown that in the classic situations of hacking (at which the UK equivalent of this provision was directed), there would be no difficulty determining whether that particular access was authorised. The English Law Commission had no doubt that a remote hacker who obtained access to a computer system without permission from the system provider or the person managing the system on his behalf would be 'unauthorised'.[45] And where the potential offender was an 'insider' in relation to a computer system (*eg,* an employee whose job involved some use of the employer's computer system), proving authority or want of it was a matter of analysing the relationship between potential offender and system provider, provided that relationship was governed by clear rules regulating the use of the system.[46] The English Law Commission's consideration of the meaning of 'authority' did not go beyond these fairly obvious types of potential offenders because that represented the main area of concern behind their recommendation of the 'unauthorised access' offence.

Such an understanding of the concept of 'authority' would have been quite adequate had the section 3 offence been confined to dealing with simple hacking. As has been pointed out earlier[47] the very wide terms by which

[43] This term is used in its technical sense; see the main text accompanying note 41, *supra*.

[44] *Supra*, note 12, at para 3.34. An interesting question arises whether s 9A(2) of the Interpretation Act, Cap 1 1985 Rev Ed (inserted by s 1 of the Interpretation (Amendment) Act (Act 11 of 1993), which permits courts in Singapore to consider material not forming part of a statutory provision to aid in interpretation of that provision, extends to the use of material relating to a foreign statutory provision on which a local statutory provision was based. For the purposes of this discussion, it is assumed that such recourse is permitted.

[45] *Ibid*.

[46] *Ibid*, at para 3.37. The means of regulating use of the system would depend on the nature of the system and the type of use involved. In the case of a bulletin board to which members of the public subscribe, rules of use would be found in some form of agreement having contractual force; the manner in which this contract arises is discussed in greater detail at note 53, *infra*. An in-house computer network used by employees of a large concern would be governed by regulations made by the employer under its contractual power to give instructions to its employees.

[47] *Supra*, main text accompanying notes 24 to 27, and 36 to 38. Some other non-hacking conduct which would give rise to offences under this provision are described in the main text accompanying notes 178 to 203, *infra*.

the section 3 offence has been defined means that the offence may cover conduct beyond our understanding of the term hacking. The meaning of 'authority' in relation to non-hacking section 3 offences would, in the absence of statutory definition, have been left to the courts to develop and questions of this nature would have been left unresolved until case law provided the solution.

Section 2(5) of the Act makes some attempt to explain the concept of 'authority' to have access to programs or data generally, but it is submitted that this statutory explanation is of little assistance in situations where it is not already obvious whether a particular occasion of access is 'unauthorised' or not. The result of that explanation is merely to add a further layer of complexity to this already difficult exercise of determining what 'authority' means.

Section 2(5) provides:

> For the purposes of this Act, access of any kind by any person to any program or data held in an computer is unauthorised or done without authority if –
>
> (a) he is not himself entitled to control access of the kind in question to the program or data; and
>
> (b) he does not have consent to access by him of the kind in question to the program or data from any person who is so entitled.[48]

This explanation is built around the identification of a person who is "entitled to control access of the kind in question" to that program or data (hereafter to be referred to as 'the Entitled Person'). Where access is by the Entitled Person or he has given consent to access,[49] then that access is 'authorised'. It thus appears that where there is no Entitled Person in relation to access to any particular program or data, any access to that program or data must by definition always be 'unauthorised'.[50]

[48] The UK Act contains a similar explanation of this term in s 17(5).

[49] It is implicit in the definition that 'consent' given by the Entitled Person may be general (that is, consent to a person or group of persons to have access to all the program or contents, not limited to any particular occasion) or particular (to one particular occasion of access by a particular person, and only to particular contents of the computer). It is also likely that consent may be subject to conditions; the provider of a bulletin board service may only consent to subscribers having access so long as they are not in arrears of subscription.

[50] The terms of s 2(5) does not exclude the possibility that no Entitled Person may exist in relation to a program or item of data, or that there may be more than one Entitled Person.

The critical weakness of this statutory explanation is that it gives no indication what the nature of this 'entitlement' to control access could be. One can imagine several scenarios where it will not be clear who the Entitled Person is. For instance, where a network provider does not own the computer which acts as network server but uses a third party's computer as his server, is the network provider or computer owner the person who is 'entitled' to control access to the contents of the server? Or take the case of a network provider who uses a number of network servers in different physical locations in conjunction with a third party's telecommunication system (which will likely involve access to 'computers' owned by the third party) to effect telecommunication between those servers. Since the third party's computers are interposed whenever the servers communicate with each other, could the third party be said to be 'entitled' to control access between servers? To complicate matters further, section 3 can be used for non-hacking misconduct, so even more difficult problems will arise in trying to determine when such conduct is 'unauthorised'. The problems will be considered in detail in Part III of this article.[51]

It is therefore necessary to first determine what is meant by the term 'entitled' so that we can identify the Entitled Person in relation to a particular program or item of data. Although the term 'entitled' is not expressed to be restricted to legal rights, it is assumed for the purposes of this article that the 'entitlement' must be based on some legal right.[52] The problem is that no single enforceable legal right to "control access to a program or data held in a computer" can be identified in either the law of Singapore or the UK which is completely appropriate for our purposes.[53]

[51] See the main text accompanying notes 184 to 186, 195 and 200, *infra*.

[52] Non-legal rights (for instance, moral 'entitlements') would, it is submitted, be too uncertain and incoherent to be applied by the courts as a basis for determining criminal liability.

[53] Some legal rights that at first sight might appear capable of being the subject of this 'entitlement' prove on closer examination to be quite inappropriate to deal with all possible cases of misuse to which s 3 might apply. They are:

(i) *Ownership of Copyright*

The terms of S 2(5) refer to access to computer programs and data, which are essentially 'information' so intellectual property rights, and in particular, copyright appears a suitable source of this 'entitlement'. Using a computer to obtain access to data or a program in a computer would almost certainly result in that program or data, or a part of that program or data, being copied into the random access memory of the computer so a person who does not have permission from the copyright owner to run a program or obtain access to data infringes copyright in that program or data (see ss 31, 26, 10 and 17 of the Copyright Act Cap 63, 1988 Ed). Thus, copyright could be said to entitle the copyright owner to control access to programs or data.

Problems arising with this argument are firstly, that copyright does not subsist in all computer programs or items of data; it subsists only in an author's expression. Thus, bare facts do not attract copyright. Even where copyright subsists in a work, it lapses after a period of

It may therefore be concluded that the concept of the Entitled Person is a flexible one and depends on the particular circumstances of the case under consideration. The terms of the explanation in section 2(5) provide little assistance in identifying him beyond leading us to this conclusion, and requiring that he be the holder of some legal right which allows him

time defined by the Act (see s 28 of the Copyright Act). Thus, if copyright were the source of the entitlement, there would be no Entitled Person for a signficant volume of material and access to that material could never be 'authorised' (see the discussion in the main text accompanying note 50, *supra*).

A practical difficulty arises where a computer contains several different programs or items of data and the copyright in each is owned by a different person. Each of the copyright-owners is then entitled to 'control access' to his own program, so there would be several Entitled Persons in relation to the 'contents of that computer' taken as a whole. S 3(3) (which reads "for the purposes of [s 3], it is immaterial that the act in question is not directed at ... any particular program or data") suggests that in such a case, 'authority' to have access to its contents depends on having the consent of *all* the different copyright owners, which is hardly sensible.

Another practical objection is that this interpretation of 'entitlement' would attach serious criminal penalties to relatively trivial breaches of copyright. Use of a computer program without the consent of its copyright owner would automatically mean commission of the s 3 offence. Even licensed users of a computer program could commit this offence if they breached any term of a licence which provided that such breach would lead to its automatic cancellation and the user thereafter ran the program. Copyright-owners are already conferred significant rights of enforcement under Part V of the Copyright Act including limited rights under s 136 to invoke criminal law sanctions for serious infringements. Interpreting 'entitlement' in the Computer Misuse Act to mean copyright would effectively criminalise *all* infringement of copyright in computer programs, including relatively minor infringements which the Copyright Act itself does not punish with criminal sanctions. It is therefore submitted that s 2(5) cannot be interpreted as referring to ownership of copyright in that program or data as the source of the 'entitlement' to control access to a program or data.

(ii) *Contract*

Since the principal concern of the English Law Commission was the protection of on-line computer systems from remote hackers, the English equivalent of s 2(5)(a) was probably drafted with the provider of a conventional computer system (or his agent, the system operator) in mind as the Entitled Person. The terms of s 2(5) could arguably permit a contractual basis for the system provider's 'entitlement' to control access.

A contractual relationship would in most cases quite easily be found between subscribers to a bulletin board and the system provider (and perhaps between subscribers *inter se*, applying the principle in *Clarke* v *Dunraven* [1897] AC 59). The terms of this contract would include the rules governing the use of the bulletin board. In the case of a network used by employees of a large organisation, the relationship between network provider and users would still be contractual; employers would be entitled to control employees' access by virtue of their power to give directions to employees under their contracts of employment. In either case, the system provider would give his consent to users to have access to the system pursuant to that contractual relationship with the user. A person who was not a party to such a contractual arrangement would not have consent from the system provider and access by him would thus be 'unauthorised'. If this is the case, the scope of any consent given by the system provider should be clearly spelled out since the s 3 offence would also be committed by authorised users who sought access beyond the scope of their consent.

to exercise some control over the use of the target computer. Ultimately, it will have to be left to the courts to develop rules for determining when access is authorised. The analysis is likely to proceed on the basis of practical and policy considerations and in particular, the mischief that section 3 was intended to deal with.

As pointed out at note 49, *supra*, consent can be specific to a particular person, type and duration of access. Difficult practical problems can arise in determining the scope of consent where the agreement governing use of the network is not sufficiently clear, so it is important that such agreements set out the scope of the consent to access in sufficient detail.

The law of contract is not entirely satisfactory as the source of the entitlement under s 2(5). One problem is raised by the doctrine of privity of contract. Contractual obligations afflict only persons who are parties to that contract. A hacker who is an outsider to a network or non-subscriber to a bulletin board would necessarily not be party to a contract with the system provider. The law of contract thus cannot explain the system provider's 'entitlement' to refuse access to the hacker who does not have a contractual relationship with him. It is submitted that this is not a fatal objection; the concept of 'entitlement' is used only to designate the source of 'authority' to obtain access to the contents of the network or bulletin board server. S 2(5) does not require that the right which serves as the source of this 'entitlement' to control access be enforceable against all potential offenders.

A more serious practical problem is that this interpretation places a very powerful weapon in the hands of system providers to enforce users' obligations under their respective agreements. The argument is similar to that raised in relation to copyright earlier in this footnote; if the consent given to subscribers is defined very narrowly, subscribers would commit the s 3 offence by using the system in a way that is expressly or impliedly prohibited by that agreement. System providers could use the threat of prosecution under s 3 as a means of enforcing their contract with the user. Notwithstanding this problem, it is submitted that the contractual analysis remains the most appropriate for identifying authorisation to have access to on-line conventional computer systems, given the nature of the explanation in s 2(5).

Even so, the appropriateness of contract law as a source of this 'entitlement' is limited to conventional computer systems. In the case of stand-alone computers, this contractual analysis is inapplicable. The appropriateness of contract law to determine the Entitled Person in relation to a network of other electronic processing devices should be considered in the light of the discussion in the main text accompanying notes 186 and 195, *infra*.

(iii) *Ownership of the computer or medium of storage*

There are a number of problems in using ownership of the physical device as the source of the entitlement to control access to its contents. First, s 2(5) clearly refers only to an entitlement to control access to the contents of the computer, rather than to the physical device in which those contents are stored. Secondly, argument could be made that a proprietary interest in the computer or storage medium does not translate into an 'entitlement to control access' to the contents of that device since an act that leads to 'obtaining access' need not necessarily involve any direct physical interference with the device. It is not at all clear whether, under existing rules of tort law, an action for trespass or conversion would lie in the owner of a computer or storage medium against a hacker who obtained access to the contents of that computer or storage medium from a remote location without actually physically interfering with the device. And unless there was some physical damage, destruction or diminution in value or utility of the computer, the criminal offence of mischief under s 425 of the Penal Code, Cap 224 cannot be made out.

In spite of these difficulties, it is submitted that there is no other legal right which is less

With this singularly unhelpful explanation of 'authority', the test of 'authority' to have access to a conventional computer system is probably no different than if there had been no statutory explanation of the term.[54] The provider of the network or bulletin board is likely to be the Entitled Person; so access is only authorised if it is with his consent. In relation to a stand-alone conventional computer, the position is less clear, but access is probably authorised only where it is with the consent of the owner or person having legal possession of the device.[55] Where circumstances are such that other parties have a greater interest in the protection of the integrity of the contents of that computer, it is possible that the consent of such persons is also required, and much will depend on the exact circumstances of a case. An illustration of a situation calling for further analysis is where the owner of a conventional computer uses that computer to provide facilities management services to third parties.[56] In such a situation, determination of who has the greatest interest in the integrity of the programs and data and rights of access to it is not straightforward and must involve reference to the contractual arrangements regulating the relationships between the parties.

Identification of the Entitled Person in relation to other electronic processing devices, whether they operate on their own or as part of networks, is more difficult. The determination would depend on factual considerations such as the nature of the device, the function it performs and other practical and policy considerations. Some illustrations of the difficulty in determining whether access to such devices is authorised will be dealt with later in this article.[57]

(d) *Consent of the entitled person to access*

Once the Entitled Person can be identified, determining whether an occasion of access is authorised is a simple matter of asking whether the Entitled Person consented to that access. Practical difficulties could arise

inappropriate for determining whether access to the contents of a conventional stand-alone computer (*ie*, one that is not connected to a computer system) is authorised.

54 Described in the main text accompanying notes 45 and 46, *supra*.

55 *Supra*, note 53.

56 The term 'facilities management' is sometimes used to describe a situation where an organization contracts with a third party for the third party to provide information technology services required by that organization. A simple illustration could involve an organization which has data processing needs but does not wish to perform those operations in-house; it therefore engages a computer bureau to process the data. The practice, and some security-related and other matters raised by facilities management are set out in an article by Michael Dempsey in the Financial Times of 20 July 1993. Legal aspects of this topic are considered in Nimmer, *The Law of Computer Technology* (2nd ed, 1992), Ch 9 Pt C.

57 *Infra*, main text accompanying notes 184 to 186, 195 and 200.

where the Entitled Person gives express consent to an occasion of access but that consent is couched in ambiguous terms, or where the consent is not express but implied from words or conduct. It will then be a matter of interpretation whether that consent covered that occasion of access.

These difficulties are extremely likely to arise in relation to other electronic processing devices (assuming the Entitled Person can be found). As will be seen from the discussion in Part III of this article,[58] access to the contents of such devices is merely an incident of the normal use of that device, with little thought being given to the fact that 'access' is being had to the contents of a 'computer'. Any consent to access to the program or data contained in such a device will necessarily be implied rather than expressed – it would need to be deduced from some broader permission to use the device (which may itself be only implied from the circumstances or from industry practice related to the device). Finding authority, and even where that is possible, going on to determine the exact scope of that authority will give rise to some legal and factual uncertainty until clear principles can be laid down by case law.

(iii) *The knowledge element*

The term 'knowingly' in a criminal provision such as this denotes a need for subjective knowledge in a potential offender of the facts giving rise to the offence.[59] In section 3, the word 'knowingly' clearly applies to the following:

(i) the offender's acts cause a device to perform a 'function'; and

(ii) that device is a 'computer'.

It is also necessary that the offender know that a likely result of his physical acts is that he will obtain 'access' to a program or data held within a computer.[60] The drafting of this section is less clear than its UK equivalent on the question of whether the offender must know that his access is unauthorised, but given that these offences are closely modelled on their

[58] *Ibid*.

[59] See, for instance *Wolfgang Pzetzhold* v *Public Prosecutor* [1970] 2 MLJ 195 at 197; *Burton* v *Bevan* [1908] 2 Ch 240 at 246, 247; *R* v *Hallam* [1957] 1 All ER 665 at 665.

[60] As pointed out in the main text accompanying note 35, *supra*, it is not clear if the word 'knowingly' as used in s 3 is intended to qualify the phrase "for the purpose of securing access without authority". It is, however, implicit in the use of the word 'purpose' that a potential offender must know that the probable result of his acts is that he will obtain 'access', *supra*, the main text accompanying note 41.

UK equivalents,[61] and seeing that the question of 'authority' to have access is central to the offence, there can be little doubt that an offender must also subjectively know at the time of the offence that the impugned access is unauthorised.

Thus, no offence can be established if the potential offender does not subjectively know of any one of the above facts at the time he performs the physical act element. A difficulty arises at this stage because critical terms used in defining the offence such as 'computer', 'function', 'access' and 'authority' are the subject of arcane technical definitions in the Act which differ significantly from the layman's understanding of what those words mean. The role of these definitions in determining what specific knowledge an offender must possess deserves further consideration.

(a) *'Computer'*

As was pointed out earlier,[62] the definition of the term 'computer' is so wide that it includes other electronic processing devices – that is, devices that would not ordinarily be considered to be 'computers' by laymen. It is thus possible for a person to operate an electronic processing device without subjectively appreciating that it is a 'computer' as that term is defined in the Act. Could a person who did not realise that the device he was operating was a 'computer' under the Act be said to have 'knowingly' caused a 'computer' to perform a function since he did not subjectively consider the device to be such? If the answer to this question was 'no', it would be extremely difficult use the section 3 offence in relation to other electronic processing devices.

It is submitted that a potential offender's subjective failure to appreciate that he is dealing with a 'computer' should not be relevant to satisfaction of this element. The section 3 offence does not require that the offender subjectively consider the device he operates to be a 'computer'. That term carries a technical, defined meaning to denote the devices whose misuse constituted offences under the Act. Lack of knowledge that a particular device falls within a term used in the Act is nothing more than ignorance of the law which is irrelevant to establishing whether the offence was committed 'knowingly'.[63]

[61] The words of s 1(1)(c) of the UK Act very clearly implement the recommendation of the Law Commissioners that the offence could only be committed where the offender knew at the time of the offence that the access which amounted to the offence was unauthorised; see the Report of the Law Commission, *supra,* note 12, at para 3.33.

[62] See main text accompanying notes 24 to 27, *supra*.

[63] *Grant* v *Borg* [1982] 2 All ER 257. At page 263, Lord Bridge said "the principle that ignorance of the law is no defence in crime is so fundamental that to construe the word 'knowingly'

That still leaves unanswered the question of what exactly the potential offender must know about the device which he operates (or causes to be operated) in order to satisfy this requirement. It is submitted that the potential offender must subjectively appreciate that the device has some 'computer-like' capability.[64] It is not necessary that he knows of the internal workings of that device, nor that he believes it to be a computer in the ordinary sense of the word or appreciate the breadth of the definition in the Act. All that is needed is that he be aware that the device's operation involves some type of 'computer-like' as opposed to purely mechanical implementation.

In practice, proving knowledge in the potential offender that he was dealing with a device with 'computer-like capability' should seldom ever give rise to difficulties. The devices in relation to which this provision is likely to be used such as conventional computers and ATMs are clearly devices having 'computer-like capability' and ordinary persons using them (or causing them to be used) would be presumed to be aware of this. It is thus likely that prosecutions on charges involving such devices would not require specific evidence that the potential offender had the necessary knowledge since a court could infer this from the circumstances. It would only be where the device were of a type which most people would not associate with electronic or other data processing operations that specific proof of this knowledge would be required.

Even in a normal case, where a court is prepared to infer knowledge in the potential offender that the device in question was a 'computer', it would be open to the accused to raise a defence under section 79 of the Penal Code which reads:

> Nothing is an offence[65] which is done by any person ... who by reason of a mistake of fact and not by reason of a mistake of law in good faith believes himself to be justified by law in doing it.

in a criminal statute as requiring not merely knowledge of the facts material to the offender's guilt, but also knowledge of the relevant law, would be revolutionary and, to my mind, wholly unacceptable." Note that the issue of 'knowledge' arises in relation to matters which a prosecution must prove to establish a *prima facie* case that an offence has been committed. It is thus distinct from the question of whether mistake or ignorance of the law affords a defence. S 79 of the Penal Code provides that mistake may be a defence to liability, and will be discussed separately in the main text accompanying notes 65 to 67, *infra*. That discussion is premised on a *prima facie* case of liability first having been established in relation to the accused person (*ie*, that all the elements of the offence, including this aspect of the mental element are proved).

64 This deliberately vague phrase will be employed for the present to indicate that some degree of subjective knowledge is required that the device has some electronic (or other) processing capability, without necessarily involving subjective knowledge of the particular electronic (or other) operations involved.

65 The explanation of this term 'offence' in s 40(2) of the Penal Code makes it clear that this

Thus, proof that the potential offender acted under a mistaken belief of fact that he was operating something other than a 'computer' would excuse the offence. Section 79 operates as a defence to liability; so the burden of proving the defence lies on the accused person[66] (though this burden only arises after the prosecution has proved all the elements of the offence to the criminal standard, *ie*, beyond reasonable doubt). This defence imports the intensely difficult legal distinction between errors of law and errors of fact. Clear examples of errors of fact that would excuse an offence are where the potential offender manipulated the controls of a computer believing that the computer did not work, or that the computer was not connected to a power source, or under a mistaken impression that the device was purely mechanical (and thus lacked data processing capability). On the other hand, a misapprehension that section 3 did not extend to a particular electronic processing device or complete ignorance of the existence of the Act would not afford a defence.[67]

(b) *Function*

The term 'function' gives rise to a slightly different problem. The definition of this term[68] is only meaningful when one understands something of the way computers work. There are probably many people for whom this will not be the case. Persons who happily operate a computer without understanding (or ever trying to understand) its internal processes may be said to lack subjective 'knowledge' that their acts cause the computer to perform 'functions'. Again, the argument might be made that a person who lacks the technical knowledge to subjectively appreciate the processes described in section 2(1) of the Act cannot commit the section 3 offence.

It is submitted that the particular knowledge which section 3 requires a potential offender to have is not knowledge of the matters set out in the statutory definition of 'function' in section 2(1). All that the prosecution should be required to prove is that the potential offender subjectively knew that his acts would lead to the computer being operated *qua* computer (that

particular exception extends to all other criminal offences, including those created by statutes other than the Penal Code such as ss 3 to 7 of the Computer Misuse Act.

66 S 107 of the Evidence Act, Cap 97 (1990 Rev Ed).

67 This corresponds to the common law maxim *ignorantia juris non excusat* which was adverted to at note 63, *supra*, and accompanying main text. It is not clear whether that common law maxim applies in Singapore. Although that maxim was accepted to be part of the law of Singapore by the Privy Council in the case of *Public Prosecutor* v *Koo Cheh Yew & anor* [1980] 2 MLJ 235, there remains some doubt whether that decision is correct since s 79 of the Penal Code covers very much the same ground; see Koh, Clarkson & Morgan *Criminal Law in Singapore and Malaysia; Text and Materials* (1989), at 176 *et seq*.

68 Set out at note 36, *supra*.

is, as an electronic or other data processing device). This formulation requires us to give less than full effect to the definition of 'function' in section 2(1), but it is submitted that such a reading is necessary in this context. If the statutory definition of 'function' meant otherwise – and if section 3 required proof that a potential offender was sufficiently computer-literate to appreciate how his acts led to "logical, control, arithmetic, deletion, storage or other similarly technical operations within the computer"[69] – it might pose an impossible burden for any prosecution where the accused person cannot be proved to have had formal training in a relevant area of computer technology.

Some support for this position may be derived from the fact that the UK Act, unlike ours, does not contain a definition of the term 'function'. The definition in our Act is (together with section 6 of the Act) drawn from Canadian legislation which adopted a significantly different approach to defining offences of computer misuse than did the UK Act.[70] The inappropriateness of this definition in assisting our interpretation of the knowledge element of the section 3 offence is thus easily understood, and we may conclude that the context of section 3 requires us to disregard that definition.[71] So long as there is appreciation in the potential offender that his acts would cause the device to operate in the manner of a data or other processing device, this part of the knowledge element should be satisfied.

(c) *'Access'*

Section 3 does not expressly require that an accused person know that his acts will lead to 'access' or that this access is unauthorised; it provides only that the purpose of the physical act should be to secure unauthorised access. While having a 'purpose' is not the same as having subjective knowledge, it was explained earlier[72] that the potential offender can only have 'unauthorised access' as his purpose where he has subjective knowledge that 'access' is a likely result of his acts and that the access is unauthorised. This requirement for subjective knowledge of 'access' raises a similar difficulty as the term 'computer' which was discussed earlier.[73] It could be argued that a person who is not computer-literate may realise that his acts will likely lead to some kind of 'use' of a computer, but will not actually

69 S 2(1).

70 *Infra*, main text accompanying notes 137 and 138.

71 S 2(1) introduces the definitions used in the Act with the words: "In this Act, unless the context otherwise requires...." A strong argument can be made that the context of the knowledge element of the s 3 offence requires that this definition of 'function' not apply.

72 See the main text accompanying notes 41 and 43, *supra*.

73 See the main text accompanying notes 62 to 67, *supra*.

know that this will fall within the terms of the technical definition of 'access'. It is submitted that for the reasons set out earlier in relation to the term 'computer',[74] it is not necessary for the potential offender to appreciate how his acts fall within the definition of 'access' since that would be nothing more than ignorance of the law. It is enough that he subjectively appreciates that some use of a computer *qua* computer is a likely result of his physical acts.

(d) *'Authority'*

In the classic case of hacking, where a hacker obtains access by deliberately circumventing security systems or using a password which was not issued to him, it is unlikely to be necessary for a prosecution to present evidence that the potential offender knew that he lacked authority. A court would readily infer from such circumstances that the hacker was aware that he was not supposed to gain access to the computer system either at the time he (or she) first sallied forth into cyberspace, or at the latest, when he was challenged by some security feature of the computer system to which he sought access.

Outside the classic hacking situation, a requirement that the potential offender know at the time of access that he lacked authority to have that access is capable of giving rise to some uncertainty, in particular:

(1) where the potential offender was unaware that consent must be obtained before obtaining access to the contents of a computer in any circumstances or in relation to a particular computer; and

(2) where the potential offender mistakenly believed that he was the Entitled Person or that he had consent from the Entitled Person (which, given the inadequacy of the statutory explanation of authority in section 2(5) of the Act[75] may not be an uncommon occurrence).

No legal difficulty is presented by the situation where a person gets unauthorised access to the contents of a computer under a mistaken belief that no authorisation was necessary because he is unaware of the existence of the Act. Such an error would be little more than common garden-variety ignorance of the law, so normal criminal law principles indicate that he would not be excused from criminal liability.[76] Similarly, if the potential

[74] *Ibid.*

[75] S 2(5) is set out in the main text accompanying note 48, *supra*, and the difficulty in interpreting that provision is described in the main text accompanying notes 48 to 57, *supra*.

[76] The reasoning is set out at the main text accompanying notes 65 to 67, *supra*.

offender was unaware that the device he was dealing with was a 'computer' under the Act or that he would commit an offence unless he had consent of the Entitled Person to his having access to its contents, his mistake of law would not excuse liability under section 3.[77]

It is not as easy to tell whether a mistaken belief in a potential offender that he is the Entitled Person, or that he has consent to access from a person whom he wrongly believes is the Entitled Person, is a mistake of law or of fact. The mistake is one relating to the factual existence or non-existence of a legal status and is therefore not easily classified as either. It is submitted that it does not matter either way. If a mistaken belief relating to authority is a mistake of fact, Section 79 of the Penal Code will apply to exculpate liability. If it is a mistake of law, it falls under an exception to the principle that a mistake of law will not be relevant to whether an offence was committed 'knowingly', being an offence defined by reference to knowledge of the lack of some legal right.[78]

Illustrations of these types of exceptional offences where a mistaken belief relating to a legal right negatived criminal liability are to be found in the English cases of *R* v *Smith (David)*,[79] and *Secretary of State for Trade and Industry* v *Hart*.[80] In the former, it was held that a charge of causing criminal damage to property belonging to another could not be sustained where the accused person mistakenly believed that the property in question belonged to him. The charge here was brought under section 1(1) of the UK Criminal Damage Act 1971 which defined the offence as follows:

> A person who without lawful excuse destroys or damages any property belonging to another intending to destroy or damage such property or being reckless as to whether any such property would be destroyed or damaged, shall be guilty of an offence.[81]

[77] *Ibid.*

[78] The English Law Commission was also of the view that a mistake as to authority would negative any offence without considering this exception to the principle on mistakes of law, *supra*, note 12, at para 3.36 and 3.37.

[79] [1974] QB 354.

[80] [1982] 1 All ER 817.

[81] It is worth noting that the phrase 'without lawful excuse' in this provision is explained in s 5(2) of that Act as follows: "A person charged with an offence [under s 1(1)] shall ... be treated ... as having a lawful excuse – (a) if at the time of the act or acts alleged to constitute the offence he believed that the person or persons whom he believed to be entitled to consent to the destruction of or damage to the property in question had so consented..." The terms used in this explanation are not dissimilar to those used in s 2(5) of the Computer Misuse Act (set out in the main text accompanying note 48, *supra*) to explain the concept of 'authority' to have access to a program or data.

The intentional conduct at which that offence is directed is the destruction or damage of "property belonging to another"; the mental element of this offence is clearly defined by reference to the legal concept of ownership of the property destroyed. A mistake in relation to this legal concept was held to affect the satisfaction of the mental element under that provision.

In the case of *Hart,*[82] a person charged with knowingly acting as a company auditor while disqualified was found to have a good defence where he did not actually realise that he was disqualified, even though his state of disqualification was a matter of law. The criminal proceedings here were brought under section 13(5) of the UK Companies Act 1976 which reads:

> No person shall act as auditor of a company at a time when he knows that he is disqualified for appointment to that office...

The offence thus defined, knowledge of disqualification (a legal concept) was also found to be critical if the mental element of the offence was to be made out, notwithstanding that it related to a matter of law.[83]

The concept of 'authority' is, like ownership of property or disqualification to be a director, based on a legal concept (albeit a vague and imprecisely-defined one). Knowledge in a potential offender that he lacks 'authorisation' to have access is thus an essential part of the mental element of this provision, and if he believes otherwise as a result of a mistake of law, then the offence cannot be made out.[84]

(iv) *Summary*

In straightforward hacking cases, the section 3 offence would be easily made out because its physical act and purpose elements are extremely widely drafted and thus easily satisfied. The knowledge element is considerably more difficult to understand, but it is submitted that what needs to be proved is relatively simple: that a potential offender knows at the time of the offence that he operated (or caused to be operated) a device having some processing capability[85] as such. He must also know that this operation was 'unauthorised'

[82] *Supra*, note 80.

[83] Unlike the court in *R* v *Smith (David),* the Court of Appeal in this case considered lack of knowledge as a defence to the charge rather than as negativing an element of the offence. That does not affect the applicability of the reasoning in *Hart* to the problem at hand.

[84] But note that this is to be distinguished from the situation where the potential offender does not know of his want of authorisation because of complete ignorance of the Act, or ignorance of the fact that his conduct falls within the Act. Similarly, recklessness or disregard of the question of authority will not excuse the offence; it is only where the potential offender works on an honest but mistaken misapprehension that his access was authorised that he will fall within this special class of cases.

[85] These phrases are deliberately vague since it is the technical nature of the definitions that

and will not be liable under the offence where he honestly but wrongly believes that his access is 'authorised'. Non-hacking situations are capable of giving rise to great difficulty in interpreting the unsatisfactory definition of the concept of 'authority', which is central to the offence.

2. *Section 4 – unauthorised access with intent to commit or facilitate further offences*

Section 4(1) of the Act provides:

> Any person who causes a computer to perform any function for the purpose of securing access without authority to any program or data held in any computer with intent to commit an offence to which this section applies shall be guilty of an offence...

This provision corresponds to section 2 of the UK Act. Like its UK counterpart, it provides for a distinct offence with enhanced punishment[86] where the unauthorised access offence is committed in order to facilitate the commission of some further offence, defined in section 4(2) as one "involving property, fraud, dishonesty or which causes bodily harm punishable on conviction with imprisonment for a term of 2 years or more." This further offence will be referred to as the 'ulterior offence'.[87]

The section 4 offence is defined in terms similar to those used in section 3; indeed, the physical act element of this offence and a purpose element of this provision are identical to the corresponding elements of the section 3 offence so nothing further will be said about those elements here.[88] The critical difference between sections 3 and 4 lies in the mental element;

can complicate our understanding of what the knowledge element entails; see the main text accompanying notes 64, 69 and 74, *supra*.

86 The punishment prescribed in s 4(1) is a fine of up to $50,000 or imprisonment up to 10 years or both; *cf* s 3(1) where the basic punishment is a fine not exceeding $2,000 or imprisonment for up to two years or both, while an offence accompanied by serious damage is punishable with a fine not exceeding $20,000 or imprisonment for up to 5 years or both.

87 The requirement for an ulterior offence is discussed at notes 89 to 101, *infra*, and accompanying main text.

88 These are discussed in relation to s 3 in the main text accompanying notes 36 to 58. That discussion is also relevant in determining the elements of the s 4 offence.
The use in s 4 of the word "purpose" in relation to the words "securing access without authority" to the contents of a computer means that the potential offender must also subjectively know that his acts are likely to lead him to have 'access' to the contents of a computer, and that this access is unauthorised. The discussion of this knowledge requirement in relation to s 3 (*supra*, notes 72 to 84 and accompanying main text) is thus also relevant to the interpretation of s 4 even though the words of this provision do not carry an express knowledge requirement.

section 3 only requires that the physical act be performed 'knowingly', while section 4 imports as the mental element the intention to commit the ulterior offence.

(i) *The ulterior offences*

Section 4(2) defines the ulterior offences to which section 4 applies by reference to two conjunctive requirements; first, the offence must be one involving "property, fraud, dishonesty or which causes bodily harm";[89] and secondly, the offence must be "punishable on conviction with imprisonment for a term of 2 years or more".[90]

The English Law Commission Report set out some examples of the types of crimes that section 4 might deal with. They included theft by hacking into a bank's computer system to remove or transfer funds,[91] hacking to obtain confidential and personal information for blackmail,[92] and hacking to cause physical injury to persons (for instance, by hacking into a hospital's computer system and rearranging data such as blood group or treatment records in order to cause harm to a patient).[93]

Section 4 of the Act should cover most of these situations, since the definition of the ulterior offence covers the Penal Code offences of theft,[94]

[89] The terms of the definition in s 4(2) are set out at the main text accompanying note 87, *supra*. The UK equivalent is not restricted to particular types of offences and it is not clear why it was felt necessary to introduce this requirement in the Singapore Act. It may be that this provision merely states the obvious; one cannot easily imagine computers being used to facilitate the commission of offences other than those having this character. Even so, this limitation on the application of s 4 seems somewhat inconsistent with the trend in the drafting of this Act to provide for unforeseen developments, even at the expense of certainty or ease of interpretation.

[90] The phrasing of this second requirement opens it to the argument that it applies only to ulterior offences involving the causing of bodily harm, and that there is no such requirement for offences involving property, fraud or dishonesty. This argument is supported by the lack of a comma after the word 'harm'. This article will nevertheless proceed on the assumption that the qualification that the offence be of a certain seriousness (as to be punishable with at least two years' imprisonment) applies to all the types of offences listed in s 4(2) since there can be no good reason for restricting the application of s 4 to ulterior offences involving bodily injury but not so qualifying the other types of offences to which it may apply.

[91] See para 3.52 of The English Law Commission Report, *supra*, note 12. An illustration of such theft can be found in the English case, *R* v *Thompson* [1984] 1 WLR 962, which also illustrates some of the difficulties faced by a prosecution in trying to bring a new situation created by computer technology within the terms of an offence whose drafting pre-dated the technology.

[92] *Supra*, note 12, at para 3.53

[93] *Ibid*, at para 3.55.

[94] S 378 read with s 379 of the Penal Code.

extortion,[95] aggravated cheating,[96] culpable homicide not amounting to murder,[97] causing grievous hurt[98] and causing hurt by means of poison.[99]

Offences which, interestingly, cannot be ulterior offences for the purpose of bringing a charge under section 4 are cheating and the basic offence of causing hurt; both of these offences carry punishments of up to one year's imprisonment only.[100] The omission of simple cheating as a possible ulterior offence is unfortunate since some relatively serious computer-related misconduct (including one considered by the English Law Commission) may not easily be brought within the terms of other Penal Code offences to which section 4 applies.[101]

(ii) *'Intent to commit' the ulterior offence*

The meaning of the term 'intent' or 'intention' as it is used in the Penal Code and other criminal statutes in Singapore has given rise to some uncertainty. This is the subject of academic consideration elsewhere[102] so no discussion will be devoted to it here. It is only necessary to point out that the section 4 offence requires an 'intent to commit' the ulterior offence, which is not to be confused with the mental element of that ulterior offence. The mental element of that ulterior offence will depend on the terms by which the offence is drafted. Merely having that state of mind will not of itself satisfy the mental element required by section 4. The 'intent to commit' the ulterior offence requires that a potential offender intends to perform conduct that satisfies *all* the elements of that ulterior offence – mental and physical – at the time he causes a computer to perform a function.

The definition of the section 4 offence by reference to an ulterior offence under the general body of criminal law prevents this provision from fully

[95] *Ibid*, s 383 read with s 384. Computer-related extortion might occur where a hacker threatened to enter the victim's computer system and delete data or otherwise disrupt the victim's computer-based operations.

[96] Offences of cheating a person whose interest the offender is bound to protect (s 415 read with s 418 of the Penal Code), cheating by personation (ss 415 and 416 read with s 419) and cheating and dishonestly inducing to deliver property (s 415 read with s 420) fall within the description of the ulterior offence in s 4 of the Computer Misuse Act, but the offence of basic cheating slips through the net; see the main text accompanying note 100, *infra*.

[97] Ss 299 and 300 of the Penal Code read with s 304.

[98] *Ibid*, ss 319, 320 and 322 read with s 325.

[99] *Ibid*, ss 319 and 321 read with s 328.

[100] *Ibid*, s 415 read with s 417 and ss 319, 321 and 323 respectively.

[101] The offence of hacking into a bank's computer system to transfer funds provides an illustration of such a difficulty. This is explained in the main text accompanying notes 104 to 110, *supra*.

[102] See Koh, Clarkson & Morgan *Criminal Law in Singapore and Malaysia; Text and Materials* (1989), at 56 *et seq*.

achieving the objective of overcoming difficulties in applying the old laws to new technology-related misconduct. It was partly the inadequacy of the pre-Act rules of law in dealing with misconduct involving the new technology that led to the Act;[103] hence this approach to defining the section 4 offence is self-defeating.

Take for instance, the application of section 4 to a situation contemplated by the English Law Commission; a hacker who uses a computer to get unauthorised access to records of his account with that bank. He amends files so that his once negligible bank balance now shows a credit of several million dollars in his favour. Would he have satisfied the mental element of the section 4 offence? That depends on what the ulterior offence is. The obvious ulterior offence is theft under section 378 of the Penal Code, which is punishable by up to three years' imprisonment.[104] In order to show the potential offender 'intended to commit' theft, it must be shown that he intended to do all things required by section 378 of the Penal Code to constitute the offence; that is, he must have intended to move some movable property in the bank's possession without the bank's consent, intending thereby to take the property dishonestly out of the possession of the bank.

This is possible[105] where it is necessary for the potential offender to withdraw the 'stolen' money in cash since that would require him to handle movable property (the cash) in the bank's possession. But with cashless transactions reasonably common, it may be unnecessary for our hypothetical offender to withdraw his ill-gotten gains as cash. He might perhaps have the account balance in the victim bank transferred to another bank; that would not involve his moving any movable property which was in the bank's possession so the section 4 offence could not be made out. Or he could have this amended credit balance set off against amounts already owing by him to the bank, or apply the credit balance towards electronic share applications or payments by GIRO. If our hypothetical offender can prove that his intention at the time he satisfied the physical act element was not to obtain cash but to use appropriate cashless means to draw down this bank balance, then the mental element of section 4 cannot possibly be satisfied. The potential offender's intent in effecting the funds transfer could not then be said to have been the commission of the offence of 'theft'.

In these premises, successful prosecution of the offender under section 4 would require us to cast further afield for suitable ulterior offences – perhaps forgery for the purpose of cheating[106] or falsification

[103] *Supra*, main text accompanying notes 7 to 10.

[104] S 378 read with s 379 of the Penal Code.

[105] Though proof of this intention will pose distinct practical problems.

[106] S 468 of the Penal Code. It is actually not altogether clear that the purpose of the conduct in this hypothetical is 'cheating' as defined in s 415, since that definition requires that a person be deceived. Directly altering a bank balance in a computer record will not amount

of accounts.[107] Establishing forgery for the purpose of cheating as the ulterior offence would require exactly the kind of mental gymnastics that the Act was meant to avoid,[108] while a charge of falsification of accounts would only be available in certain restricted circumstances,[109] so the section 4 offence would not, in these circumstances, help us to overcome the difficulties involved in proceeding under "general laws [contained in the Penal Code] because of the special nature of computer technology".[110]

to cheating since it is unlikely that any person would have been deceived in the process. But so long as any use of the funds represented by this altered bank balance requires some employee of the victim bank ultimately to act in reliance of that altered bank balance (for instance, a teller of the victim bank is asked to effect the transfer of funds from that account to another account) which he would not have done but for the alteration to the bank balance, the offence of cheating may be made out.

[107] S 477A of the Penal Code.

[108] S 463 of the Penal Code defines the offence of forgery by reference to the making of a "false document or part of a document". The term 'document' is defined in s 29 of the Penal Code as "any matter expressed or described upon any substance by means of letters, figures, or marks, or by more than one of those means, intended to be used, or which may be used, as evidence of that matter." It is not altogether clear that the state of magnetic particles on the surface of a storage medium could comfortably fit within the words "expressed or described by means of letters, figures, or marks, or by more than one of those means...." There is no local case interpreting this provision positively to include electronically stored information.

It has been suggested that an identical definition of the word 'document' in s 3 of the Evidence Act, (Cap 97, 1985 Rev Ed) is wide enough to cover electronically stored information; see TY Chin, *Evidence*, (1988), at 215 and SK Toh, "Computer Crime in Singapore – Should We Legislate", *supra*, note 3, at xxiv. The latter cites in support of this view an English case, *Grant* v *Southwestern & County Properties* [1975] Ch 185. A more recent English case, *Derby & Co Ltd* v *Weldon (No 9)* [1991] 1 WLR 652, also supports the view that data stored in a computer was in a 'document'. It must, however, be borne in mind that these two English cases were not concerned with the interpretation of a statutory definition, let alone a statutory definition similar to those contained in the Evidence Act and Penal Code; they were interpreting the term as it is used (without definition) in the English Rules of the Supreme Court. The approach adopted in those cases is thus not necessarily applicable to the interpretation of particular local statutory definitions.

Even if the reasoning used in the English cases is correct for the purposes of determining the meaning of 'document' in the law of evidence, the same interpretation need not necessarily apply to the term as it is used in a different context – the Penal Code. A definition contained in a penal statute should be interpreted strictly and the context here (the definition of the offence of 'forgery') may be argued to be different enough from the determination of whether to permit discovery of documents (as was the issue in the English cases cited) that a different result is justified.

[109] S 477A only applies to a person who is a "clerk, officer, or servant, or employed or acting in the capacity of a clerk, officer, or servant".

[110] *Supra*, note 4, at col 300.

Even more complex transactions falling into lacunae in the pre-Act criminal law are possible. An illustration is to be found in the English case of *R* v *Thompson*, *supra*, note 91. The accused here had access to a bank computer which stored records of account balances and processed transactions involving those accounts. The accused loaded into that computer

It is not necessary that the ulterior offence actually be committed at the same time as the section 4 offence.[111] Nor is it is necessary for the conduct to amount to an 'attempt' to commit that ulterior offence[112] since section 4 refers only to intention to commit the ulterior offence and not its actual commission or the commission of acts that could amount to an attempt. Section 4 of the Act does not contain the equivalent of sub-section (4) of the UK Act which makes it clear that an offence may be committed even if the ulterior offence is incapable of performance. This probably does not represent a significant difference between our provision and its UK equivalent. The terms of our section 4 do not require that the ulterior offence contemplated be capable of achievement; all that is necessary is that the potential offender intended to commit the offence, whether or not that intention was realizable.

3. *Section 5 – unauthorised modification of computer material*

Section 5 states that "any person who does any act which he knows will cause an unauthorised modification of the contents of any computer shall be guilty of an offence...."

Like the section 3 offence, this provision is clearly based on its UK

a program which effected a transfer of money to his account by automatically debiting other accounts and crediting the accused's account. No human intervention was involved at this stage. The charge against him under s 15 of the UK Theft Act, 1968 (1968, c 60), required the prosecution to show that he had done some act to obtain "ownership, possession or control" of property. The Court of Appeal in that case was not prepared to view the alteration of computerised records as satisfying this ingredient of the charge since the 'acts' were done by a computer rather than the accused. It was only by virtue of the accused's subsequent conduct in writing to the bank later to transfer his ill-gotten gains that the criminal offence was constituted in that case.

[111] S 4(3).

[112] Under s 511 of the Penal Code.

[113] The comparable portions of the UK s 3 read as follows:

(1) A person is guilty of an offence if –
  (a) he does any act which causes an unauthorised modification of the contents of any computer; and
  (b) at the time when he does the act he has the requisite intent and the requisite knowledge.

(2) For the purposes of subsection 1(b) above the requisite intent is an intent to cause a modification of the contents of any computer and by so doing –
  (a) to impair the operation of any computer;
  (b) to prevent or hinder access to any program or data held in any computer; or
  (c) to impair the operation of any such program or the reliability of any such data.
  [subsection (3) omitted.]

(4) For the purposes of subsection (1)(b) above the requisite knowledge is knowledge that any modification he intends to cause is unauthorised.

equivalent though significant changes were made by the local draftsman.[113] Major differences from the UK equivalent will be noted at relevant points in our discussion.

This offence represents a different approach to protecting the integrity of computer systems from that taken in section 3. Because section 3 is directed towards 'unauthorised access' to the contents of computers, some means of compromising the integrity of computer systems might slip through the net where the potential offender needed no 'access' to effect his evil purpose. An illustration is where a person disseminates a computer virus[114] by placing the virus on a floppy disc and then selling or giving that floppy disc to an unwitting victim. The virus would then infect the victim's computer when the victim himself loaded the program. Section 5 provides the means to deal directly with such wrongdoing.

Naturally there is considerable overlap between the offences created by section 3 and section 5. Some scenarios of straightforward hacking (*eg*, modification to data in a network file server by a person who was not authorised to have access to that network, or by a person who had consent to have access but not to make changes to programs or data contained in the server) would constitute offences under both sections. There is little reason to prefer applying one offence over the other since the penalties are exactly the same (including the enhanced penalty where serious damage is caused by the offence)[115] so the availability of the two provisions to deal with that single occasion of misconduct would simply give the prosecution a choice of alternative charges to bring against the offender, and that could be determined by considering which offence was easier to prove under the circumstances. This is to be contrasted with the approach taken in the UK. Under the UK Act, the offence of unauthorised modification is viewed as a much more serious offence than the basic hacking offence, carrying a significantly more severe penalty and is more restrictively defined.[116]

The elements of our section 5 offence are relatively simpler than the section 3 offence so reference will be had to the traditional division of criminal offences into *actus reus* and *mens rea*.

[114] A computer virus is defined thus in H Freedman, *The Computer Glossary* (4th ed, 1989): "A computer virus is a program that is used to infect the operation of a computer system. After the virus code is written, it is buried within an existing program, and once that program is loaded into the computer, the virus replicates by attaching copies of itself to other programs in the system. the purpose of a virus can range from a simple prank that pops up a strange message on the screen out of the blue, to the actual destruction of programs and data that may be set to occur at any time in the future..." Computer viruses are discussed in Chan, "Legal Aspects of Computer Viruses" (1990) 11 Sing LR 15.

[115] S 5(2); *cf* s 3(2).

[116] The UK unauthorised modification offence is punishable with imprisonment for up to five years while the unauthorised access offence attracts imprisonment of up to six months only. The most significant differences between the scope of the Singapore and UK offences are discussed in the main text accompanying notes 124 to 127, *infra*.

(i) *The actus reus*

The *actus reus* of this offence is the doing of "any act which [the offender] knows will cause an unauthorised modification of the contents of any computer". As with the earlier offences, this definition of the proscribed conduct is in the widest of terms and is not limited to acts relating to the direct operation of the target computer by the offender. Such a wide description of the *actus reus* is necessary if the offence is to cover dissemination of a computer virus by way of 'infected' floppy disks.

(a) *'Modification'*

The limit on the types of conduct which can attract liability under this provision is provided by the explanation of the term 'modification' in section 2(7). This states that a 'modification' takes place for the purposes of section 5 if:

> by the operation of any function of the computer concerned or any other computer –
>
> (a) any program or data held in the computer concerned is altered or erased;
>
> (b) any program or data is added to its contents; or
>
> (c) any act which impairs the normal operation of any computer [sic],
>
> and any act which contributes towards causing such a modification shall be regarded as causing it.

This explanation is premised upon the performance by a computer of some 'function', so only modifications to the contents of computers arising from the operation of a computer *qua* computer can fall within section 5.[117] Section 5 thus would not cover conduct such as placing a strong magnet near a hard disk to render its contents unusable since that conduct does not involve operation of the computer's processing capability.[118]

[117] The term 'function' is discussed at note 36, *supra*, and accompanying main text.

[118] The lacuna is not particularly serious since it would be possible that the conduct described may amount to an offence of mischief under s 425 of the Penal Code.

The conduct described in paragraph (a) of section 2(7) also falls within the definition of 'access' in section 2(2).[119] This overlap means that this part of the definition of 'modification' does not actually give section 5 any significance going beyond the section 3 offence. Unauthorised modification as defined in section 2(7)(a) would necessarily amount to unauthorised access as well. For example, the Entitled Person in relation to a server (it is assumed that this is the same person for purposes of access as well as modification) may allow a user to read or copy data or programs in the server only but not to make any changes to those data or programs. Failure to abide by the terms of the consent (by amending or erasing some data or program in the server) would amount to unauthorised access as well as an unauthorised modification.

Paragraph (b), by contrast, goes beyond the definition of access. The term 'access' does not cover the addition of a program or data to the 'contents' of a computer;[120] so an unauthorised modification as defined by section 2(7)(b) is unlikely to give rise to the section 3 offence as well.

(b) *'Contents' of a computer*

Paragraphs (a) and (b) of sub-section 2(7) go beyond stating a common sense understanding of the term 'modification'. The use of the phrase "contents of a computer" as the equivalent of "program or data held in the computer" indicates that the analysis of the section 5 offence centres around changes made to the contents of storage media in the computer concerned. This includes the contents of removable storage media such as

[119] S 2(2) provides *inter alia* that "a person secures access to any program or data held in a computer if...he (a) alters or erases the program or data...." The term 'access' is discussed in the main text accompanying note 43, *supra*.

[120] *Ibid*. The meaning of the phrase 'contents of a computer' is considered in the main text accompanying notes 121 to 123, *infra*.

It may in practice be difficult to distinguish between 'adding' a new program or data to the contents of a computer and merely 'altering' an existing program or data. Computer programs or data files are unlikely to exist in computer storage media as discrete, identifiable 'objects'; a single program or item of data may be stored in diverse physical locations on the storage medium. To complicate things further, a complex computer program may consist of a large number of constituent parts, each of which is capable of being considered a computer program in its own right, and each of which may be similarly distributed among several different locations in the computer. Where a change to that program involves writing in new code on a different physical location without erasing any of the pre-existing code, can that amount to having 'access' to the program, even though the 'program' has clearly been 'altered', or does it amount to addition of a new program to the contents of the computer? This potential practical difficulty may well be a good reason why changes to the contents of a computer are best dealt with by s 5 rather than s 3, the overlap between them notwithstanding.

[121] S 2(6) of the Act.

floppy disks or tapes which are for the time being in a computer.[121]

Although the words of the Act do not make this clear, the English Law Commission[122] felt that the phrase 'contents of a computer' should include a computer's random access memory ('RAM'). It is submitted that this interpretation is less than ideal and would have the effect of rendering our section 3 offence redundant. On this interpretation, merely running a program or having access to data would amount to a 'modification' because that program or data (or part of that program or data) would be 'added to the contents' of the RAM. Even switching on a computer would involve some of the operating system software being copied to the RAM. Thus, such an interpretation of the term 'contents' would make section 5 cover all conceivable situations of 'access'. 'Unauthorised access' would be nothing more than a subset of 'unauthorised modification'.[123] The term 'contents of the computer' should, if our section 3 is to represent a meaningful, distinct offence from the section 5 offence, exclude the RAM and thus be limited to the contents of a non-transient storage medium (*ie,* a storage medium whose contents are not lost when the computer is switched off).

Such a restricted reading of the phrase would not make section 5 less able to deal with the basic mischief that it was directed at. The provision remains wide enough to cover many foreseeable types of computer-related misconduct such as moving files to different directories without altering their contents, or changing a password to stymie a lawful user. These would still be caught by the term 'modification' since non-transient data in a storage medium other than the RAM relating to the organization of data or to passwords would be altered. Disseminating a virus will also be within the ambit of the section 5 offence since viruses operate by causing the 'infected' computer to perform functions and, depending on the type of virus, altering, deleting or augmenting data in a storage medium other than the RAM.

(c) *Section 2(7)(c)*

Of these three limbs, 2(7)(c) is clearly the odd one out. Unlike paragraphs (a) and (b), it was not drawn from the definition of 'modification' in the

[122] *Supra*, note 12, at para 3.67.

[123] This argument would not apply to its UK equivalent since s 3 of the UK Act contains a requirement for specific intent to commit the offence that is much narrower than the intent for the UK unauthorised access offence; compare s 3(2), which is set out at note 113, *supra*, with s 1(1)(a) which is set out at the main text following note 34, *supra*. Because of the specific intent required by s 3 of the UK Act, an offence under s 1 will not automatically amount to an offence under s 3 even if one reads the phrase 'contents of a computer' to include the computer's RAM.

[124] S 17(7) of the UK Act. The words of s 2(7)(c) are actually adapted from s 3(2)(c) of the UK Act, which is part of the definition of the *mens rea* of the offence. The full text of s 3(2) of the UK Act is set out at note 113, *supra.*

UK Act.[124] Section 2(7)(c) also stands out because its terms are ungrammatical when read in the context of the whole of section 2(7), to the point that it is difficult to see what was intended by that limb of the definition.

Section 2(7)(c) refers to "any act which impairs the normal operation" of a computer. It is not clear what was intended by the words "any act" – they may refer to the act of the offender or some other person or might even extend to 'acts' of computers. The words themselves also give no guidance about what was intended to be the relationship between this 'act' and the "operation of any function of the computer" mentioned earlier in that statutory explanation.

It is possible that the draftsman meant to use the words "any event occurs" instead of the unfortunate "any act". If that were the case, section 2(7)(c) would prescribe that a modification takes place where as a result of operation of the computer, "any event occurs which impairs the normal operation of any computer...." Thus phrased, section 2(7)(c) could have been intended as a 'catch-all' provision to deal with situations which fell outside the terms of section 2(7)(a) and (b). Such an interpretation would leave section 2(7)(c) capable of dealing with modification of data in a non-permanent storage medium by the use of a computer; other than that, this writer cannot conceive of any other application of section 2(7)(c) that is not already covered by section 2(7)(a) and (b).

Alternatively, the draftsman may have intended a more drastic change from the UK equivalent. Section 2(7) may have been meant to read:

> a modification of the contents of any computer takes place if –
>
> (a) by the operation of any function of the computer concerned or any other computer –
>
> (i) any program or data held in the computer concerned is altered or erased; or
>
> (ii) any program or data is added to its contents; or
>
> (b) any act is done which impairs the normal operation of any computer...

In this case, the scope of section 5 would be augmented somewhat to include conduct which did not involve operation of the computer *qua* computer.[125] This reading, while possible, would take the application of section 5 well beyond the mischief discussed during the Second Reading of the Bill in

[125] For instance, the conduct described in the main text accompanying note 118.
[126] *Supra*, note 4.

Parliament.[126] For instance, 'modification' of the contents of a computer would occur where the wrongdoer locks the computer keyboard and hides the key, or hides diskettes containing vital data or programs. Furthermore, it is submitted that such an interpretation would involve too great a departure from the words of a criminal statute.

It is this writer's view that the first of the possible interpretations of section 2(7)(c) is the less unacceptable alternative. If it is necessary to give some effect to that provision, then until it is amended, it ought to be read with the words "any event occurs" in place of "any act". Since we can only speculate over its meaning, no further discussion will be devoted to this provision.

(ii) *The mens rea*

The *mens rea* of this offence is 'knowledge' in the potential offender that his *actus reus* will lead to the unauthorised modification of the contents of any computer. This represents a significant departure from its UK equivalent which defines the *mens rea* as an intention directed at adversely affecting the performance of the computer by that modification. The English Law Commission intended their equivalent of the section 5 offence to be a specific offence with more severe penalties than the basic hacking offence; relatively minor misconduct involving modification of the computer's contents would not fall within the terms of the 'unauthorised modification' offence and would be dealt with as 'unauthorised access', while serious misconduct would be dealt with as 'unauthorised modification'.[127] By contrast, the approach of the local draftsman – making the *mens rea* element of section 5 easier to establish than its UK counterpart while defining the *actus reus* so widely as to potentially cover all situations of unauthorised access and more – means that our section 3 offence is probably redundant. Any offence under section 3 is almost certainly also an offence under section 5.

Under our section 5 then, the potential offender must subjectively know of the following:

(a) the result of his acts is 'modification' of the contents of a computer (that is, the "operation of any function of the computer" which results in the addition to, or alteration or erasure of a program or data in a computer);[128] and

(b) that result is 'unauthorised'.

[127] *Supra*, note 12, at para 3.62 to 3.64.
[128] S 2(7). This provision is explained in the main text accompanying notes 117 to 123, *supra*.

Some of the terms used to define (a) above (that is, 'computer', 'modification', 'function' and 'authorised') are the subject of the same technical definitions and raise similar problems of showing subjective knowledge as the section 3 offence. Proof of subjective appreciation of the causal link between an offender's acts and the result will involve similar difficulty as the term 'function' since the result can only be subjectively understood by a person having some knowledge of how computers work. Since problems of this nature were considered earlier,[129] no detailed discussion will be undertaken in this part of the article. The reasoning of the earlier discussion[130] is applicable here, *mutatis mutandis*, and leads to the conclusion that this offence requires the offender to appreciate that he causes the contents of an electronic device to be 'modified' in that the device no longer functions as it would have done before his acts. It is not necessary for the offender to appreciate exactly how the result of his acts falls within the explanation of that term in section 2(7) or how that result is achieved.

Proving that a modification is 'unauthorised' involves consideration of another provision in the Act. The concept of an 'unauthorised modification' is explained in section 2(8) in terms similar to those used to explain 'unauthorised access' in section 2(5).[131] It revolves around the concept of a "person ... entitled to determine whether the modification should be made..." (who will also be referred to as 'the Entitled Person' for the purposes of this discussion). A modification by someone other than that Entitled Person without consent of the Entitled Person is 'unauthorised'. Like section 2(5), section 2(8) does not explain further the nature of this 'entitlement' to determine whether the modification should be made. There is, again, no single legal concept that can adequately serve as the source of this 'entitlement' to determine whether a modification should be made.[132]

The distinct statutory explanation of 'unauthorised modification' clearly indicates that authority to have access to a computer is not the same thing as authority to modify its contents. It is also clear that the Entitled Person for the purposes of determining whether a modification to the contents of a computer is 'authorised' need not be the same as the Entitled Person for

[129] *Supra*, main text accompanying notes 59 to 84.

[130] *Ibid.*

[131] S 2(8) reads: "Any modification ... is unauthorised if –

(a) the person whose act causes it is not himself entitled to determine whether the modification should be made; and

(b) he does not have consent to the modification from any person who is so entitled."

Cf the concept of 'unauthorised access' which is set out in the main text accompanying note 48, *supra*, and explained in the main text accompanying notes 49 to 57, *supra*.

[132] *Supra*, notes 52 and 53 and accompanying main text. That discussion, *mutatis mutandis* applies to the concept of 'authority' to modify contents of a computer.

determining authority to have access to the contents of a computer. However, given the overlap between the terms "access" and "modification", it is submitted that in most cases, the Entitled Person in relation to questions of access to a computer will also be the Entitled Person in relation to modification of the contents of that computer. Both terms are equally vague and the analytical process which designates the most suitable person for one entitlement works equally well to designate the most suitable person for the other.[133] In either case, the Entitled Person should be the one with the greatest interest in protecting the integrity of the computer or computer system in question; he would be equally concerned with preventing unwanted access as with preventing unwanted modification to the contents of a computer.

(iii) *Summary*

The role played by the section 5 offence (if that can be discerned at all) is very different from its UK equivalent. It may be speculated that in his eagerness to make section 5 as widely applicable as possible, the draftsman turned it into a 'basic' offence, whose application goes beyond that of the section 3 offence, rendering the latter almost redundant.

At the level of interpretation, the drafting of section 5 raises the same basic difficulties as section 3; the problems of determining whether a modification is 'authorised' and defining the subjective knowledge needed to constitute the offence arise here with equal force. Additional uncertainties arise in determining what constitutes the 'contents' of a computer and in understanding the statutory explanation in section 2(7) of the term 'modification'. It is this writer's view that the offence should cover only modification of the contents of storage media which form an integral part of computers (excluding the RAM).

4. *Section 6 – unauthorised use or interception of computer service*

This section represents the major departure from the scheme of the UK Computer Misuse Act. It introduces three offences which were based on a source other than the UK Act – that is, section 342.1 of the Canadian Criminal Code (as amended by section 45 of the Criminal Law Amendment Act 1985). This will be referred to as 'the Canadian provision' hereafter.

[133] *Ibid.* It could be argued that the law of copyright seems a more appropriate source of the entitlement to determine whether a modification should be made than it is an entitlement to 'control access'. It is submitted, however, that the reasons why copyright is unsuitable for determining entitlement to control access (set out at note 53, *supra*) are equally overwhelming in relation to the entitlement to determine if a modification should be made.

The terminology of the Canadian provision was altered somewhat in an attempt to achieve consistency with that used in sections 3 to 5 of the Act, and the result has not been entirely a happy one from the point of view of clear drafting.

The new offences introduced by section 6 are:

1. Securing access without authority to a computer for the purpose of obtaining a computer service;[134]

2. intercepting without authority any function of a computer;[135] and

3. using a computer or other device for the purpose of committing offences (1) or (2) above.[136]

(i) *Securing access without authority for purpose of obtaining a computer service*

In the scheme of the Canadian provisions on computer misuse, the Canadian equivalent of this section provides the basic weapon against hacking; it is an offence thereunder to "fraudulently and without colour of right, obtain directly or indirectly, any computer service."[137] It will immediately be clear to the reader that although this section is meant to perform the same basic function as our section 3 and section 1 of the UK Act, it adopts a different approach to criminalising hacking, focusing as it does on the obtaining of a 'computer service'.[138] Thus the resulting offence is built around protection of the utility and value of a computer, treating it like other useful or valuable tangible property. The mischief at which the offence is directed can be compared to criminal offences involving misappropriation of such property. By contrast, the section 3 offence is directed at the obtaining of access to the contents of a computer only; the utility or value of that access is irrelevant to the offence.

Although the end result of these provisions is, for the most part, that similar conduct is criminalised by both offences, the conceptual gulf between them called for great care in any attempt to transplant terminology from the UK Act into the section 6(1)(a) offence. Given that we already have

[134] S 6(1)(a).
[135] S 6(1)(b).
[136] S 6(1)(c).
[137] S 342.1(1)(a) of the Canadian Criminal Code.
[138] The definition of this term has also found its way into s 2(1) of the Act which provides that the term 'computer service' includes "computer time, data processing and the storage or retrieval of data".

section 3 of the Act to deal with the basic hacking offence, one could be forgiven for thinking that it was not necessary (and perhaps somewhat confusing) to have a separate provision in the Act which creates another distinct offence in different terms but covering very much the same type of misconduct.[139] It is assumed for the purpose of this discussion that the intention behind the enactment of section 6(1)(a) was not simply to create an alternative source of criminal liability for conduct already covered by section 3, so this attempt to interpret the section 6(1)(a) offence will concentrate on trying to discern circumstances where the section 6(1)(a) is not merely superfluous.

The task of construing section 6(1)(a) is made more difficult by the fact that in trying to achieve consistency of terminology between this and the section 3 offences, the parliamentary draftsman replaced the terms used in the Canadian provision "...fraudulently and without colour of right, obtaining [a computer service]..." with the familiar "...secures access without authority to a computer for the purpose of obtaining [a computer service]...." The result was to graft on to the Canadian approach the complexities of interpreting the terms 'access' and 'authority'. This subtle alteration to the standard formulae used in section 3 makes matters even worse. For instance, section 3 employs the phrase "securing access ... to any *program or data held in any computer*" to describe the criminal intent needed to give rise to that offence. That phrase is explained in section 2(2). By contrast, section 6(1)(a) defines the *actus reus* of that offence as "securing access ... to any *computer*". The use of different terms and the different context imply that the explanation in section 2(2) is not available for the interpretation of that phrase in section 6(1)(a). There is no attempt elsewhere in section 2 to explain the latter phrase "access to a computer" so its meaning must therefore be derived independently of the terms of the statute.

Although the word 'access' does have a specific technical meaning in the context of computer technology, that technical meaning is unlikely to be applicable in this context since that technical meaning involves using that word as a verb,[140] whereas the word 'access' in section 6(1)(a) is used as a noun. Furthermore, the word 'access', used in its technical sense, is directed at the contents of the computer (as in section 3) rather than the physical device itself. The word 'access' in section 6(1)(a) thus cannot be given its technical meaning.

The Oxford English Dictionary (2nd ed, 1989), under the entry on 'access' states two possible meanings that may be appropriate to this provision:

[139] *A fortiori* where there is already a large degree of overlap between the s 3 and s 5 offences; see main text accompanying note 115, *supra*.

[140] See, for instance, the explanation in H Freedman, *The Computer Glossary* (4th ed, 1989): "Access is used as a verb and refers to storing data on and retrieving data from a disk or other peripheral device."

1. The action of going or coming to or into, coming into the presence of, or into contact with; approach, entrance...

2. The habit or power of getting near or into contact with; entrance, admittance, admission, (to the presence or use of)...

I shall refer to the former definition as the 'narrow' definition, while the latter is the 'broad' definition of access. The former is specific to the act of coming into physical contact with the computer while the latter refers to a state of being able to obtain either physical contact or simply the use of the computer. Under the broad definition, it is possible to have 'access' to a computer without ever having direct physical contact with it. For instance, where an authorised user of a computer agrees to comply with (or is tricked into complying with) directions from a stranger as to the use of the computer, the stranger could be said to have secured 'access' to the computer in the broad sense. Furthermore, 'access' in the broad sense is not limited to the immediate computer which the offender (or the person acting on his instructions) operates. A person having 'access' in this sense to a computer which is linked to a network also has 'access' to the network server and any other computer in the network which can be operated through that computer.

There is little to choose between these two meanings of the word 'access'. Either interpretation would allow the section 6(1)(a) offence to cover conduct going beyond section 3 (wide as section 3 is), though whether any useful purpose would be served in having such a criminal provision is debatable. Under either of these meanings, section 6(1)(a) might apply to make an offence of acts of preparation that allowed a person to easily come into physical contact or proximity with the computer in question. Such conduct, however, would likely constitute an offence under the Penal Code. If this 'access' was obtained by taking the key to a secure room where computers were kept, that could be theft under section 378, or criminal misappropriation of property under section 403 of the Penal Code. If the potential offender 'secured access' by leaving a window to that secure room open so he could enter later, his subsequent entrance might amount to the offence of housebreaking under section 445 of the Penal Code. Other situations are imaginable, but so long as our focus is on securing contact or proximity to the physical device, the existing property-based offences in the Penal Code are probably quite adequate to deal with the wrongdoing.

Thus, although the *actus reus* of the offence may cover some situations that fall outside section 3, any situations where it does so are probably adequately covered by existing criminal law offences. Furthermore, it is submitted that this section 6(1)(a) offence does not fit comfortably within

the scheme of the Act. A simpler offence which does not import the complicated conceptual baggage of section 3 – perhaps one defined by reference to the obtaining of a computer service by fraud or deception – may have been sufficient to deal with any perceived lacuna in section 3. For the moment, section 6(1)(a) as it is drafted is probably redundant, and nothing more will be said about it, except to consider problems in understanding the *mens rea* requirement.

The *mens rea* of this offence is to "knowingly secure access without authority ... for the purpose of obtaining, directly or indirectly, any computer service". The phrase 'computer service' is defined in section 2(1) in broad terms[141] to cover any use of a computer or computer system. The phrase 'directly or indirectly' is not entirely clear, but could cover the situation discussed above as the 'broad' definition of access – where the potential offender does not personally operate the computer, but has a third party do so on his behalf. It could also indicate that the computer service being obtained without authority is the use of a computer (*eg,* a network server) other than the one to which the potential offender has secured physical access.

The position of the term 'authority' in section 6(1)(a) makes it clear that it relates to authority to have access to the computer rather than the obtaining of the computer service. Because 'authority' here is related to rights to have contact with or use of the physical device, the explanation in section 2(5) of when 'access' to the contents of a computer is unauthorised is not applicable to the term used in section 6(1)(a). Indeed, relating as it does to some kind of right to control contact with or use of a physical device rather than its intangible contents, 'authority' here can be construed much more simply than the same word used in section 3. In this provision, 'authority' probably relates to consent by the lawful owner (or person having legal possession) of the relevant computer[142] to the offender having contact with or use of the device.

(ii) *Intercepting without authority any function of a computer*

This provision is meant to address a potential problem not expressly dealt with in the UK Act: 'electronic eavesdropping'. With increasing use of computer networks in offices and businesses, the interchange of data (which for simplicity will be referred to hereafter as 'communications') between computers and other computers or peripheral devices (*eg,* printers,

[141] *Supra*, note 138 and accompanying main text.
[142] Which is not necessarily the computer being directly operated.
[143] These devices are also likely to fall within the definition of 'computer' in the Act. That definition is discussed in the main text accompanying notes 22 to 27, *supra*.

facsimile machines)[143] is becoming an integral part of the functioning of those offices and businesses. It could be argued that there is little use in protecting the security of data and programs stored in computers if the security of communications is overlooked.

Electronic eavesdropping can take a number of forms. At its simplest, an eavesdropper who is an authorised user of a network may be able to circumvent security devices and tap into messages between users of the network as they are stored in static storage medium. This type of conduct is quite easily covered by section 3; so no more need be said about it. For eavesdroppers who are not (or choose not to be) authorised users of the network on which they wish to eavesdrop, it is possible to physically tap public communication lines, or attach devices to the target computer. Physical interference with computers or public telephone lines used for transmission may constitute the tort of trespass or criminal mischief, and possibly a criminal offence under the Telecommunications Act,[144] but that will depend on the exact nature of the acts involved. The law prior to the Computer Misuse Act could not deal with situations of eavesdropping which did not involve actual physical interference with the computer or communication lines. It is technically possible to place a device near a wire carrying communications signals without touching or interfering with it in order to read the signals passing through; or to use remote devices to 'read' and interpret electromagnetic signals emitted by computer monitors and reproduce the screen display of that monitor. Such techniques of eavesdropping fell outside the scope of the law prior to the Act.

The place of a provision on unauthorised interception of computer communications in the Act is therefore quite clear. While sections 3 and 6(1)(a) are directed at acts in relation to a computer or network which actively extract data or use from the computer, section 6(1)(b) can deal with the special situation of passive extraction of data from a computer or computer system. The problem with section 6(1)(b) lies in defining the offence.

Section 6(1)(b) makes it an offence to intercept or cause to be intercepted without authority any function of a computer by means of an electromagnetic, acoustic, mechanical or other device. As stated earlier in our discussion of section 3,[145] the term 'function' of a computer is defined in section 2(1) in the widest possible terms to cover not just signals passing to and from the central processing unit (CPU) of the computer to peripheral devices like storage media, monitors, keyboards or printers, but signals passing between and within the components of the CPU, as well as the operation

[144] Cap 323, 1993 Rev Ed. S 77 provides that it is an offence to touch or damage a telecommunications installation in order to intercept the contents of a 'message'. That term 'message' is defined in s 2 of the Act in sufficiently wide terms to include the transmission of electronic messages through telephone lines or by wireless means.

[145] *Supra*, note 36 and accompanying main text.

of some of those components. By providing also an the exhaustive list of means that can be used to intercept such signals ("electromagnetic, acoustic, mechanical or other..."), this provision is meant to cover all known and foreseeable means of computer-related eavesdropping.

The major difficulty with the offence created by section 6(1)(b) betrays the fact that section 6 has a different pedigree from sections 3, 4 and 5. The offence here is defined by reference to a concept of 'interception without authority' for consistency with those other provisions, but the definition provisions do not contain an explanation of that phrase, unlike the apparently similar concepts in sections 3 and 5.[146]

Assuming that the intention of Parliament in using the term 'authority' in section 6(1)(b) was to try to have a conceptually consistent thread running through the offences created by the Act, one can interpret the meaning of 'authority' in section 6(1)(b) by analogy to the explanations of that phrase in sections 3 and 5. Adapting the explanations in sections 2(5) and (8), 'authority' to intercept a computer function is determined by reference to a person 'entitled' to determine whether interception should take place. If an act of interception is not by that person and without his consent, then that act is 'unauthorised'.

It is difficult enough to try to understand what 'entitled' means in relation to controlling access to or determining modification of the contents of computers; the problem of trying to interpret that word in relation to 'interception' is compounded by the fact that the common law does not recognise any proprietary rights in information as such[147] nor a right to privacy[148] which could serve as a basis for the entitlement.

It is clear, then, that the term 'authority' in section 6(1)(c) cannot be interpreted in a manner consistent with its use in the earlier provisions. Lacking a legal right to prevent interception which might otherwise have

[146] *Cf* s 2(5) and (8) which explain 'unauthorised access' and 'unauthorised modification' respectively. The Canadian equivalent uses the concept of performing those acts "fraudulently and without colour of right" – s 342.1(1) of the Canadian Criminal Code.

[147] See *Oxford* v *Moss* (1978) 68 Cr App R 183; *R* v *Stewart* (1988) 50 DLR (4d) 1. The equitable doctrine of confidence cannot represent the source of this 'authority' since the rules relating to confidence are directed only at the dissemination but not the gathering of confidential information. In an English case, *Malone* v *Commissioner of Police of the Metropolis* [1979] 2 All ER 621, it was held that the equitable doctrine of confidence could not provide a remedy against tapping of telephone lines because that risk of tapping was said to be inherent in any use of a telephone system. Following from that decision, it is not possible to argue that a person who has a right to prevent disclosure of confidential information has an 'entitlement' to prevent its interception.

[148] Some legal rules that might be used to protect privacy are discussed in Rowe & Proudler, "A Review of the Right to Privacy, with Emphasis on Interception of Communications" (1993) 9 CL&P 224, but none of the rights considered in that article is of any assistance in this context.

permitted us to deduce who this Entitled Person ought to be, we are forced to the conclusion that authorisation does not follow from any legal right. To give effect to section 6(1)(b), we have to interpret the concept of 'authority' purposively, determining which party or parties to a communication between computers have the greatest interest in its security and taking such party or parties to be the Entitled Person(s).[149] Depending on the exact circumstances the following may be fill this position:

a. the owner of the computer or device which originated the intercepted function;

b. the owner of the computer or device which was the intended recipient of the communication;

c. the system provider or operator where the communication passes through a network;

d. the owner of the computer or the telecommunication medium through which 'interception' takes place (which will depend on the exact method by which the 'interception' occurs);

e. the originator of the communication, if human; or

f. the intended recipient of the communication, if human.

Note that, in the simplest case, a single person may fill all the positions listed, but a sophisticated network involving transmission of information between continents through leased telephone lines could see different parties occupying each position.

Of these many will be inappropriate under certain circumstances. The owner of the medium through which interception takes place ((d) above) will not be appropriate where the medium of communication through which interception takes place is not capable of ownership, *eg*, a wireless signal. The very wide definition of 'function'[150] of a computer means the originator or recipient of a communication ((e) and (f) above) is ruled out if the signals intercepted do not originate from a human source, or are not intended for a human audience.

[149] This raises the interesting question whether s 6(1)(b) creates a new legal right to control interception of communications between computers by implication. It is not possible to do justice to this question in this article so no more will be said of it here.

[150] The definition of this term is set out at note 36, *supra,* and discussed in the accompanying main text.

The system provider ((c) above) is not always appropriate because it is clear from section 6(1)(b) that the provision is not limited to communications within a network. Even so, it is submitted that in relation to communications through a network, the system provider is the most appropriate person to control interception since he has the greatest interest in maintaining the security of communications within it. His responsibility for the operation of the system also requires him to be able to monitor communications within the network; this would be an offence under section 6(1)(b) unless he were indeed the person entitled to control interception of communications. Furthermore, it would be consistent with our understanding of 'authority' in relation to networked computers under sections 3 and 5 of the Act.[151]

Where a communication is not sent through a network, the person with the greatest interest in controlling interception would probably be either the owner of the computer or device which originates the communication, or the owner of the computer or device which is intended to receive the communication ((a) and (b) above). Between these two, equally strong arguments could be made about their respective interests in preserving the security of the communication. Either or both these parties should be the Entitled Person in this case.

One consequence of the very wide definition of the terms used in defining the offence is that section 6(1)(b) can apply in unexpected situations. The wide definition of computers means that handphones and perhaps relatively sophisticated telephones, walkie-talkies or television sets are 'computers' for the purposes of the Act. Any transmissions to or from such 'computers' fall within the definition of 'function' of a computer.[152] Intercepting such transmissions without 'authority' would therefore be an offence under this provision. That would mean that listening in on telephone conversations through a telephone extension without permission could (depending on the sophistication of the telephone being used) give rise to liability under this provision! As telecommunication systems become more sophisticated, it is only a matter of time before the section 6(1)(b) offence is committed whenever an ordinary telephone extension is used to eavesdrop on an ordinary

[151] Discussed in the main text accompanying notes 54 to 56, 132 and 133, *supra*.

[152] The definition of 'computer' is considered in the main text accompanying notes 22 to 27, *supra*, while the definition of 'function' is set out at note 36, *supra*, and discussed in the accompanying main text.

[153] This would be the case where, for instance, a telephone processed words spoken into its receiver by converting words spoken into the microphone in the mouthpiece into digital signals through a 'logical or arithmetic' operation. These digital signals would be transmitted through the telephone line to be received and processed by the receiving telephone. Such a telephone would clearly have 'electronic processing capability' and would very likely fall within the definition of 'computer' in s 2(1), while signals running through the telephone

telephone call.[153]

More startling, since television and radio broadcasting in Singapore presently certainly involves the use of electronic processing equipment – 'computers' under the Act – broadcast signals emanating from such equipment (for instance, television broadcasts by the Television Corporation of Singapore ('TCS')) are a 'function' of those 'computers'.[154] If (which is arguable, given the uncertainty surrounding that term) TCS was the Entitled Person, then its consent for members of the public to intercept this 'function' could be conditional upon their holding valid radio or television licences issued by The Singapore Broadcasting Authority.[155] The result of this analysis is that using an unlicensed television could amount to an offence under section 6(1)(b) of the Act!

While these scenarios are the result of extreme interpretation of section 6(1)(b), and the dangers of such a wide interpretation would be avoided by judicious application of the Public Prosecutor's discretion, it is submitted that so wide and uncertain a definition of a criminal offence is undesirable. Considerable clarification of the terms of this offence is needed to make it workable, let alone to exclude the possibility of unexpected results.

(iii) *Using a computer or other device for the purpose of committing offences (1) or (2) above*

Section 6(1)(c) makes it a distinct offence to "use or cause to be used, directly or indirectly the computer or any other device" for the purpose of committing one of the other offences created by section 6(1). Some points may be made about the terminology in this provision. The *actus reus* of the offence is defined by reference to 'use' of a computer. It is probably because this provision is drawn from a different source than sections 3 and 4 that the usual formula "causing the computer to perform a function" was not employed. The Act does not define the term 'use' in relation to computers.[156] The plain and literal meaning of that term covers more than simply "causing a computer to perform a function"; a computer can also be said to be 'used'

cable would be communications between computers. Eavesdropping on such a communication would thus fall within s 6(1)(b) and associated definitions.

154 As "communication or telecommunication ... from ... a computer"; *supra*, note 36 and accompanying main text.

155 Until regulations are promulgated under the Singapore Broadcasting Authority Act (No 15 of 1994), s 80 of that Act provides that the issue of television licences will continue to be governed by the former Singapore Broadcasting Corporation (Broadcasting and Television) Regulations, GN S 21/80 (Subsidiary Legislation, 1990 Ed).

156 The phrase "use of a program" is explained at s 2(3), but that explanation is expressed to be limited to interpretation of the phrase as used in s 2(2)(c) which explains the meaning of 'access' to the contents of a computer.

when it is employed as a paperweight, though a purposive interpretation of this term ought to limit this offence to operation of the device *qua* computer. The *actus reus* also extends to causing a computer to be used, directly or indirectly.

In the light of our understanding of section 6(1)(a) and (b), it is not easy to see what purpose section 6(1)(c) serves in the scheme of the Act. Section 6(1)(c) crept into the Act on the coat-tails of the other parts of the Canadian provision (the significance of which is also diminished by the extremely wide terms in which sections 3, 4, 5 are defined). It appears to this writer that this provision does not apply in any realistic situation which is not already covered by other provisions of the Act. With the elements of our section 3 and 5 offences defined in such wide terms,[157] any conduct that disclosed an offence under section 6(1)(c) of using a computer or other device for the purpose of committing the section 6(1)(a) offence would already amount to commission of either the unauthorised access or modification offences. Section 6(1)(c) is thus redundant in relation to use of a computer for the purpose of committing the section 6(1)(a) offence.

Section 6(1)(c) is slightly wider than 6(1)(b) in that it covers unsuccessful attempts at committing the latter offence (for instance, where interception does not take place). Even so, section 6(1)(c) would still be redundant in relation to section 6(1)(b) since there is already a general provision in section 7[158] for attempts to commit offences under the Act.

(iv) *Summary*

With the exception of section 6(1)(b), the section 6 offences add little to the Act except unnecessary complexity. Sections 6(1)(a) and (c) do not serve any useful purpose since situations to which they can be applied are already adequately covered by the other offences in the Act or the Penal Code. The section 6(1)(b) offence of 'unauthorised interception' does cover new ground, but suffers from serious problems of definition.

5. *General points raised by sections 3 to 6*

(i) *Punishment*

The basic offences under sections 3, 5 and 6 carry penalties of a fine not exceeding $2,000 or imprisonment for up to two years or both. Sections 3(2), 5(2) and 6(2) provide an enhanced penalty of a fine of up to $20,000 or imprisonment for up to 5 years or both if "any damage is caused by

[157] Discussed in the main text accompanying notes 36 to 43 and 117 to 126, *supra*.
[158] *Infra*, main text accompanying notes 170 to 173.

an offence under [the relevant section] which exceeds $10,000".

Although the application of the enhanced penalty depends on the offence having resulted in 'damage' which is measurable in monetary terms, that term 'damage' is not defined in the Act. That leaves some uncertainty whether the enhanced penalty is intended to extend to situations where the 'damage' is caused to non-corporeal property or interests created by the new technology; for instance, loss or corruption of data or computer programs which can have serious economic consequences for the victim of computer misuse. An argument might be made that the term 'damage' is limited to physical damage to corporeal property. Since computer programs and data are intangible, the description 'physical damage' could not possibly apply to harm in the form of loss or corruption of computer programs or data without accompanying hardware damage and thus could not give rise to the enhanced penalty. Given that the intention of the Act is to protect the integrity of computers and their contents[159] by deterring hackers, and that hacking accompanied by modification of the contents of computers can lead to computer system failure falling short of physical damage to corporeal property,[160] such a narrow reading of the term 'damage' would not be helpful in achieving that end. Points were made about the meaning of 'damage' during the debate accompanying the second reading of the Computer Misuse Bill,[161] but the matter was not conclusively settled. It appears to this writer that the Minister for Home Affairs adopted a conservative interpretation of the word 'damage', excluding from its ambit damage to intangible property.[162]

Against that interpretation, section 10(1) of the Act speaks of compensation for "any damage caused to [a] computer, *program or data* by [an offence under the Act]..." (emphasis mine). These words imply strongly

[159] S 3(1) is directed at unauthorised access to "any program or data held in any computer" rather than the physical device itself.

[160] The English Law Commission, in its report (*supra*, note 12, at para 1.31), referred to what it considered to be a reliable estimate that the cost of restoring a commercial computer system that had been the subject of unauthorised access could run into hundreds and thousands of pounds. Charlesworth, *supra*, note 5, at page 87, cites an American survey reported in *Computing* magazine in 1992 which claimed that 85% of companies which experienced a major breakdown in their computer systems failed to recover and went out of business within 18 months.

[161] See the speeches by Mr Kenneth Chen, Member for Hong Kah GRC, Dr Ho Tat Kin, Member for Toa Payoh GRC and Nominated Member, Dr Toh Keng Kiat, *supra*, note 4, at cols 308, 310 and 315 respectively.

[162] In his reply to questions in Parliament, *ibid*, at col 317, the Minister for Home Affairs, Prof S Jayakumar, did not unambiguously exclude the application of the enhanced penalty to abuses which led to 'damage' to computer programs or data, but in the light of the members' remarks to which he was responding at the time (and particularly those of Dr Toh Keng Kiat, *ibid*), it appears unlikely that his reference to 'physical damage' as the trigger for the enhanced penalty included damage to intangible property.

that the term 'damage' as it is used in the Act encompasses non-corporeal harm in the form of alteration or erasure of computer programs and data. Further support is to be found in some recent criminal cases in England which have taken the view that the term 'damage' is not limited to physical damage to corporeal property.[163] Finally, deeming non-corporeal harm to be 'damage' would result only in a larger range of penalties being available to the court trying an offence that resulted in such non-corporeal damage. It would not fetter the court's discretion but would instead enhance it by permitting the court to impose the wider range of penalties where the circumstances (that is, the serious economic or other consequences of an offence) justified it.

It is therefore submitted that the term 'damage' should be construed liberally to include circumstances where the result of an offence is that non-corporeal articles ceased to exist or the value of the computer system was otherwise impaired, even though section 9A(3)(c) of the Interpretation Act[164] requires that weight be given to the position of the Minister of Home Affairs cited above.

A slightly different question is whether a purely economic harm caused by an offence amounts to 'damage' for the purposes of this provision. One possible consequence of an offence of hacking into a computer system is that upon its discovery, the owner or user of the system would as a matter of prudence shut it down to check for computer viruses[165] or corruption of programs and data contained in the system. Even if no physical damage were found, the natural consequences of the offence would still include the cost of these investigations, loss of revenue for the owner of the system, and a type of harm that can be described as 'loss of computer time'. Such harm can be expressed as an amount of money representing the economic value of time lost. These economic consequences of hacking should, using the same reasoning, be treated as 'damage' which would expose an offender who caused it to the enhanced penalty under section 3(2).

Applying the enhanced penalty to economic damage serves as a further deterrent to unauthorised access of a type that would lead a prudent victim to incur the costs of preventative maintenance upon discovery of that access. The increasingly heavy dependence of commercial entities and public bodies on computer systems and the costs involved in acquiring and maintaining such systems mean that shutting down a computer system for even a short period could quite easily lead to economic losses exceeding that threshold

[163] *Cox* v *Riley* (1986) 83 Cr App R 54, and *R* v *Whiteley* (1991) 93 Cr App R 25. Both these cases were concerned with offences under the UK Criminal Damage Act 1971 (c 48).
[164] *Supra*, note 44.
[165] The term is explained at note 114, *supra*.

sum of $10,000 stipulated in sections 3(2), 5(2) and 6(2). Uncertainties inherent in the quantification of such economic losses are well within the powers of the courts to resolve.[166]

Section 10 of the Act provides that a court convicting a person of an offence under the Act can order him to pay compensation "for any damage caused to his computer, program or data by the offence for which the sentence is passed." No limit is provided for the amount of compensation that can be ordered. There is little doubt that the term 'damage' here includes damage to non-corporeal property since computer programs and data are specifically mentioned. The UK Act does not contain an equivalent to this provision.

The civil law prior to the Act was unlikely to have been much use in obtaining compensation for victims of hacking.[167] The torts of trespass and conversion are premised on physical interference with tangible property. In the tort of negligence, the consequences of hacking would likely be classified as 'pure economic loss' unless there was some accompanying physical damage to tangible property and thus would be irrecoverable.[168] An action in conspiracy could obtain compensation for the consequences of hacking, but founding that cause of action would depend on satisfying the elements of that tort[169] and this remedy would have been of no use against lone hackers. The compensation provision in the Act thus overcomes a significant lacuna in the pre-existing law.

(ii) *Section 7 – abetment and attempt*

This provision has no equivalent in the UK Act. It provides that it is an offence to:

a. abet the commission of;

b. attempt to commit; or

c. do any act preparatory to, or in furtherance of, the commission of

any of the other offences in the Act. The punishment for an offence under

[166] *Cf* the Report of the English Law Commission (*supra,* note 12, at para 3.62), which expressed some doubts whether the courts could satisfactorily resolve these questions.

[167] It was thus likely that the Minister for Home Affairs was referring to the possibility of civil liability under this provision when he spoke of purely economic injury being adequately dealt with by civil remedies for damages; *supra,* note 162.

[168] *Spartan Steel* v *Martin* [1973] QB 27.

[169] The elements of conspiracy are set out briefly in *Halsbury's Law of England* (4th ed, 1985), Vol 45, at paras 1526 to 1530.

this section is the same as that for the offence which was abetted, attempted or for which preparatory or assisting acts were performed. The concepts of abetment and attempt are not explained in the Act, though general principles of criminal law on abetment and attempt are well understood in relation to Chapters V and XXIII of the Penal Code respectively;[170] so, no discussion will be devoted to abetment and attempt here, except to note that abetment of the section 3 offence could arise from such acts as publishing passwords for access to computer systems, running bulletin boards on which information useful to hackers is pooled, and selling and manufacturing equipment or software for breaking passwords or cloning handphones. Publishing information on how to create computer viruses, or assisting in the dissemination of a computer virus might amount to abetment of the section 5 offence.

It is also noteworthy that the definitions of the substantive offences in sections 3, 4, 5 and 6(1)(a) criminalise acts which may fall well short of hacking, so it is unlikely that it would ever be necessary (or even possible) to use section 7 in practice.

Of some academic interest is the last limb of the section 7(1) offence, which makes it an offence to do "any act preparatory to or in furtherance of the commission of any offence" under the Act. For convenience this offence "shall hereafter be referred to as 'assistance' of an offence". This phrase reproduces the formula employed in section 12 of the Misuse of Drugs Act, which also deals with abetment and attempts of offences under that Act. The terms by which this offence is defined – the doing of "any act preparatory to or in furtherance of the commission of any offence" – are so wide that they can cover all manner of innocent conduct. A technician who delivers, unpacks and installs a computer which is later used for hacking might be described as having performed an "act preparatory to the commission of [the hacking] offence".

The equivalent provision in the Misuse of Drugs Act was briefly discussed in the judgment of the Privy Council in *Ong Ah Chuan* v *Public Prosecutor*.[171] Lord Diplock, delivering the judgment of the court noted that the words creating that offence were extremely wide, but his Lordship did not offer any express guidance as to their limits. His speech seems to imply a mental element not expressed in the terms of that provision in the Misuse of Drugs Act and to suggest that an offence under this provision can only be made out where the act amounting to assistance was directed towards the

[170] The law in Singapore on abetment and attempt is discussed in Koh, Clarkson & Morgan, *Criminal Law in Singapore and Malaysia – Text and Materials* (1989), Chs 16 and 14 respectively.

[171] [1981] 1 MLJ 64. The charge in that case was brought under s 10 of Act 5 of 1973, the predecessor to s 12 of Cap 185, 1985 Rev Ed.

[172] *Ibid*, at 69.

commission of the further offence.[172] The need for a particular state of mind in the potential offender is clearly implied by the use of the word 'preparatory'; a person can only commit this offence where he subjectively views his acts as facilitating the commission of the subsequent offence. Applying that reasoning to this limb of section 7(1), an offence under this provision requires proof that the accused person intended by his assistance to commit a further offence under the Act or intended to assist another person in the commission of an offence under this Act. An offence under this provision may be constituted even where the acts performed do not amount to abetment or attempt so this provision could be used against a person who is authorised to have access to a network and uses that access to try to derive the passwords of other authorised users[173] as a prelude to the commission of an offence under the Act in future.

(iii) *De minimis principle*

Because it is relatively easy to satisfy the terms of the section 3, 5 and 6 offences, it may usefully be noted that section 95 of the Penal Code provides for a defence where the result of the offence is harm "so slight that no person of ordinary sense and temper would complain of such harm". Like section 79 of the Code, this provision is of general application to any criminal offence under the law of Singapore.[174]

The term 'harm' used in this provision is not defined elsewhere in the Penal Code. As defined in a dictionary, the term covers "[e]vil (physical or otherwise) as done to or suffered by some person or thing; hurt, injury, damage, mischief...."[175] This term clearly extends beyond physical damage to corporeal property and is capable of covering even intangible harm such as the impairment of the function of a computer or economic losses in the form of consumption of electricity by the unauthorised use of a computer.

What constitutes harm which is "so slight that no person of ordinary sense and temper would complain of such harm" is a question of fact the answer to which depends on the exact circumstances of the offence, and not simply the extent of any physical or other injury occasioned by the offence. Thus, the provision is unlikely to avail a remote hacker who simply obtains unauthorised access to a commercial computer system without doing more, since the consequence of such hacking is not trivial; the network provider may incur actual economic loss in shutting down the network for preventative maintenance. Even if no such costs are incurred, discovery

[173] Computer programs exist which can be used for this task.

[174] S 95, like s 79 (which was discussed in the main text accompanying note 65, *supra*) also falls within Part IV of the Act. The discussion in that note thus applies equally to s 95.

[175] The Oxford English Dictionary (2nd ed, 1989).

of the unauthorised access would undermine confidence in the integrity of the system, which cannot be described as a trivial harm. It was exactly such consequences of hacking that moved the English Law Commission to recommend the UK Act.[176]

Section 95 of the Penal Code is likely to be useful for dealing with purely technical non-hacking offences that could occur as a result of the very broad terms in which offences under the Act are defined. So for instance, changing the time setting on an electronic alarm clock without permission would technically be an offence under section 3 of the Act but a defence under section 95 would be available in such a case. Similarly, sending an unsolicited fax would cause the receiving machine to perform functions and involve execution of electronic instructions within that machine. An offence might be made out by such conduct, but in such cases, a defence under section 95 of the Penal Code might be available.

III. Application of the Computer Misuse Act Offences to Computer-Assisted and Computer-Related Crimes

The value of broadly defining sections 3, 4 and 5 of the Act is undeniable. With the increasing computerisation of banking and other commercial arrangements, these provisions are capable of dealing with misconduct involving computers and other such devices which goes well beyond the term 'hacking'. In particular, section 3 may be useful for dealing with misconduct involving computers and other devices that cannot be adequately covered by existing criminal law concepts,[177] such as 'tricking' a computer (which is not presently capable of falling within the description of 'cheating' in section 415 of the Penal Code). Section 5, on the other hand, can be applied to modern types of 'theft' that fall outside the Penal Code definitions because in a sophisticated commercial setting, account balances reflected in computerized records are as important as corporeal property although not similarly protected under the Code.

The price of defining these offences so broadly that they can cope with as yet unforeseen technological developments and new types of misconduct is that the provisions must necessarily be expressed in such general terms that they can be difficult to use. Such difficulty is most evident as we try to identify the Entitled Person (*ie,* the person whose consent is required for access to or modification of the contents of a computer to be authorised) in relation to the section 3 and 5 offences, particularly with respect to the

[176] *Supra*, note 12, at paras 1.10 and 1.29.

[177] S 4 may be less useful in this respect, tied as it is to those very criminal law concepts considered to be inadequate to deal with the new technology; *supra*, main text accompanying notes 103 to 110 and accompanying main text.

range of other electronic processing devices to which these offences can apply. Because of this wide range of possible situations in which the Act may be invoked (and the types of situations in which these offences may be invoked are likely to grow as technology advances), this article can offer only a few illustrations of how these provisions might be used in relation to non-hacking misconduct and demonstrate some of the difficulties in identifying the Entitled Person. The following situations will be considered:

(a) unauthorised use of ATM cards;

(b) use of forged credit cards;

(c) use of 'cloned' handphones;

(d) voice-mail eavesdropping; and

(e) protection of electronic databases.

A. *Unauthorised Use of ATM Cards*

Using a forged or stolen ATM Card in an Automated Teller Machine to withdraw cash could fall within the terms of section 4.[178]

1. *Physical act element*

An Automated Teller Machine is a 'computer' under the definition in section 2(2).[179] It performs 'functions' as defined in section 2(2) when an ATM card is inserted – reading data stored in the magnetic stripe of the card, running a program or programs which leads to processing of the data read from the card, changing the screen display that communicates with the user and communication with a server in which account particulars are

[178] The use of forged ATM cards is a real and growing problem in Singapore. A recent case was reported in an article, "2 Used Fake ATM Cards to Withdraw $96,000", The Straits Times, 17 June 1993.

[179] This assumption is not strictly necessary for this illustration. An offence may be committed even if one does not find the ATM to be a 'computer' since operating the ATM will necessarily result in signals being exchanged between the ATM and a remote computer ('the server') in which the relevant bank stores account records. That exchange of signals will amount to the performance of functions by the server in the form of telecommunication with the ATM (see the definition of 'function' in s 2(1) set out at note 36, *supra*).

stored. The physical act element of this offence is thus easily established.

2. *Mental element*

This would be satisfied by the intention of the wrongdoer to commit theft under section 378 of the Penal Code.[180] From the offender's conduct, it can easily be inferred that he intends dishonestly to take movable property (money) from the bank,[181] and does indeed move that property (by removing the money from the machine) without the consent of the bank.

3. *Purpose element*

Section 4 requires that physical acts be performed "for the purpose of securing access without authority to" some program or data held in any computer. By inserting the ATM card into the requisite slot in the machine, the offender secures 'access' to the program that operates the ATM machine.[182] The fact that 'securing this access' was a necessary step to the offender's ultimate objective of withdrawing money from the ATM means that this securing of access can be said to be the purpose of his acts.[183]

The most difficult part of our analysis is to determine whether the access was 'unauthorised'. Under section 2(5), that would depend on whether the 'access' was obtained without the consent of the Entitled Person. The earlier discussion interpreting the meaning of 'authority' in relation to section 3[184] shows that the Act provides little guidance to help us determine who is the Entitled Person in relation to the program that operates the ATM. Assuming our earlier conclusion is correct – the Entitled Person is the one with the greatest interest in preventing unauthorised access – possible Entitled Persons in this scenario are the account-holder whose account balance is debited with the cash withdrawal, and the bank which owns the ATM and perhaps the server.[185] A court considering an offence on these facts would have to decide from first principles whether the Act requires us to look to any one of these parties, or either or both to determine if the transaction was authorised. Our determination is further complicated

[180] The elements of this offence are set out in the main text accompanying note 104, *supra*.
[181] Our concern here is with the taking of money out of the possession of the bank rather than the account-holder, since only the former can be said to have 'possession' of the money in the ATM.
[182] The way in which this is achieved is set out in the main text accompanying note 179, *supra*.
[183] See the definition of 'purpose' at notes 41 and 42, *supra*, and accompanying main text.
[184] *Supra*, main text accompanying notes 44 to 57.
[185] Additional complications will arise where a third party owns the server, but these will not be considered in this article.

by the fact that there are at least two possible occasions of 'access' which may be used in defining the offence; access to the program which leads to operation of the ATM and access to data (that is, the account balance) held in the server.

In the process of deciding whether the Entitled Person is the bank or the account-holder, or both, a court may need to consider the broader implications of designating either party as the Entitled Person to the exclusion of the other. If only the bank is the Entitled Person, then even legitimate holders of ATM cards must take care not to exceed the terms of the consent given by the bank since that would make their access 'unauthorised' and expose them to criminal liability under section 3 of the Act. As an illustration, consider a situation where a bank issues ATM cards subject to a condition that only the account-holder personally may use the card and know the Personal Identification Number (PIN) needed to operate an account with the card. In these premises, if a third party other than the account-holder uses the card and PIN to check the account balance or withdraw money from an ATM, he does so without the consent of the Entitled Person even if he had permission from the account-holder; he thereby commits an offence under section 3 unless he operated under an honest misapprehension that he had the consent of the Entitled Person. And if the account-holder had requested this third party to use the card to check the account balance or withdraw money on his behalf, the account-holder may himself have committed an offence of abetment of the unauthorised access offence.[186]

In view of this awkward result if only the bank is the Entitled Person, it is submitted that the better view is that in situations of access involving ATM machines, both the bank and the account-holder should be considered to be Entitled Persons, and that either is capable of authorising 'access' through the normal use of an ATM card.

B. *Use of a Forged Credit Card*

Although wrongdoers who use forged credit cards to make purchases are capable of being dealt with under existing provisions of our criminal law,[187] it may still be desirable to have the option of charging an offender under section 4 of the Act because of the higher penalty stipulated there than

[186] S 7 of the Act; *supra,* at note 170 and accompanying main text.

[187] Possibly the offence of cheating under ss 415 to 420 of the Penal Code.

[188] An offence under s 4 of the Act carries liability for a jail term of up to 10 years, while the most severe punishment for a cheating offence that may be used in this situation – cheating which induces a delivery of property – is a maximum sentence of imprisonment of up to 7 years – s 420 of the Penal Code.

is available under the Penal Code offences.[188] This article will therefore illustrate how section 4 of the Act might be applied in relation to the use of a forged credit card. It is also instructive to note the difficulty that arises in identifying the Entitled Person under these circumstances.

Section 4 may be invoked in these situations because merchants in Singapore tend to accept payments by credit card only after obtaining approval for that transaction from the party which purchases their credit card vouchers (the 'merchant acquirer' hereafter), or someone acting on his behalf. This approval is now commonly sought and obtained through the use of computer technology – the merchant runs the card's magnetic stripe through a card reader attached to a telephone line (sometimes called 'swiping' the card). This card-reader would almost certainly fall within the definition of 'computer' under the Act[189] since it would contain a program which is activated when the credit card is swiped. The device will read the cardholder's account particulars from the magnetic stripe and transmit that data *via* the telephone connection to a remote server which approves transactions on behalf of the merchant acquirer. That data would then be processed by the server together with transaction details provided by the merchant and if all is in order, approval is given in the form of a code transmitted back to and displayed by the card-reader. In some cases, the server will also transmit instructions to a device in the merchant's shop that prints the credit card voucher complete with card and transaction details.

In these premises, the elements of the offence are made out as follows:

1. *Physical act element*

By proffering the forged credit card, the potential offender will cause the merchant to run the card's magnetic stripe through the card-reader; he will therefore have caused a 'computer' (the telephone-cum-card-reader or the server) to perform a 'function'.[190]

2. *Mental element*

For the purposes of this discussion, it is assumed that the potential offender actually knows that the card is a forgery (and that this can be proved). His intention to commit an offence of cheating will necessarily follow – the offender's aim is clearly to deceive the merchant to hand over property

[189] See the discussion on the definition of the term 'computer' in the main text accompanying notes 22 to 27, *supra*.

[190] S 4, like s 3 does not require that the offender actually directly operate a computer; *supra*, main text accompanying note 36. The operations performed by the computers as described in the preceding paragraph clearly fall within the definition of 'functions'.

or provide some service that he would not provide if he knew that the card was a forgery. Exactly what cheating offence is committed depends on whether the credit card is used for a payment that involves delivery of goods or otherwise. If the former, the intended offence is cheating which dishonestly induces the person deceived to deliver property.[191] This offence is punishable with up to seven years' imprisonment so it falls within the ambit of section 4 of the Act. If no goods are to be delivered by the merchant accepting payment by means of the credit card, then the offence intended may fall within the definition of cheating by personation[192] which is punishable with imprisonment of up to three years.[193]

3. P*urpose element*

The ultimate objective of our hypothetical offender is to cause the merchant to deliver goods or provide some service to him in exchange for his purported payment by credit card. In achieving this objective, it is likely that the merchant will swipe the card in order to seek approval from the card company or its agent. This will necessarily involve 'access' to the contents of a computer. The access in question could be access to the program in the card-reader or access to the program in the server which checks the account particulars and approves the purchase – both occasions would fall within the explanation of 'access' in section 2(2)(c) read with 2(3)(a) – access in the form of causing that program to be run. It can therefore be said that the purpose[194] of the physical act (offering the card for payment) is to obtain access to some program contained in either of these computers since obtaining access is a necessary incident to his broader purpose.

Determining if the access sought was unauthorised is again difficult. In this case, there are a number of potential Entitled Persons – the merchant acquirer, the card issuer (*ie,* the party which issued the credit card to the cardholder); the party which owns the server; the merchant or person who owns the card-reader; and the cardholder whose card is forged and whose

[191] S 415 read with s 420 of the Penal Code.

[192] S 416 read with s 419 of the Penal Code.

[193] In this scenario, the potential offender, by proffering the forged card and signing the credit card voucher, falsely represents that he is the credit card account holder.

[194] *Supra*, notes 41 and 42 and accompanying main text.

[195] A single party may, depending on the circumstances, fill more than one of these positions; the credit card issuer may also happen to be the merchant acquirer. As specific arrangements between the parties can vary, it will be assumed for the purposes of this article that all these parties are distinct. The relationships between the parties to credit card transactions are described in a report by the Monopolies and Mergers Commission, *Credit Card Services: A Report on the Supply of Credit Card Services in the United Kingdom*, Cm 718 (1989), Ch 2.

account will be debited with the cost of the transaction.[195] Again, it is not clear if any one or a combination of some of these parties, or even all together are the Entitled Person(s). A court faced with the choice would again have to consider the implications of designating a particular individual as the sole source of authority.

Designating the card issuer, for example, would place great legal significance upon the terms of issue of the cards. The terms of issue could, if appropriately drafted, be construed as leading to an automatic revocation of authority when the card has expired, or when the cardholder's credit limit is exceeded. If that is the case, a cardholder would commit the section 3 offence by using the card after it has expired or by exceeding his credit limit provided he knew of the relevant facts.

In a complex situation like this, it is submitted that a court may, in determining who is the Entitled Person, consider who would be most likely to suffer loss as a result of such an offence. Such a person has the greatest interest in being able to determine whether a use is 'authorised' or not, and would have a strong claim to be the Entitled Person. The determination of the Entitled Person could thus depend on the nature of the agreement between the card issuer and the cardholder, and/or that between the merchant and the merchant acquirer in relation to the allocation of losses involving the use of such credit cards.

Although this discussion considers only a scenario where the merchant uses an electronic device to obtain the merchant acquirer's approval for the purchase, section 4 might still be available where the merchant obtains approval by telephoning his merchant acquirer (or someone acting on his behalf) and reading out the card particulars before obtaining an oral approval. This is because the merchant acquirer (or the person acting on his behalf) is likely to give the approval only after checking those particulars against data held in a computer database. The offender could still be said to have "caused a computer to perform a function for the purpose of securing access" to that data since there is a direct causal link between his acts and the ultimate operation of the computer.

It is also to be noted that both the offences of use of forged ATM and credit cards could give rise to offences under section 5 of the Act; a necessary result of the offender's ultimate purpose would be modification of data in computers, being a debit in the account particulars of the person whose ATM or credit card was forged. It is unlikely that resort will be had to section 5 given that a heavier penalty can be imposed under section 4 of the Act.

C. *Use of 'Cloned' Handphones*

Section 4 may be used against persons who knowingly make calls on 'cloned

handphones'. The term 'clone' is used to describe handphones whose electronic serial number (ESN) is changed. Every handphone is programmed with a unique ESN which is used by the telephone system to identify the source of calls through the system. Thus, changing the ESN on a handphone will cause the telephone system to record calls from that handphone (the 'clone') as having been made by another handphone – the one whose ESN was copied into the clone. The subscriber who owns the handphone whose ESN is copied into the clone (the 'victim') is thus billed for calls made through the cloned handphone.[196]

1. Physical act element

This could be satisfied either by the reprogramming of the cloned handphone with a new ESN (which would necessarily involve the use of electronic equipment falling within the definition of 'computer') or by the offender switching on the cloned handphone or simply the making of a call on that handphone; the clone (which falls within the definition of the term 'computer' in the Act by virtue of its microprocessor-based operation) performs functions in the form of logical operations upon being switched on or in the process of making the call.

2. *Mental element*

Provided the potential offender was aware that the handphone he used was cloned, and that he was operating an electronic device, he would satisfy the requirement that he knowingly cause a computer to perform a function with intent to commit another offence.

The ulterior offence in this case is an offence under section 79 of the Telecommunication Authority of Singapore Act which goes under the short title of "fraudulent use of telecommunications system".[197] An act of knowingly using a cloned handphone would probably allow a court faced with these facts to infer that the accused person had intended to commit that offence.

3. *Purpose element*

[196] The process of 'cloning' a handphone is described in an article entitled, "Illegal Software Used to Clone Handphones" in The Straits Times, 6 July 1993, at 22.

[197] S 79 of the Telecommunication Authority of Singapore Act provides as follows: "Any person who dishonestly uses or permits another person to use any telecommunication service provided by a public telecommunication licensee with intent to avoid payment of any charge applicable to the provision of that service shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both."

Making a call through the cloned handphone would necessarily lead to the operation of computers other than the clone itself. In Singapore, the hardware performing the electronic switching functions necessary to connect the call would fall within the definition of a 'computer' in section 2(1) of the Act. Recording of the billing details would similarly be computerized. In either of these cases, the computers would respectively execute their programs to connect the call or record billing details when a call was made on a cloned handphone. This would amount to 'access' by the handphone user to those programs.[198] Since this access is necessarily incidental to the making of the call on the cloned handphone, the physical act is performed "for the purpose of securing" this access.[199]

To determine whether this access to the programs which execute the switching functions or record billing details is 'authorised' or not, we must consider who the Entitled Person is in this case. The most likely parties (*ie,* those with the greatest interest in preventing the undesired access to the switching functions or billing details) are the party providing the telephone service and the victim whose ESN has been copied. The former is probably more appropriate, since our concern is with access to programs in computers owned and operated by the service provider.[200] Under this analysis, then, the telephone service provider is the Entitled Person and only subscribers to the telephone service have his consent to have access to these programs and data. Unless the terms of the arrangement between the service provider and the handphone owner prohibit lending of handphones, the consent to have access would probably impliedly extend to persons permitted to use the handphones by the owners. Users of cloned handphones are, on this analysis, clearly 'unauthorised'.

Proving knowledge of this lack of authority may be more difficult, though it is submitted that the requisite knowledge will be inferred by a court where it can be shown that the potential offender knew that the handphone was

[198] S 2(2)(c) read with s 2(3)(a) provides that causing the program in a computer to be executed amounts to access.

[199] *Supra*, notes 41 and 42 and accompanying main text.

[200] The victim would clearly be concerned as well, since he would be faced with a demand for charges incurred through the cloned handphone. Even so, his concern is with his liability to pay for calls recorded by that system and not directly with the access to the contents of the computerised switching system so it is assumed for the remainder of this discussion that the system provider, being the party with the most direct interest in preventing unauthorised access, is the Entitled Person.

cloned and that some other person would be charged for the call made by the potential offender.

D. *Voice Mail Eavesdropping*

This is a fairly straightforward application of section 3. The purpose of raising it in this article is simply to point out that section 3 is an extremely powerful weapon for dealing with new types of misconduct raised by emerging technologies. There is little doubt that voice-mail systems (which are almost certainly computerized) are vulnerable to eavesdroppers.[201] If the message which is compromised is sufficiently important, it can have serious consequences for the victim.

The basic hacking offence in section 3 is committed when a voice-mail eavesdropper gets access to messages stored in the computer which provides the voice-mail service; the eavesdropper would necessarily cause the computer which implements the voice-mail system to perform some function in order to get access to its contents. His purpose in doing so is to get that access. Once again, in order to determine whether that access is authorised, it is necessary to identify the Entitled Person in relation to that access. This would be either the provider of the voice-mail system or the person to whose mail the access was sought. As with cloned handphones, the provider of the voice-mail system would probably be the Entitled Person since it would have the greatest interest in maintaining the integrity of the whole system. The system provider would give consent to individual users to have access to their own electronic mailboxes only. An eavesdropper accessing another user's mailbox without consent is unauthorised and the section 3 offence is easily constituted in this scenario.

The section 5 offence may be committed by a voice-mail eavesdropper if he erases or alters any message contained in the mailbox.

E. *Protection of Electronic Databases*

If the conclusions reached earlier in this article as to the concept of 'authority' are correct,[202] then section 3 may be used to protect the interests of providers of electronic database services independently of copyright. The nature of electronic databases and problems relating to the protection of

[201] Voice-mail eavesdropping is discussed in a newspaper article, Bulkeley, "Hot Numbers – Voice-Mail Eavesdropping Emerges as Security Risk", Asian Wall Street Journal, 29 September 1993.

[202] *Supra*, notes 48 to 57 and accompanying main text.

[203] The EC Commission Draft Directive on the legal protection of databases (92C 156/03) OJ [1992] C156/4.

the interests of those who would commercially exploit them (particularly by copyright law and new *sui generis* regimes of protection such as those proposed by the EC Commission[203] (as it was then called) are discussed in a number of articles.[204] It is only necessary to add here that the section 3 offence would be available to providers of electronic database services against persons who obtain access to the contents of an electronic database without their consent (and more importantly, without paying), or where persons with consent exceed the terms of the consent given to them. The latter would depend on the provider of that electronic database service clearly defining the nature of the consent which is given to users of the database to have access to the contents. While an argument may be made that failure by a licensee to observe the terms of his license should not give rise to criminal consequences but should only involve a civil claim in contract between the database provider and the licensee, there can be little doubt that so long as the database provider is designated as the Entitled Person in relation to that database, it is possible for him to use the Act to protect his interests.

Bringing the conduct of unauthorised users of an electronic database within the terms of the section 3 offence is a straightforward application of the principles discussed earlier so nothing more need be said on this point.

IV. Conclusion

The offences created by the Act represent a welcome attempt to deter new types of undesirable conduct. The range of computer-related misconduct and the possible evolution of further types of misconduct yet undreamed of requires offences to be defined in the most general of terms. Breadth of application has been achieved, but at the expense of ease of interpretation, and by creating a great deal of overlap between the types of conduct covered by sections 3 to 7.[205] The terminology used in the Act (some of it inherited from the UK Act, but much self-inflicted) requires considerable clarification. In particular, the concepts of 'authorization' to have access to a computer or its contents, to modify the contents of a computer, and to intercept the functions of a computer all require more precise definition or interpretation by the courts if they are to be usable.

[204] See articles by Pattison, "The European Commission's Proposal on Protection of Computer Databases" [1992] 4 EIPR 113; and Nimmer and Krauthaus, "Information as Property – Databases and Commercial Property" 1 International Journal of Law and Information Technology 3.

[205] This is discussed in the main text accompanying notes 115, 119, 120, 123, 139 and 157, *supra*.

Although no discussion was devoted to the provisions on evidence and investigation, it must be noted that the likely deterrent value of the computer misuse offences depends in no small measure on the ability of the authorities to enforce the new offences. The Act contains significant new provisions on evidence and investigation to facilitate the policing of offences, but space does not permit further discussion beyond some brief observations.

Even with heightened investigative powers and clearer rules on computer-generated evidence under the Act, proof of the commission of computer misuse offences is unlikely to come easily. The hacking offence at which the Act was primarily directed can be committed in the privacy of a hacker's home through telephone lines. It is possible to criminalise conduct that does not involve physical presence of the wrongdoer at the place where the harmful effects are suffered, but the lack of a physical nexus to tie the offender to the offence will make proof of the offence extremely difficult, special investigative powers notwithstanding. Proof of offences will depend to a great degree on evidence yielded by computerized records kept by computers that have been subjected to the offence (whose reliability may have been affected by the offence, anyway). Any such evidence is unlikely to amount to more than a record of telephone numbers of persons who have called in to the system, and that may not be sufficient to tie an individual to the offence. It may be that proof of an offence under the Act will require the hacker to be caught with his fingers on the keyboard.

There is also a danger that victims of offences, particularly commercial organisations, may not wish to report that their computer systems have been subject to offences under this Act since that might undermine public confidence in their operations. Ultimately, the deterrent effect of offences created by the Act will not be significant unless further steps are taken to increase the likelihood that offences are detected and offenders charged. The minor changes made by the Act are a start, but only that; more radical changes to regulate computer use or preferably to educate computer users would make a significant difference to the ability of the Act to achieve its objectives. It is up to system providers, the potential victims of offences, to regulate properly their relationships with users, keep proper records of use of their systems, institute security measures against unauthorised use or access and monitor their systems to detect offences. Such measures would greatly assist in investigating and proving computer misuse offences. As computerisation filters down to relatively small organisations, there is a danger that such concerns might find it uneconomic to institute such measures without encouragement from the authorities.

These matters go beyond the nuts and bolts of a criminal statute. They require education of the public, and perhaps ultimately, some non-criminal, regulatory framework for computer use by commercial concerns, particularly

in situations where such computers can be misused to cause harm to third parties. In this respect, the call by the MP for Fengshan, Dr Arthur Beng, during the debate following the second reading of the Computer Misuse Bill for a regulatory body to oversee the information technology industry is worthy of further consideration.[206]

CHRISTOPHER LEE GEN-MIN*

[206] *Supra*, note 4, at cols 306 and 307. In reply, the Minister for Home Affairs, Professor S Jayakumar pointed out (at col 318) that such action was properly within the purview of other Ministries.

* LLB (NUS), LLM (Lond), Advocate & Solicitor (Singapore).
I would like to thank Professors Koh Kheng Lian and EP Ellinger, Mr Terence Tan Bian Chye, Mr Tan Yock Lin, Mr Yeo Tiong Min, Mr Gilbert Leong and Ms Valerie Ong for their kind assistance and comments. All errors are mine.