2002

Vaguely Going Where No-one has Gone: the Expansive New Computer Access Offences

Alex Steel, *University of New South Wales*

Vaguely Going Where No-one Has Gone: the Expansive New Computer Access Offences

Alex Steel

Faculty of Law, University of New South Wales[*]

Both the New South Wales and Commonwealth governments have enacted major reforms to computer-related offences. These reforms are based on the Model Criminal Code Chapter Four: Damage and Computer Offences. The reforms move from an emphasis on access to an emphasis on damage. While they provide principled limitations on some previous offences they also introduce new sweeping offences relating to network impairment and control of data preparatory to other offences. This article outlines the elements of these new offences and highlights the issues that are likely to arise in their enforcement.

Introduction

Computers constitute an indispensable part of modern life. Increasing aspects of our lives, the conduct of commerce, and government administration are now controlled by computerised systems. With the large scale networking of these systems and the consequent increased ease of access to them, the potential for unauthorised access leading to misappropriation of information or illegal financial gain is enormous. Traditionally, the laws that dealt with these types of activities have been the various offences of larceny (or theft) and obtaining by false pretences (or obtaining by deception). Illegal access has been covered by the laws of trespass, breaking and entering, and criminal damage. But all of these offences were developed to deal with tangible property only and are not easily applicable to the digital environment.

The deficiencies in these laws led to a number of government inquiries in the late 1980s into appropriate laws to protect computer systems.[1] This in turn led to a raft of computer access crimes which were *sui generis* in nature. However, as technology has developed significantly since then, it was felt further reform was necessary, particularly to take into account the prevalence of computer networks. The new offences in New South Wales[2] and the Commonwealth[3] represent this latest wave of reform.

This article examines these new substantive offences. They are based entirely on the recommendations of the Model Criminal Code Officers Committee (the Committee) Report *Chapter 4: Damage and Computer Offences* (the MCCOC Report).[4] In comparison with the previous

* The author wishes to thank Ian Leader-Elliott for his valuable and detailed comments on earlier drafts of this paper. All opinions expressed in the article are of course entirely the author's.

[1] There were a large number of reports on the problem in the 1980s, the most significant in Australia being the Review of Commonwealth Criminal Law Interim Report on Computer Crime 1988 (the "Gibbs Report") and, in the United Kingdom, The Law Commission Working Paper No 110: Computer Misuse 1988.

[2] *Crimes Amendment (Computer Offences) Act 2001*.

[3] *Cybercrime Act 2001*.

[4] http://www.law.gov.au/publications/Model_Criminal_Code/DamageReport.pdf

laws on computer crime, the new offences show a marked change in emphasis from criminalising access to computers to an emphasis on damage to, or degradation of, computers and electronic communication between computers. However, the breadth of the terms by which the damage is defined has created an even broader scope of potential criminality. Appendix A provides a comparative overview of the change in emphasis, based on the NSW offences.

The new offences are arranged by placing general definitions first and then ranking the offences from most serious to least serious. However the easiest way to appreciate the scope of the offences is to deal with the substantive offences in what is effectively a reverse order. Consequently, the following analysis does not follow the sections in order, but instead deals with subsections in the order in which the issues might be dealt with when considering prosecution under the sections.

Jurisdictional issues

Apart from a small number of wording differences, the Commonwealth and NSW laws are substantively identical. The one major difference is that, while the State legislation is expressed generally, the Commonwealth law is necessarily limited in its jurisdiction. The Commonwealth legislation however seeks to maintain the broadest possible scope and relies on four bases for its enforceability. Commonwealth jurisdiction arises under the *Criminal Code* if the substantive actions involve, generally speaking, one of the following:

- the data is held in a Commonwealth computer,
- the data is held on behalf of the Commonwealth in another computer;
- a Commonwealth computer is used in the commission of the offence; or
- a telecommunications service is used in the commission of the offence.

Each offence is expressed as a series of permutations of these elements. In order to avoid doubt, the Commonwealth offences deem these jurisdictional elements to be absolute liability elements.[5]

"Commonwealth computer" is defined in s 476.1 of the *Criminal Code* to include computers owned, leased or operated by a Commonwealth entity. Some uncertainty surrounds the meaning of "operate". It may be that the mere use of a computer by a Commonwealth employee in the course of their employment may be sufficient to deem that computer a Commonwealth computer. However, it is arguable that such a broad approach is not intended. This is because the offences also use the phrase "executing a function of a computer". "Operation" would appear to imply a more ongoing connection with the computer than a mere execution of a function of the computer.

In terms of jurisdictional reach, it is understandable that the Commonwealth would seek to protect the integrity of its own computer systems and data that it has stored in non-Commonwealth computers. But in also including the use of telecommunications services in the scope of the offences the Commonwealth has taken over a large proportion of all "cybercrime" in Australia.

"Telecommunications service" is defined in s 476.1 as "a service for carrying communications by means of guided and unguided electromagnetic energy or both." The definition is in similar terms to that of "carriage service" in the *Telecommunications Act 1997* and is obviously designed to cover comprehensively all forms of electronic communication in Australia. The only restriction lies in the notion of a "service". Given that the word is related to "servant" which involves the notion of one person assisting another, there is a strong implication that it only applies to communication channels that are provided by a party external to the owner of the computer. In choosing to refer to a "telecommunications service" and not an "electronic link or network"[6] the implication is that the communication channel is in someway ongoing and maintained.

If such restrictions are to be read into the legislation, the Commonwealth offences might not apply to telecommunications networks that are

[5] This is necessary as s 5.6 of the *Criminal Code* provides that if any physical element of an offence that consists of a circumstance does not have a fault element then recklessness is required as the fault element. Absolute liability is appropriate in these circumstances, as the elements do not increase or decrease the scope of the offences. They merely establish Commonwealth or State and Territory jurisdiction.

[6] This is part of the definition of "electronic communication" in s 476.

exclusively controlled and maintained by the owners of the relevant computers. But if the intranet of an organisation involves use of methods of communication leased from others, then the Commonwealth would have jurisdiction.

The use of the telecommunications power as a constitutional basis for Commonwealth jurisdiction has major implications for State and Territory legislation. Such provisions may only have the residual force of applying to use of stand alone computers or where there is no use of the network to which the computer is connected. As such the inclusion of "telecommunications service" represents a major grab for power by the Commonwealth over electronic crime. In many ways the national approach that this results in is welcome. It is unfortunate though, that the extent of the jurisdiction of the Commonwealth law is undefined and uncertain. It is clear, however, that, as the large majority of computer crimes will involve at some stage the use of commercial telephone and cable services, much of the enforcement of this legislation is likely to be done through Commonwealth law.

A further complicating issue is the interaction of the Commonwealth offences with other areas of Commonwealth legislation. Section 476.4 of the *Criminal Code* states that the new offences are not "intended to exclude or limit the operation of any other law of the Commonwealth, a State or Territory." This will probably have the result of leaving any State or Territory laws of similar effect in concurrent force,[7] but could have the effect of, for example, limiting some provisions of the *Copyright Act*.[8]

Definitional issues

Executing a function of a computer

The three crucial actions underlying the offences are unauthorised access, modification or impairment. However the criminality of these actions is limited to:

> "such access, modification or impairment caused, whether directly or indirectly, by the execution of a function of a computer."[9]

Thus, the first prerequisite for any breach of these offences is that the defendant caused the execution of a function of a computer. This term is copied from the *Computer Misuse Act 1990* (UK). Despite its technical nature, the MCCOC Report considered it an important restriction. The MCCOC Report states that the definition is designed to exclude the mere reading of a screen and physical damage to computer hardware (this is left to be dealt with by the general laws of criminal damage to tangible property). But the offences are designed to go beyond the paradigmatic case of keyboard entry. Thus:

> "These offences must extend beyond the obvious cases in which a hacker uses a keyboard or other direct physical means to activate a computer program and cause havoc. They must also cover offenders who cannot be said to 'use a computer' in any normal sense of the words. The wrong done by a saboteur who puts a virus infected disk

[7] See eg *Credit Tribunal; Ex parte General Motors Acceptance Corp, Australia* (1977) 137 CLR 545 per Mason J

[8] The NSW Society for Computers and the Law in its *Submission on Crimes Amendment (Computer Offences) Bill* (http://nswscl.socialchange.net.au/home/crimebill.html) raised a number of concerns about the effect that the offences relating to unauthorised access to data might have on the copyright regime in Australia. They said:

"The practical effect of clause 308H is to criminalise actions which previously were only protected by copyright law (or the laws governing confidential information) and, therefore, only been subject only to a civil sanction. The level of criminality involved in copyright infringements has been the subject of much debate and many submissions to the Commonwealth on modifications to the *Copyright Act* (see sections 116A-116D of the *Copyright Act*). This provision effectively creates a new information protection regime sufficient in its breadth (and in the hands of a sufficiently skilled copyright lawyer) to supplant copyright for practical purposes, but does so without the same level of policy discussion of the role of balancing the public interest against a legislative monopoly. [C]ompare the complex and finely structured application of section 116A of the *Copyright Act* (with its manifold qualifications and exceptions) against the blunt action of 308H."

The issue is an important one, but one that is probably less than it appears. The previous law in fact created a broader criminality. The data now has to be in some way restricted. Also, the criminal law and the civil law have had a long history of being incompatible and while continued incompatibility is to be discouraged it is not rare to see this occur. However, there is a very interesting constitutional point that this raises. If the New South Wales law is in fact incompatible with the Commonwealth copyright laws, s 109 of the Constitution may operate to invalidate the NSW laws to the extent of the inconsistency.

The Society's point remains a strong one, but it is hard to see how it could be easily exploited by intellectual property lawyers, given that prosecutions would be largely in the discretion of the police force and the Director of Public Prosecutions.

[9] *Criminal Code*, s 476.1(2) and *Crimes Act 1914* s 308A(4).

> into circulation, with the eventual effect of destroying or corrupting data held in a computer, is no different in principle from the hacker who obtains access via a communications link. Though the conduct of the saboteur is akin to criminal damage, this conduct obviously belongs in the computer offence provisions."[10]

The definition seems to require that the defendant must do something that results in the computer operating in a manner in which it would not have otherwise operated. To use a mechanical metaphor it must be made to "tick over". But any minimal operation can be enough. The real restriction therefore is in the requirement that the function is of a "computer".

Computer

Somewhat surprisingly, although the term "computer" is used as a central concept throughout the offences, it is not defined. The Report followed the *Computer Misuse Act 1990* model of not defining the term because of the dangers of either not including technological developments in its definition, or alternatively defining the concept too broadly and thereby including many day-to-day items that in some way utilise computer derived technologies.

The report rejected leaving the concept to be a factual issue to be determined by a jury, arguing that "computer" had no ordinary meaning. Instead they intended it to be left as a legal concept to be defined by the courts over time. But their commentary gives an indication of their thinking.

There are many ways which one can "cause a computer to perform a function" which do not require one to do anything which might be described as "using a computer". So, for example, a person who sets off a computer operated burglar alarm causes a computer to perform a function. The mere act of driving a motor vehicle equipped with the most recent electronic control systems might be described as causing a computer to execute a function.

The operations of machines and conveyances are increasingly computerised. So too are environmental and security controls in buildings. If a function is "computerised", recourse to "ordinary meanings" suggests that behind the function one will find a computer. It seems inappropriate, however, to extend the scope of computer crime legislation to include, say, any unauthorised action which might result in "access" to a computerised function of a modern motor vehicle.

It might be suggested that definition of the term "computer" is necessary to limit the scope of prohibitions which will otherwise extend to much conduct which does not merit criminal prosecution. Existing legislation in some jurisdictions makes unauthorised access to a computer a criminal offence. If any electronic data processing device counts as a computer, it will be a criminal offence in these jurisdictions for one child to use another's computer game or pocket calculator without permission.

There are grounds for disquiet when criminal prohibitions extend to trivial misconduct. The problem of over-criminalisation cannot be avoided, however, by adopting a restrictive definition of what is and what is not a "computer". If unauthorised use of another's pocket calculator is too trivial a matter for criminal punishment, exactly the same thing can be said of unauthorised use of another's laptop computer.

The Committee thus recognised that the lack of definition of "computer" raises the problem of potentially criminalising the use of everything from toys to kitchen appliances. The commentary implicitly expresses a hope that judges will take these comments into account in defining computers. But if one looks at the comments closely it appears that their concern is not so much with the technical nature of the computing device but with the use to which it is put. If it is put to a "non-serious" use (from an adult and economic point of view), or if the computing device is merely ancillary to the purpose of another device, the commentary suggests that the property in question not be defined as a "computer". Implicit in the examples would seem to be an economic result-based approach to criminality. Whether this form of analysis is open to the courts in construing the meaning of "computer" is doubtful. The term is likely to be one that the courts will have a great deal of difficulty containing within a restricted boundary. However, the concerns that the Committee expresses about over-criminalisation will no doubt figure greatly in the approach to sentencing that the courts take.

[10] MCCOC Report, n 5, pp 133-134.

The Report is hopeful that the definition of the actual offences will act to diminish the problems the lack of definition of "computer" causes.

The draft provisions proposed by the Committee avoid this particular consequence of the proliferation of computers and computer users. The offences in this part are directed to computer misuse preparatory to the commission of another crime and computer misuse which is comparable to the offence of criminal damage, whether by way of unauthorised modification of data or by defeating security systems. Mere borrowing or use of another's computer or computer data or programs does not fall within the scope of the proposed offences. The report does recommend enactment of a summary offence of unauthorised access to data. The offence is limited, however, to data held in a computer which is protected by a computerised access control system.

However, the following discussion of these offences suggests that the barriers erected are not as strong as the Report suggests. This whole area remains the weakest part of the new laws. The Report encapsulates the concerns:

> "Rapid expansion of the functions assigned to computers has eroded, to an uncertain extent, confidence that the limits of computer crime legislation can be determined [by recourse to ordinary meanings]. The decision to refrain from definition, which seemed reasonable at the beginning of the decade, begins to assume the aspect of an extensive delegation of legislative responsibility to courts…
>
> …The Committee concluded that the scope of the offences cannot be determined by restrictive definition of what is and what is not a 'computer'. The term is left undefined in other contexts of statutory application and, with very few exceptions, submissions to the Committee and expert advice were opposed to definitions which attempt to impose restrictions on the application of the offences: the safest guides to the meaning of 'computer', 'data', 'program' and like terms are to be found in the evolving common understanding of those terms modified, where appropriate, by their statutory context."[11]

There seems to be a real sense in these passages of King Canute's fabled attempt to stop the tide. The Committee does not wish to protect information generally, but cannot define the boundaries it wishes to maintain. The question must be asked, "Why have the restriction at all?" Why not give up the notion that information is not property and enact laws that criminalise access, modification or impairment of information generally? It would seem unprincipled that information that is stored on a piece of paper in a file marked confidential can be read with relative impunity but reading the electronic file from which the document was printed exposes one to criminal penalties. The law has steadily resisted any attempts to create property in information.[12] However the increasing importance of the various forms of intellectual property and electronic transactions are making the insistence that only information contained in specific forms receive legal protection increasingly artificial. Attempts to contain the protection of information within definitions of rapidly evolving technology doom the law to either an endless game of catch-up, or the creation of law with uncertain scope.

Intellectual property laws represent a highly articulated compromise between competing interests that include privacy, freedom of expression, commercial interests and community access. In developing such compromises it is recognised that all these competing interests are legitimate interests. In the criminal law however, the interests of the victims are largely seen to be paramount. As a result, the expansion of criminal liability for access and interference with data has not been subject to the same debates. The degree of dependence modern society places on computer networks appears to have overshadowed the longstanding debates on the role of information and knowledge in society.

The problems of over-criminalisation occur when new criminal laws are not carefully targeted at defined social evils. As the analysis of the specific offences below attempts to show, while at times there is a clear limitation of criminality based on intent or results, there are also significant areas in which no such restrictions exist. Thus the result of the broad definition of data and computer leads to

[11] MCCOC Report, n 4, pp 125 – 129.

[12] See, eg, *Oxford v Moss* (1978) 68 Crim App R 183.

broad swathes of conduct being criminalised without clear justification.

Access, modification and impairment

The execution of a function of a computer, as noted above, is required as a causal element that results in access, modification or impairment. These terms are defined as follows:

"**476.1(1) *Criminal Code* / 308A Crimes Act**

access to data held in a computer means:

(a) the display of the data by the computer or any other output of the data from the computer, or

(b) the copying or moving of the data to any other place in the computer or to a data storage device, or

(c) in the case of a program—the execution of the program.

modification of data[13] held in a computer means:

(a) the alteration or removal of the data, or

(b) an addition to the data.

impairment of electronic communication to or from a computer includes:

(a) the prevention of any such communication, or

(b) the impairment of any such communication on an electronic link or network used by the computer,

but does not include a mere interception of any such communication."

Access and modification are comprehensively defined in this section, with the consequence that any action not falling within these definitions falls outside the relevant offences. "Impairment", by contrast, is defined by inclusion, thereby leaving caselaw to develop extended meanings for the term.

It is important to note that in light of s 476.1(2)/s308A(4) (executing a function of a computer) the notions of access, modification and impairment do not of themselves require any knowledge or intention on the part of the defendant that relates to such access, modification or impairment.[14] This is because both s 476.1(2)/s 308A(4) and the words of all the relevant offences speak of a person who "causes" access/modification/impairment. The terms are therefore merely the objective results of other conduct. Thus, access is the result (following the causing of an execution of a computer function) of either the display or output of information, the copying or moving of the data or the execution of a program. Awareness that this has resulted is not an element of the offences. Similar considerations apply to modification and impairment.

The Report states that the definition of access was not intended to be overly complex, but did not elaborate on the Committee's understanding of the definitions.[15] Its meaning would appear to be a commonsense meaning without any technical requirements.

Modification is defined to include the alteration, removal or addition to data. There is nothing in the definition or Report that explains how permanent such a change must be. In many computer programs, their very operation creates temporary memory files that enable the program to operate. On a technical analysis, such temporary memory files could be seen to be modifications to the data in the computer. It is therefore difficult to see a real difference in many situations between access and modification. That is, unless there is implied into the definition a restriction on modification to only those changes to the data of the computer that are not required or usual in the operation of a program. This ellipsis is important as it might undermine the policy discussed below of restricting the degree of criminality for access to data.

Impairment is a new concept in Australian computer offences and is designed to take into account the emerging forms of interference with networked communications. It requires more than mere interception — these actions are covered by Commonwealth and State interception legislation. Some form of degradation of the communication is presumably required. However, exactly what this constitutes is unknown, as the term is not defined.

[13] The *Criminal Code*, s 476.1(1) uses the phrase "in respect of data".

[14] However, due to the operation of Ch 2 of the *Criminal Code*, and s 5.6 in particular, the Commonwealth offences require proof of separate mental elements for both the physical elements of action and result. See the discussion in relation to s 477.3 below and Leader-Elliott, "Elements of Liability in the Commonwealth *Criminal Code*", (2002) 26 Crim LJ 28.

[15] MCCOC Report, n 4, p 135.

Both inclusive definitions are, if not obvious, then clearly based on a commonsense understanding of the term.

There is Australian case law on the concept, although it largely refers to issues of physical impairment. The term is defined in those terms in number of statutes.[16] The decisions in this area, if they are applicable, would suggest that a merely nominal degradation would not be sufficient, what is required is a noticeable change.[17] There is also some suggestion that there needs to be some form of actual or direct interference.[18]

The Report states that it is intended to apply to "flooding e-mail with input beyond its capacity, resulting in system breakdowns".[19] However, the degree of impairment can be slight or transitory:

> "[It] has an extremely broad band of application, from harms which are transient and trifling to conduct which results in serious economic loss or serious disruption of business, government or community activities. The prohibition would be breached by conduct which impaired communication of a single message of no importance… Once it is accepted that criminal liability should be imposed for intentional impairment of electronic information, conduct which impairs the capacity to receive or transmit that information must similarly fall within the scope of prohibition."[20]

The implications of this statement appear to be quite startling. Note that the offence actually includes reckless impairment so that the offence is even broader than this passage suggests.

Data and communication

The access or modification must then be seen to be to "data held in a computer". Any impairment must be to "electronic communication" to or from a computer.

> "**476.1(1) *Criminal Code* / 308 Crimes Act**
>
> ***data*** includes:
>
> (a) information in any form, or
>
> (b) any program (or part of a program)."

"Data" is a very broad term defined in the Report as encompassing "information in any form, programs or parts of programs, which have been entered into a computer [or] which forms part of the operation system of a computer".[21] There is no requirement that the data be in any way related to the operation of the computer. Throughout the offences data is referred to as being "held" or "contained" in, "entered" into, or "copied" or "moved" to or from a computer or data storage device. There is nothing in these phrases that would require the computer or storage device to be anything more than a conduit or receptacle for the data.

[16] See eg *Medical Practice Act 1992* Dictionary 3: Impairment: "A person is considered to suffer from an impairment if the person suffers from any physical or mental impairment, disability, condition or disorder which detrimentally affects or is likely to detrimentally affect the person's physical or mental capacity to practise medicine. Habitual drunkenness or addiction to a deleterious drug is considered to be a physical or mental disorder."

[17] See eg *Re Erdstein and Comcare* (1991) 24 ALD 382. The concept of impairment is also well known in US constitutional law where Art 1 Sect 10 forbids the passing of laws impairing the obligations of any contract. There it has been held to mean to make worse, to diminish in quality, value, excellence or strength; to deteriorate. However the constitutional nature of the concept has seen the courts hold that not all changes to contracts constitute impairment. See eg *Beaumont v Faubus* (1965) 394 S W 2d 478

[18] See a number of statements in *Minister for Foreign Affairs and Trade v Magno* (1992) 37 FCR 298 which discussed the meaning of the phrase "impairment of dignity" in relation to the protection of premises of diplomatic missions. White crosses had been placed outside the Indonesian embassy as a form of protest but removed by police under pursuant to powers granted under the *Diplomatic Privileges and Immunities (Amendment) Regulations 1992*. Although not directly asked to interpret the phrase French J noted:

"It does not seem that a protest or demonstration conducted outside the premises of a diplomatic mission would by reason of its critical content and mere proximity to the mission amount to an impairment of its dignity. On similar reasoning it would not amount to an attack on the dignity of the relevant diplomatic agent. Whether proximity might give rise to the possibility of impairment of the dignity of the mission or an attack upon the dignity of the agent is another question. But it is difficult to see how the lawful placement of a reproachful and dignified symbol on public land in the vicinity of a mission would amount to a disturbance of its peace or an impairment of its dignity or an attack upon the dignity of its officers." (At 326. See also Gummow J at 303.)

[19] MCCOC Report, n 4, p 137.

[20] MCCOC Report, n 4, pp 171-72.

[21] MCCOC Report, n 4, p 121 Presumably the quoted passage inadvertently omits a disconnecting "or".

"**476.1(1) *Criminal Code* / 308 Crimes Act**

data held in a computer includes:

(a) data entered or copied into the computer,[22] or

(b) data held in any removable data storage device for the time being in the computer, or

(c) data held in a data storage device on a computer network of which the computer forms part."

The use in s 308 of the *NSW Crimes Act* of "entered or copied" rather than "placed" suggests an awareness that electronic transfer of data is accomplished by the copying of data from one place to another, not the complete movement of the original data. The Commonwealth does not have this first limb of the definition.[23] The definition also emphasises that the data need not have any utility in relation to the computer — no purpose is required by the notion of holding.

However, the definition in (c) is highly problematic.

The Report states:

> "Electronic access to data held on the storage device usually requires it to be inserted in a computer. The physical location of the data storage device "in" a computer is a merely incidental feature of much familiar, current technology. Liability for these offences should not be constrained by the physical location of the device. The definition of data held in a computer extends to data in a device located outside the computer, so long as it is electronically accessible by that computer."[24]

The problem is that neither the definition, nor the Report provide any basis for excluding the Internet from this definition.[25] The Internet is clearly a network of inter-linked computers. Thus any data on the internet is defined to be data "held in a computer". This definition could also presumably include any data in any electronic device that a computer connects to, no matter how fleetingly. The very act of connection normally requires communication between the two devices and this, or indeed its potentiality, could be enough to create a temporary network.

That is not to say that the law should not prohibit unauthorised use or manipulation of electronic networks. In fact this is what it should be doing. The problem is that by concentrating on the undefined grey box that is a "computer", transgressions on a network have to be seen counter-intuitively as being held in this box. The reality, increasingly, is that the holding of information is spread throughout many boxes on a network and the computer at the centre of the prosecution's interest is merely being used as an entry point to that data, not as its receptacle. This suggests that further reform of computer crimes are likely to replace the definition of computer with one based on electronic networks, the computer becoming the residual term.

"**476.1(1) *Criminal Code* / 308 Crimes Act**

data storage device means any thing (for example a disk or file server) containing or designed to contain data for use by a computer.

electronic communication means a communication of information in any form by means of guided or unguided electromagnetic energy."

Both "electronic communication" and "data storage device" definitions are sourced from the *Electronic Transactions Act 1999*. The Explanatory Memorandum to the *Electronic Transactions Bill* stated:

> "Data storage device is defined to mean any article or material from which information is capable of being reproduced with or without the aid of any other article or device. This definition is intended to include items such as computer disks and CD ROMs from which information can be accessed or retrieved with the aid of appropriate devices. It is not intended to include items such as filing cabinets, books and newspapers. This definition should be interpreted in the context in which it is used — that is, as a

[22] The Commonwealth definition of "data held in a computer" eschews the specific inclusion of "data entered or copied into the computer".

[23] This might cause problems if the courts interpret "held" to have a more than transitory meaning. For example, if a person is monitoring a stream of data flowing through a computer, such data may not be held in the computer. However it is not likely to arise as a practical issue on the basis that such data is likely to have originated from another computer and could be seen to be held there.

[24] MCCOC Report, n 4, p 121.

[25] In fact, the Report expressly eschews any attempt to define the concept of a network (MCCOC Report, n 4, p 129-130).

> law dealing with the electronic communication of information…
>
> Electronic communication is defined as a communication of information by means of guided and/or unguided electromagnetic energy … The definition is consistent with similar definitions of electromagnetic energy in the *Telecommunications Act 1991* and *Telecommunications Act 1997*, and is intended to have the widest possible meaning. Communications by means of guided electromagnetic energy is intended to include the use of cables and wires, for example optic fibre cables and telephone lines. Communications by means of unguided electromagnetic energy is intended to include the use of radio waves, visible light, microwaves, infrared signals and other energy in the electromagnetic spectrum. The use of the term unguided is not intended to refer to the broadcasting of information, but instead means that the electronic magnetic energy is not restricted to a physical conduit, such as a cable or wire. The term communication should also be interpreted broadly. Information that is recorded, stored or retained in an electronic form but is not transmitted immediately after being created is intended to fall within the scope of an electronic communication."

The concept of data storage device is an enormously broad one. It is odd, and a little worrying, that in the *Electronic Transactions Act* this problem was recognised but dealt with only by means of an attempt in the Explanatory Memorandum to instruct the courts to read down its meaning. The same problem therefore applies to the computer crime area. Thus, for NSW, the interpretation of the concept is derived from a reference in a law reform Report to a passage in an Explanatory Memorandum to a different, and non-criminal Bill from another jurisdiction. It is to be hoped that New South Wales courts are willing to follow this torturous path in their interpretation of the new laws. It would have been far better to attempt to include the restriction in the definition.

"Electronic communication" only occurs in these offences as part of the phrase "electronic communication to or from a computer", thus lessening the otherwise extremely broad definition. It seems clear that the intent is to use an expression that is technology neutral and is capable of including all forms of electrical transmission. However, as discussed, the lack of definition of computer leaves its exact scope uncertain.

Unauthorised access, modification or impairment

The final external element of the offences is that such access, modification or impairment be unauthorised. The MCCOC Report version, adopted by NSW is as follows:

> "**308B Meaning of unauthorised access, modification or impairment**
>
> (1) For the purposes of this Part, access to or modification of data, or impairment of electronic communication, by a person is ***unauthorised*** if the person is not entitled to cause that access, modification or impairment.
>
> (2) Any such access, modification or impairment is not unauthorised merely because the person has an ulterior purpose for that action.
>
> (3) For the purposes of an offence under this Part, a person causes any such unauthorised access, modification or impairment if the person's conduct substantially contributes to the unauthorised access, modification or impairment."

The Commonwealth provisions are more tightly linked to the actual offences, though to the same effect:

> "**476.2 Meaning of unauthorised access, modification or impairment**
>
> (1) In this Part:
>
> (a) access to data held in a computer; or
>
> (b) modification of data held in a computer; or
>
> (c) the impairment of electronic communication to or from a computer; or
>
> (d) the impairment of the reliability, security or operation of any data held on a computer disk, credit card or other device used to store data by electronic means;
>
> by a person is unauthorised if the person is not entitled to cause that access, modification or impairment.

(2) Any such access, modification or impairment caused by the person is not unauthorised merely because he or she has an ulterior purpose for causing it.

(3) For the purposes of an offence under this Part, a person causes any such unauthorised access, modification or impairment if the person's conduct substantially contributes to it."[26]

The lack of authority is a crucial restriction on the offences' scope. The motivation of the person in accessing, modifying or impairing the data is again not relevant. What is relevant is the question of their authorisation. The common law issues of consent thus reappear in the statutory formula.

The High Court has held in *Kennison v Daire*[27] that a computer cannot give consent. Kennison had a cheque account and Easybank card with the Savings Bank of South Australia. Following the closure of his account he fraudulently used the card to withdraw $200 from a computerised automatic teller machine (ATM) in circumstances where he knew he had no right to the money. The ATM paid him the money because it was off-line and programmed to dispense up to $200 cash to anyone correctly entering a card's personal identification number (PIN). Kennison was charged with simple larceny. His defence was that the bank, through its programming of the computer consented to the passing of property in the money. The High Court held:

"The fact that the bank programmed the machine in a way that facilitated the commission of a fraud by a person holding a card did not mean that the bank consented to the withdrawal of money by a person who had no account with the bank… The machine could not give the bank's consent in fact and there is no principle of law that requires it to be treated as though it were a person with authority to decide and consent. The proper inference to be drawn from the facts is that the bank consented to the withdrawal of up to $200 by a card holder who presented his card and supplied his personal identification number, only if the card holder had an account which was current. It would be quite unreal to infer that the bank consented to the withdrawal by a card holder whose account had been closed."

Thus any taking of property by means of a computer can be assumed to be without consent unless evidence of consent by the owner of the property can be otherwise established. Unfortunately this decision by the High Court was extremely brief and did not seem to appreciate the complex factual issues that surround the intention of persons who program and use automated computer systems – particularly in large scale networks.[28] Thus the breadth of the precedent is in some ways uncertain.

However it would seem to be the law that the use of a computer without the express permission of the owner of that computer is unauthorised. This is because, as the High Court held, a computer cannot give consent and in the absence of evidence of any such consent by the owner of the computer, lack of authorisation would be inferred. This makes sense when one is considering an outsider hacking into a private computer system, though it is more contestable in circumstances where some forms of outsider access are permitted and encouraged.

In cases involving "insiders" however, it is critical to determine the extent of the authorisation. In *Gilmour*[29] the concept of authority was held to be by default a general authority to access data for any purpose. However, if the authority was given for a particular purpose, then any access for any other purpose was an unauthorised access to data. In so holding, an analogy was drawn with the law of

[26] The *Criminal Code* also contains provisions excluding from liability persons acting under warrants and Government security agency officers. Such provisions are beyond the scope of this article.

[27] (1986) 160 ALR 129.

[28] The High Court's approach has not been the only approach courts have taken. Compare the differences of opinion between the decisions in *Kennison v Daire* (1985) 38 SASR 404; *Evernett* [1987] 2 Qd R 753; *Mujunen* [1994] 2 Qd R 647 and *Townsend v Doyle and Paynter* (unreported Supreme Court of Western Australia 3 December 1992, No 1125 and 1126, 1992); and cf the approach taken in *Baxter* [1988] 1 Qd R 537.

[29] (1995) 134 ALR 631. Gilmour was employed to enter data into the Australian Tax Office computers, including entering the "43" code to signify that a taxpayer had been granted a relief from payment of income tax. In 19 cases Gilmour entered a "43" code without any determination by an appropriate officer that relief should be granted. He did this because of "a desire to expedite the process, a heavy workload and concern about suggested inconsistencies in determinations of applications for relief". See also *Murdoch* (1993) 1 VR 406.

trespass.[30] The court also noted that in light of the High Court's decision in *Kennison v Daire*, the authority could not come from the fact that the computer permitted access. Such authority had to come from human actors or published procedures. This approach is considered by the MCCOC Report to be consistent with the new definitions.[31]

Ulterior motives

The new offences do, however, result in a significant clarification and reduction of the applicability of the offences to persons who are authorised to access, etc data but who do so for ulterior purposes. The MCCOC Report noted:

> "Should individuals who are authorised for one purpose be guilty of an offence under this Part if they act for another, ulterior purpose? Liability should certainly be imposed if the original authorisation was obtained by deception as to the offender's purposes. It does not follow, however, that liability should be imposed when authorisation was obtained without fraud and the defendant misuses the authorisation. The issue is clearly contentious. As the Victorian case of *DPP v Murdoch* indicates, there is an analogy, which some authorities have found persuasive, with current definitions of the offence of burglary, which would extend the offence to a person who enters a Department store with the intention of shoplifting. In its discussion and recommendations on the offence of burglary, the Committee has taken the view that entry pursuant to permission should not be trespassory, even though accompanied by an intention to steal or commit another offence: [Chapter 3: *Theft, Fraud, Bribery and Related Offence*s, Final Report, December 1995, s16.3(2) and commentary, pp 83-89]…
>
> It should be noted, at the outset, that the issue is unlikely to arise in the offences which prohibit unauthorised modification of data and unauthorised impairment of electronic communications. When breach of those provisions is charged, the issue is whether some particular modification or instance of impairment is authorised. If the modification or impairment is authorised, the private motives of the individual involved will rarely if ever provide cause for concern. The issue of ulterior motivation is most likely to arise when the offence of unauthorised *access* with intent to commit a serious offence is charged. It is also likely to arise, of course, when the summary offence of unauthorised access to restricted data is charged."

Such a clarification is important in that ensures a concentration on the degree of actual authorisation explicitly given to the defendant and does not permit a reliance on less well defined notions of what constitute appropriate motives. No problems will arise if persons are given authorisations that are linked to specific purposes or procedures, as was the case in *Gilmour*.

To permit a motive-based approach to the notion of authority would have been to concentrate on the ultimate aim of the defendant, not on the access. These offences are access, modification and impairment offences. Motivations that involve criminal intents are more appropriately prosecuted as such, not as computer access offences.

Knowledge, intent and recklessness

In New South Wales these are still terms defined by common law. The exact extent of intent is not entirely clear for crimes of this sort but it can include not only an intention to bring about the result by the defendant's own actions or omissions but also circumstances where the result is one that the defendant foresaw would be the inevitable consequence of their actions — even if this was not their purpose.[32]

The mental elements at Commonwealth level are now defined by the *Criminal Code*. Section 5.2 defines intention as:

> "(1) A person has intention with respect to conduct if he or she means to engage in that conduct.
>
> (2) A person has intention with respect to a circumstance if he or she believes that it exists or will exist.
>
> (3) A person has intention with respect to a result if he or she means to bring it about or is aware that it will occur in the ordinary course of events."

[30] The court referred to *Barker* (1983) 153 CLR 338.

[31] MCCOC Report, n 4, p 145.

[32] *Hyam* [1975] AC 55.

In including awareness that a result will occur "in the ordinary course of events", the Commonwealth definition appears broader than a requirement that the result be "inevitable".

At common law, knowledge requires an actual belief in the truth of facts,[33] and as all the offences require knowledge that access, etc is unauthorised a claim of right defence is open on the basis of a mistaken belief that the defendant had authority. The Commonwealth definition appears in s 5.3:

> "A person has knowledge of a circumstance or a result if he or she is aware that it exists or will exist in the ordinary course of events."

Presumably, to be told of circumstances and to disbelieve the account would not be to be "aware" of the circumstances.

The summary, preparatory and ancillary offences all require knowledge and intent. However, the two main offences of modification of data and impairment of communication do not require intent. Instead knowledge and recklessness suffice as the mental elements. As Ian Leader-Elliott explains,[34] recklessness is the core mental element of the new offences.

In *Pemble*[35] Barwick CJ defined recklessness:

> "Recklessness…involves foresight of or, as it is sometimes said, advertence to, the consequences of the contemplated act and a willingness to run the risk of the likelihood, or even perhaps the possibility, of those consequences maturing into actuality. This aspect of recklessness entails an indifference to a result of which at least the likelihood is foreseen. An awareness of the consequences of the contemplated act is thus essential."

The leading cases on recklessness largely deal with murder or assault and Barwick CJ's description has been confined in some respects, notably in relation to the need for the consequences to be seen to probable and not just possible.[36] It is therefore uncertain as to the exact scope of recklessness for these offences. However, as the offences will often involve the setting in course of a chain of events it is likely that the courts will be willing to apply the broader definition outlined by Barwick CJ in *Pemble*.

The Commonwealth offences are based on the definitions in the *Criminal Code*. Recklessness is defined in s 5.4 of the *Code* including the following:

> "(2) A person is reckless with respect to a result if:
>
> (a) he or she is aware of a substantial risk that the result will occur; and
>
> (b) having regard to the circumstances known to him or her, it is unjustifiable to take the risk.
>
> (3) The question whether taking a risk is unjustifiable is one of fact.
>
> (4) If recklessness is a fault element for a physical element of an offence, proof of intention, knowledge or recklessness will satisfy that fault element."

The *Criminal Code* definition represents a middle road between the possibility and probability options. It is beyond the scope of this article to examine the implications of the need for prosecutions to prove concepts such as substantial and unjustifiable in relation to computer offences, but it is likely to generate a degree of caselaw.

The offences

The summary offences

Unauthorised access or modification

This offence is the basic offence under the new law. There is no need to prove an intent to affect the data or its use, the act of causing access or modification is sufficient. The offence is therefore a summary offence with the lowest of the penalties in this part. The NSW offence is worded as follows:

> "**308H Unauthorised access to or modification of restricted data held in computer (summary offence)**
>
> (1) A person:
>
> (a) who causes any unauthorised access to or modification of restricted data held in a computer, and
>
> (b) who knows that the access or modification is unauthorised, and

[33] *Raad* [1983] 3 NSWLR 344.

[34] Leader-Elliott, "Elements of Liability in the Commonwealth *Criminal Code*", (2002) 26 Crim LJ 28.

[35] (1971) 124 CLR 107.

[36] See *Crabbe* (1985) 156 CLR 464 and the discussion in Bronitt and McSherry, *Principles of Criminal Law*, (LBC 2001) pp 181 – 184.

(c) who intends to cause that access or modification, is guilty of an offence.

Maximum penalty: Imprisonment for 2 years.

(2) An offence against this section is a summary offence.

(3) In this section:

restricted data means data held in a computer to which access is restricted by an access control system associated with a function of the computer."

The Commonwealth offence in s 478.1 of the *Criminal Code* is to similar effect,[37] other than in its definition of restricted data, which is discussed below.

While previous NSW and Commonwealth law was heavily based on the prohibition of unauthorised access, the new legislation downgrades the restrictions on unauthorised access from an indictable to a summary offence. Importantly, the new unauthorised access crime is now confined to access to restricted data.

Under the previous Commonwealth and NSW offences unauthorised access to any data was prohibited by minor offences,[38] and other more serious offences prohibited unauthorised access to an express list of information.[39] In NSW that list included:[40]

- confidential government information in relation to security, defence or inter-governmental relations; or
- the existence or identity of any confidential source of information in relation to the enforcement or administration of the law; or
- the enforcement or administration of the criminal law; or
- the maintenance or enforcement of any lawful method or procedure for protecting public safety; or
- the personal affairs of any person (whether living or deceased); or
- trade secrets; or
- records of a financial institution; or
- information (other than trade secrets) that has a commercial value to any person that could be destroyed or diminished if disclosed.

The MCCOC Report indicated that the use of computer access crimes to criminalise what amounted to invasions of government, business and personal privacy was inappropriate.

Instead, the concept of "restricted data" introduces an era of laisser faire into computer protection. It will now be up to individuals to take preventative measures to secure sensitive information. If the data is not protected by an "access control system" then there is no crime in any form of unauthorised access or modification (provided that the modification does not breach s 477.2/s 308D or the access or modification is not in order to commit a serious indictable crime: s 477.1/s 308C). There is also the requirement that the access system be associated with the computer. Thus a lock on the room that the computer is in might not be seen to be an access control device.

The meaning of "access control system" however remains moot. The concept would involve all password protected files, programs and web-sites. But as almost all computers now involve an initial logging on stage when booting, it is problematic as to how far the definition extends. Does the definition require that the act of causing a computer function that accesses the data to have to pass through an access control system, or can the mere existence of such a system on the computer as a whole satisfy the definition?[41]

A strict reading of the definition suggests that this is not restricted data because access to that data *specifically* was not restricted. This would appear to be the intent of the legislation. It is unfortunate that the restricted meaning is not made clear in the definition.

[37] Unless there are major differences, only the NSW provisions are be quoted. This is because the Commonwealth provisions also contain jurisdictional subsections within each offence.

[38] *Crimes Act 1900* (NSW), s 309(1) and 309(2); *Crimes Act 1914* (Cth), s 76B(1) and s 76B(2)(a).

[39] *Crimes Act 1900* (NSW) s 309(3) and 309(4); *Crimes Act 1914* (Cth) s 76B(2)(b) and 76B(3).

[40] The Commonwealth list was similar, but not identical.

[41] For example, imagine that a library has computer terminals that are available for public use. The terminal's operating system and internet connection require a password to be entered – which is done by library staff each day. A patron discovers that because the terminal is linked to the library's databases she can access the personal records of borrowers without a password (because the initial start-up password gives general access). If she thus accesses the information has she accessed restricted data.

The problems of the wording of the definition of restricted data were recognised by an amendment to the Commonwealth *Cybercrime Bill*. As a result the Commonwealth offence now defines it in s 478.1 as follows:

"restricted data means data:

(a) held in a computer; and

(b) to which access is restricted by an access control system associated with a function of the computer."

This new definition makes it clear that the access control system relates to the actual data being accessed, not more generally to the computer.

It must also be proved that the person not only gained access but that they both knew they were unauthorised to do so and also intended to gain unauthorised access. This is more restricted than the previous offence under the then s 76B *Crimes Act* (Cth)/s 309(1) *Crimes Act* (NSW) in that that offence only required an intent to gain access. This offence makes it clear that a person is not in breach of the offence if they are unaware that they are unauthorised. This may also contain within it a defence of claim of right, in that the person believed that they had authority.

The need to prove knowledge of lack of authority is crucial. Following the decision in *Kennison v Daire* it seems unlikely that one can presume authorisation has actually been granted if a computer system permits access. Thus the default position is that access to most computers cannot be assumed to be with consent. However, despite this approach by the courts, the test will be one of subjective belief. Thus, for example, if a website, through a flaw in its server's set-up, permits access into private files not intended to be accessed by the public, such access would be unauthorised. However the lack of a restriction on entry and the apparent ease of entry might permit a belief that such entry was authorised and therefore no crime would be committed.

A further change in the new law is the fact that the previous offence in s 76B(3) *Crimes Act 1914* (Cth)/s309(4) Crimes Act (NSW) of continuing to examine data after an unauthorised access has not been replicated in this offence. Thus there is no penalty clock ticking on the amount of time spent viewing data accessed. Once the access has been made no further criminal actions occur unless there is modification or impairment.

This also raises the question of whether access is a continuing offence. If it is not, then as long as a person innocently accesses the data, that person does not commit an offence if they subsequently decide to view it, with the realisation that this viewing is unauthorised.

As access and modification are in the alternative it is likely that the emphasis will be on the unauthorised access. However the alternative of modification will be a useful way of avoiding issues over the extent of authority to access certain areas of computer systems by employees. While it may in some cases be arguable that the access was permitted, any alteration of data without express authority may be easier to prove.

The offence also constitutes a measured reduction in the severity of the previous s 76C/s 310. This section made it an offence punishable by 10 years' imprisonment to alter data without authority. The new offence recognises that sometimes the alteration of the data may not be intended to lead to any practical detriment. If the alteration is intended to lead to an impairment of the data then the person can be charged under s 477.2/s 308D. Otherwise the appropriate offence is the summary one in s 478.1/s 308H.

Unauthorised impairment of data held in a data storage device

The NSW version of the offence is as follows:

"**308I Unauthorised impairment of data held in computer disk, credit card or other device (summary offence)**

(1) A person:

(a) who causes any unauthorised impairment of the reliability, security or operation of any data held on a computer disk, credit card or other device used to store data by electronic means, and

(b) who knows that the impairment is unauthorised, and

(c) who intends to cause that impairment,

is guilty of an offence.

Maximum penalty: Imprisonment for 2 years.

(2) An offence against this section is a summary offence.

(3) For the purposes of this section, impairment of the reliability, security or operation of data is ***unauthorised*** if the person is not entitled to cause that impairment."[42]

Section 478.2 of the *Criminal Code* is to similar effect. However, as this offence does not relate to communication the Commonwealth offence only relates to computer disks, credit cards and other devices owned or leased by Commonwealth entities.

This offence is intended to extend liability for actions that affect data beyond the confines of computer networks. In attempting to create a catch-all summary offence for this the net has been thrown extremely widely.

It does not require the execution of a function of a computer and thus extends to surrounding physical actions. In this sense it overlaps physical damage offences and includes not only the erasing of data from a disk by waving a magnet near it but also to the physical destruction of the disk.

But again the prosecution will need to show that the impairment was unauthorised and in addition that the defendant both intended the impairment and knew that the impairment was unauthorised. The meaning of impairment of reliability, security or operation is discussed in relation to s 477.3/s 308D.

The preparatory offences

These offences are in many ways the most controversial aspect of the new offences. The offences in s 478.3/s 308F and s 478.4/s 308G prohibit the possession, production, supply or obtaining of data with the intention of committing a serious computer offence.

Serious computer offence

"**308 General definitions**

In this Part:

serious computer offence means:

(a) an offence against section 308C, 308D or 308E, or

(b) conduct in another jurisdiction that is an offence in that jurisdiction and that would constitute an offence against section 308C, 308D or 308E if the conduct occurred in this jurisdiction."

Initially, the NSW Bill referred to computer offences in this Part generally. However, it was amended to refer to the indictable offences only. This makes clear that the preparatory offences only apply if the prosecution can prove an intent to commit an indictable offence — not the summary offences in s 308H and 308I. Similarly, the Commonwealth offences are restricted to intents to commit or facilitate the offences in Division 477 (the indictable offences).

The extended definition in (b) criminalises any action done by any person anywhere in the world that falls within the definition of the local offences. The crucial limitation apart from issues of enforcement is the need to prove that the actions would have constituted a crime in the other jurisdiction. The effect is a lowest common denominator approach[43] to international cybercrime. One can only be convicted if the actions in question are preparatory or ancillary to actions which are criminal in both jurisdictions.

One limitation may be the use of the word "conduct" in defining serious computer crime. The extended definition appears to cover situations such as the possessing of data that is then transmitted to another jurisdiction where another person commits an offence with that data. However it is uncertain, under the NSW offences, whether the actions by means of a computer in this jurisdiction that cause unauthorised modification to a computer in another jurisdiction could constitute conduct in that other jurisdiction sufficient to constitute an offence. This uncertainty arises because "conduct" is not defined.

The Commonwealth *Code* by contrast defines conduct in para 4.1(2) to mean "an act, an omission to perform an act or a state of affairs." The concept of a "state of affairs" does not appear to require any direct action by the defendant. Thus the Commonwealth offences are unlikely to be restricted by arguments over the definition of conduct.[44]

[42] Section 308I(3) appears to have been enacted by mistake. In the MCCOC Report it appears because the summary offences are designed to be able to be enacted in separate legislation.

[43] This is in the sense that if other jurisdictions adopt a similar approach the applicable laws will be those of the jurisdiction with the least degree of restriction on the relevant conduct.

[44] In light of the common law's difficulty with the concept of "act", the breadth of the definition of conduct may give rise to equally complex and unforeseen extensions of liability in some

In circumstances where the defendant, in NSW commits all the conduct necessary to cause a prohibited result in another jurisdiction (such as causing a computer to crash), they may still be found guilty by means of s 10C of the Crimes Act:

"**10C Extension of offences if there is a geographical nexus**

(1) If:

(a) all elements necessary to constitute an offence against a law of the State exist (disregarding geographical considerations), and

(b) a geographical nexus exists between the State and the offence,

the person alleged to have committed the offence is guilty of an offence against that law.

(2) A geographical nexus exists between the State and an offence if:

(a) the offence is committed wholly or partly in the State (whether or not the offence has any effect in the State), or

(b) the offence is committed wholly outside the State, but the offence has an effect in the State."

It would therefore appear that as long as the offence is partly committed in NSW there is jurisdiction. This section is however the result of a tortured reform process and its application remains to be finally confirmed.[45]

Possession, production, supply or obtaining of data with intent to commit serious computer crime

The NSW provision is as follows:

"**308F Possession of data with intent to commit serious computer offence**

(1) A person who is in possession or control of data:

(a) with the intention of committing a serious computer offence, or

(b) with the intention of facilitating the commission of a serious computer offence (whether by the person or by another person),

is guilty of an offence.

Maximum penalty: Imprisonment for 3 years.

(2) For the purposes of this section, ***possession or control of data*** includes:

(a) possession of a computer or data storage device holding or containing the data or of a document in which the data is recorded, and

(b) control of data held in a computer that is in the possession of another person (whether the computer is in this jurisdiction or outside this jurisdiction).

(3) A person may be found guilty of an offence against this section even if committing the serious computer offence concerned is impossible.

(4) It is not an offence to attempt to commit an offence against this section.

308G Producing, supplying or obtaining data with intent to commit serious computer offence

(1) A person who produces, supplies or obtains data:

(a) with the intention of committing a serious computer offence, or

(b) with the intention of facilitating the commission of a serious computer offence (whether by the person or by another person),

is guilty of an offence.

Maximum penalty: Imprisonment for 3 years.

(2) For the purposes of this section, ***produc***e, ***supply or obtain data*** includes:

(a) produce, supply or obtain data held or contained in a computer or data storage device, or

(b) produce, supply or obtain a document in which the data is recorded.

(3) A person may be found guilty of an offence against this section even if committing the serious computer offence concerned is impossible."

The Commonwealth provisions (s 478.3 and 478.4 of the *Criminal Code*) are to similar effect subject to the difference noted below.

offences.

[45] See the commentary in the Report in the section *Amendment to Chapter 2: Jurisdiction;* MCCOC Report, n 4.

These offences are extremely broad offences and relate to the preparation to commit the following indictable offences. Producing, supplying and obtaining data all require the prosecution to prove an action by the defendant in relation to the data. The offence of mere possession or control does not. The offence in s 478.4/s 308G then appears to fall entirely inside s 478.3/s 308F, as it is difficult to imagine a circumstance in which one could produce, supply or obtain data without it being at some point in that person's control. Thus the fact that one cannot be convicted of attempting to control data under the NSW s 308F offence sits oddly with the fact that one can be convicted of attempting to obtain data (even if this is impossible to do) under s 308G. This problem has been recognised by the Commonwealth in s 478.4 which enacts that it is not an offence to attempt to commit an offence under s 478.4.

It is likely that most prosecutions will be run under s 478.4/s 308G in that the method used in producing, supplying or obtaining the data is likely to provide evidence of the intention to commit the serious computer offence. One would only bother with s 478.3/s 308F if the person were found to have the data in their control with no evidence of how that data was obtained.

This highlights the concerns that some have about the scope of these offences, in that they contain minimal external elements. While s 478.4/s 308G requires intentional actions in the movement of the data into or out of the defendant's control, no such requirement exists for s 478.3/s 308F.

The concepts of possession and control raise some further concerns. The NSW Society for Computers and the Law in their *Submission on Crimes Amendment (Computer Offences) Bill*[46] argued that possession should exclude mere knowledge and be limited to tangible forms. They argued that this was consistent with the MCCOC Report's commentary on the section and that the proposed sections should refer to "possession or control of data in a tangible form." However possession of a program designed to hack into a secure site, written and stored at all times only in digital form, is not data in a tangible form. It is data reducible to tangible form.

In fact it is the very lack of any tangible nature of data which necessitates the computer offences legislation. Data is merely information – but then so is human memory. If it passes through a computer it falls within these sections. If it is in some other form, or merely in the mind of the perpetrator it is not a computer offence.[47] The arbitrary nature of this distinction has already been noted, and the desire to limit the scope of the offences is well founded. But a reintroduction of notions of tangibility contradicts the whole rationale of the offences.

Possession is a term that can only refer to tangible property. Thus the extended definitions of "possession…of data" make it clear that possession only applies to the possession of the physical container of the data. "Control" is the concept that will apply to the data itself. It is unfortunate that the legislation does not define this concept, given the range of meanings that can be ascribed to the concept.[48] The old possession issues may re-emerge in the digital era. For example, does control require exclusive control? Is data in my control if I leave it on an open access website? Presumably the answer is yes, as I alone can edit or remove the data, though others can copy it. However if I leave the data on a computer I share with others and do not password protect access, editing and deleting of the data, is it in my control? Is it also in my control if someone places the data on my computer and I have access, editing and deletion rights to it?

There is also no need to prove that the data be in any way malicious or necessarily collated for a particular purpose. This is because it would be impossible to do so. It is not possible, for example, to restrict the offence to malicious data. Many passwords use ordinary English words and data in its basic form is merely a collection of 1s and 0s. It

[46] http://nswscl.socialchange.net.au/home/crimebill.html

[47] It may be possible to read into the concept of data, when compared to information, a requirement that the possession be in some way separate from the defendant. Thus, if the information is known to the defendant, the defendant is informed but, if they have the information in some external form, they possess data. This is drawing a long and pedantic bow. It seems unlikely that the computer offences would be used to prosecute a person for reading restricted information.

[48] See, eg, the comments of Gibbs ACJ in *Federal Commissioner of Taxation v Australia and New Zealand Banking Group Ltd.* (1979) 143 CLR 499.

is therefore impossible to characterise data as either harmful or harmless. The criminality lies in the intended use of the otherwise harmless data.

A successful prosecution under these sections will therefore be based almost entirely on proof of the intent to commit or facilitate a computer crime.[49] However, the elements of these offences are reasonably specific and the prosecution would need to prove the intention in relation to all the required elements. This can be contrasted with the broader forms of intent necessary to prove conspiracies. They are nevertheless inchoate offences and open to all the criticisms that these offences engender.

The indictable offences

Modification of data

"**308D Unauthorised modification of data with intent to cause impairment**

(1) A person who:
  (a) causes any unauthorised modification of data held in a computer, and
  (b) knows that the modification is unauthorised, and
  (c) intends by the modification to impair access to, or to impair the reliability, security or operation of, any data held in a computer, or who is reckless as to any such impairment,

  is guilty of an offence.

  Maximum penalty: Imprisonment for 10 years.

(2) A conviction for an offence against this section is an alternative verdict to a charge for:
  (a) an offence against section 195 (Maliciously destroying or damaging property), or
  (b) an offence against section 308E (Unauthorised impairment of electronic communication)."

The Commonwealth provision is more economical. On the basis that recklessness is a lesser fault element than intention, only recklessness is used as an element. As the offence relates to the reckless attitude of the defendant, rather than the result, the Commonwealth provision makes this clear.

"**477.2 Unauthorised modification of data to cause impairment**

(1) A person is guilty of an offence if:
  (a) the person causes any unauthorised modification of data held in a computer; and
  (b) the person knows the modification is unauthorised; and
  (c) the person is reckless as to whether the modification impairs or will impair:
    (i) access to that or any other data held in any computer; or
    (ii) the reliability, security or operation, of any such data; …

  Penalty:10 years imprisonment.

  …

(3) A person may be guilty of an offence against this section even if there is or will be no actual impairment to:
  (a) access to data held in a computer; or
  (b) the reliability, security or operation, of any such data."

Many of the elements in this offence have already been discussed. It follows the same logical path as the summary offence of unauthorised modification of data in s 478.1/s 308H. The distinction from that offence occurs in two ways. Firstly the data that is modified can be any data — there is no requirement that it be behind an access control system. The second difference relates to the mens rea. In this offence there must be an intention to cause some form of harm, or be reckless as to the effect of the modification. It is this difference that appears to make the offence serious enough to be indictable.

Note however that the section does not require that any harm actually be caused. The essential distinction between this offence and s 478.1/s 308H is not based on result, but on intent. The external elements are the same.

[49] Even if data controlled was to be restricted to a particular class of data (such as programs designed to hack into systems or viruses), the essence of the offence would remain an intent to commit a serious computer offence.

The distinction between this offence and criminal damage

The NSW offence is also an alternative to criminal damage under s 195 (such an alternative is not expressed in the Commonwealth provisions). It may be asked why this is so. In *Whitely*[50] the English Court of Appeal held that modification of stored data could constitute criminal damage because this involved the microscopic rearrangement of magnetic particles on the storage medium. The MCCOC Report considered that the law should avoid such a reductionist analysis and that the law should operate on a more practical and commonsense basis. Hence the enactment of a modification offence.[51] However the malicious damage verdict remains open in NSW as an alternative. That offence is as follows:

"**Maliciously destroying or damaging property**

195. A person who maliciously destroys or damages property belonging to another or to that person and another is liable:

(a) to penal servitude for 5 years; or

(b) if the destruction or damage is caused by means of fire or explosives, to penal servitude for 10 years."

There are three points to note here. The first is the inconsistency in sentencing that this produces where a modification of data in a computer is considered to be of the equivalent criminality as the use of explosives or fire. The second point is that s 195 requires that the damage be caused maliciously. Maliciously is defined in s 5, and has had a long and unhappy history of criticism. However for the purposes of this section it suffices to say that maliciously requires either intention or recklessness. The consequence is that the mental elements of the two offences are similar.

The third point is that under s 195 it must be shown that the property belongs to another, including partially. This does not require proof of ownership but it does require that the property be in the other person's control or possession. Section 308D does not have this requirement. There are a number of reasons why such a requirement would be counterproductive when dealing with data in a computer. Whether data is in fact under the control of a person might be difficult to prove in an open access network environment. Further the defendant might in any event be the owner of the computer in which the data is held and any issues of control or ownership are likely to muddy the waters.

The issue of control does however play an important role in s 477.2/s 308D. This is because the modification must be unauthorised. The lack of authority implies that another person is asserting control over the data.

The narrowed scope of the new provisions

As mentioned above, the previous offence enacted:

"**Damaging data in computer**

310. A person who intentionally and without authority or lawful excuse:

(a) destroys, erases or alters data stored in or inserts data into a computer; or

(b) interferes with, or interrupts or obstructs the lawful use of a computer,

is liable to penal servitude for 10 years, or to a fine of 1,000 penalty units, or both."[52]

That offence had the effect of criminalising any action which involved unauthorised but otherwise innocent addition or alteration of data or any action interrupting the use of a computer. It extended to such activities as accidentally saving data to the wrong area of a computer or mistakenly switching off the mains power to building housing a computer. The new legislation removes this catch-all offence and adds to the general intentions to do actions a requirement of recklessness as to those actions, in circumstances where the results could be detrimental. Further the new offences relate solely to data in computers not the physical use of terminals. Such obstruction is easily dealt with under the criminal damage offences.[53]

Impairing access, reliability, security or operation

Thus the crucial element of the new offence is the need to prove the defendant was reckless as to

[50] (1991) 93 Cr App R 25.

[51] MCCOC Report, n 4, pp157-58.

[52] The previous Commonwealth legislation was to similar effect: *Crimes Act 1914* (Cth), s76B(3).

[53] There is authority that damage extends to the "temporary functional derangement" of property (in this case, the squashing of a policeman's hat) *Samuels v Stubbs* (1972) 4 SASR 200.

causing the results of impaired access, reliability, security or operation of the data. Note that the offence does not require the actual impairment, merely recklessness in relation to its occurrence is required. The MCCOC Report points out that this is designed to cover situations such as the planting of logic bombs — where the impairment only occurs following another event and may never eventuate.[54]

The notion of access has already been discussed. Presumably impairing of access relates to conduct such as the altering or imposition of access control systems. It could also extend to an intention to slow access, such as by the reckless overtaxing of the computer on other tasks. Reliability, security and operation however are terms that are not defined or discussed by the MCCOC Report.

Reliability it would seem refers to a discrepancy between the usual meaning or interpretation an accessor would give to the data and its real import. However, data in itself is neither reliable nor unreliable. It just is.[55]

The problem can be illustrated by the facts of *Attorney General's Reference No 1 of 1991* [1993] QB 94. There a sales assistant was preparing a sale document for equipment that the defendant was purchasing. When the sales assistant moved away to check some information, the defendant entered a code which resulted in the computer giving him a discount to which he was not entitled. Under s 477.2/s 308D there could only be an offence if it was shown that there was an intent to impair the reliability of the data in the computer.[56] It may be stretching the concept of reliability to place these facts within the offence. The addition of the code does not affect the other data in the computer. All it does is to alter the outcome of an algorithm. There is nothing unreliable about the operation of that algorithm or its outcome. The only difference is that the operation is unaware of the true nature of the algorithm.

The problem is that the offence refers to the reliability of the data itself, not the conclusions that can be drawn from it. Instead it should be made clear that reliability in this offence does not refer to the data but instead refers to an intent to impair the degree to which an accessor can assume that no unauthorised modifications have been made to the data.[57] It is unfortunate that this was not made clear in a definition of the term.

Security is also an undefined term. The notion of security of data implies that in some way access to this data is restricted. Therefore an intention to impair the security of data might require proof that there were existing measures to control access and modification of the data. However it is unclear as to the extent that security also includes privacy. For example, it might be that despite the lack of any access controls on the information it is clear that the information is private and that the controller of the information would not like the information accessed by others. If this is the case then the restrictions inherent in s 478.1/s 308H relating to restricted information become less absolute. For example, any device that attempts to place a cookie on another computer without authority and thereby track the use of the computer could be compromising the security of the data on that computer. Again, this offence does not relate to restricted data, so the history of websites visited by the user of the computer could be data caught by this offence.

It is hard to see how data under its usual meaning can be "operated". It is mere information and as such is used by the computer within the operation of computer functions. Presumably an impairment of the operation of data can only refer to the extended meaning of "any program". Thus the offence refers to the impairment of the operation of a program. This is a broad concept that could refer not only to issues of reliability but also to speed of operation and the programme's interoperability. Thus the offence appears broad enough to catch the types of activities prohibited in s 477.3/s 308E. A person engaging in e-mail flooding is sending data to the receiving computer with the intention that that data will add to the amount of data in the computer and in causing the computer to add that data will

[54] MCCOC Report, n 4, p 165.

[55] Under the extended definition of data as a program it is easier to see how the modification of a program could result in it producing inconsistent outcomes at different times. Even this, though, seems to be less than the offence aims to prohibit.

[56] The entry could not be said to impair access to, or the security or operation of the data.

[57] A similar problem arose in earlier versions of insider trading offences when it was not made clear that one could not trade on conclusions drawn from inside facts. See *Ryan v Triguboff* [1973] 1 NSWLR 588.

degrade the computer's ability to operate other programs. That such an approach is permissible is underlined by the fact that s 477.3/s 308E is an alternative to s 477.2/s 308D.

Finally, it is worth noting that the offence is not complete unless the modification is to data held on a computer or network and that modification is unauthorised. Thus it is not an offence under this section merely to place hidden viruses in freeware programs on one's own website hoping that others will download it.[58] There must be an unauthorised modification. However, once the virus was downloaded by a victim it would be arguable that while the victim implicitly authorised any modification of data necessary to install and run the ostensible freeware program, no authority was given to modify data in the way in which the virus is intended to.

Nor is an offence to crack encryption on a CD or DVD as the information contained on that storage device is not modified. Arguably the loading of the data from the DVD onto one's own computer is unauthorised (and therefore a breach of s478.1/s308H) but once the copy is made it would be hard to see how modification of one's own data was unauthorised.

Unauthorised copying

This raises the important omission in these offences. There is no offence of unauthorised copying of data. The law on unauthorised copying has presumably been left to the copyright legislation.

As long as a person has the right to access data, and the method by which they access or copy the data does not result in any modification to that data it is not a crime to make unauthorised copies of that data. Thus, for example, there is nothing in this legislation that would prevent the copying of CD music to an MP3 format and then distributing it on the internet. Such actions would only be restricted by the copyright regime.

Impairment of communication

The NSW provision is as follows:

"**308E Unauthorised impairment of electronic communication**

(1) A person who:
   (a) causes any unauthorised impairment of electronic communication to or from a computer, and
   (b) knows that the impairment is unauthorised, and
   (c) intends to impair electronic communication to or from the computer, or who is reckless as to any such impairment,

   is guilty of an offence.

   Maximum penalty: Imprisonment for 10 years.

(2) A conviction for an offence against this section is an alternative verdict to a charge for:
   (a) an offence against section 195 (Maliciously destroying or damaging property), or
   (b) an offence against section 308D (Unauthorised modification of data with intent to cause impairment)."

The Commonwealth provision is more concise:

"**477.3 Unauthorised impairment of electronic communication**

(1) A person is guilty of an offence if:
   (a) the person causes any unauthorised impairment of electronic communication to or from a computer; and
   (b) the person knows that the impairment is unauthorised…

Penalty: 10 years imprisonment..."

This a new offence for Australian jurisdictions and was the Committee's response to the realisation that most computing now occurs over networks. The place of this offence can be gleaned from the alternative convictions set out. Use of crude physical force to impair communications is covered by the damage to property offence. Impairment of communications caused by the forms of interference that in some way change or alter the communication are dealt with under the unauthorised modification offence. This offence is designed to deal with those forms of interference known as "denial of service attacks". As noted above the impairment of communication requires some form of degradation, not mere interception.

[58] It could however amount to an attempt.

As previously discussed, the major unresolved issue, in relation to the physical elements of the offence, is the requirement that the communication be to or from a computer. It also seems strange that the Committee having decided that the mere intention to access or modify data in a computer should require additional specific intentions did not do so with this offence. Particularly as it is a new departure for the law it is unfortunate that the degree of specification of intent was not consistently applied. This offence has the potential to criminalise the "trivial misconduct" that the MCCOC Report was so keen to keep out of s 308D.[59]

The extreme breadth of the offence is breathtaking. The mental elements of the offence do not necessarily require any specific intent in relation to any element of the offence other than the precise act that "causes" the impairment.[60]

Knowledge that the impairment is unauthorised is satisfied if the defendant is aware in the abstract that the impairment that resulted is something that they would not have been permitted to do. Thus this element operates mainly as a claim of right defence and is unlikely to arise as a major hurdle for the prosecution.

The main mental element in the NSW offence is thus recklessness. There is not any requirement in the offence that the person be aware that they have caused the impairment. One can be convicted if it can be proved that the defendant was aware that the actions they engaged in could possibly/probably cause impairment of some kind. It is thus an offence in which the physical elements are satisfied by a result not an action and where the only state of mind required is a general awareness of the possible outcomes of the actions.

The Commonwealth might appear to be even broader than the MCCOC Report's draft and the NSW offence. This is because the Commonwealth offence does not explicitly contain any requirement of proof of intent or recklessness.[61]

It might therefore appear that causing of impairment is a strict liability element. However this is this is not the case due to the role of Ch 2 of the *Criminal Code*[62], and in particular s 5.6(2).[63] As Ian Leader-Elliott has pointed out, because there is no fault element specified for the physical element of impairment in the offence, the fact that impairment constitutes a result has the effect of importing a requirement of proof of recklessness by virtue of s 5.6(2). The *Code* also enacts that no offence can be one of strict liability unless specifically enacted as such.[64]

However it is regrettable that the offences were not drafted according to a consistent pattern – either by specifying mental elements (as in the NSW offences) or in declining to state any mental element that could be implied by s 5.6 (as in s 477.3).

As has been discussed earlier, the whole notion of impairment is unclear and apparently extremely broad. Impairment need not be anything more than temporary and it need not be significant. The combination of such a low threshold physical element with a lack of authorisation and advertence to possible outcomes means that this serious indictable offence is close to a police powers offence — spreading a broad net and relying on prosecutorial discretion for its appropriate use. It is a worrying addition to the criminal law.

The ancillary offence – unauthorised access, modification or impairment to commit another offence

The NSW provision is as follows:

"**308C Unauthorised access, modification or impairment with intent to commit serious indictable offence**

(1) A person who causes any unauthorised computer function:

---

[59] At p161.

[60] For the Commonwealth, this is mandated by s5.6(1) and can be assumed for the NSW offence. It would be extremely rare that no such intent existed.

[61] Puzzlingly, the Explanatory Memorandum to the Bill claims that in order to commit the offence it must be proved that "the person knows the impairment is unauthorised, and either intends to impair electronic communication or is reckless as to any such impairment". This appears to have been copied from the summary of the elements of the offence at p 171 of the MCCOC Report. The drafter appears to have had other ideas.

[62] See the illuminating explanation of this in Leader-Elliott, "Elements of Liability in the Commonwealth *Criminal Code*", (2002) Crim LJ 28 at 36.

[63] 5.6 (2) If the law creating the offence does not specify a fault element for a physical element that consists of a circumstance or result, recklessness is the fault element for that physical element.

[64] Section 5.6. For example, see the care that the drafters took in the offences to specify that the status of equipment as Commonwealth property was to be one of absolute liability.

(a) knowing it is unauthorised, and
(b) with the intention of committing a serious indictable offence, or facilitating the commission of a serious indictable offence (whether by the person or by another person),

is guilty of an offence.

Maximum penalty: The maximum penalty applicable if the person had committed, or facilitated the commission of, the serious indictable offence in this jurisdiction.

(2) For the purposes of this section, an ***unauthorised computer function*** is:
(a) any unauthorised access to data held in any computer, or
(b) any unauthorised modification of data held in any computer, or
(c) any unauthorised impairment of electronic communication to or from any computer.

(3) For the purposes of this section, a ***serious indictable offence*** includes an offence in any other jurisdiction that would be a serious indictable offence if committed in this jurisdiction.

(4) A person may be found guilty of an offence against this section:
(a) even if committing the serious indictable offence concerned is impossible, or
(b) whether the serious indictable offence is to be committed at the time of the unauthorised conduct or at a later time.

(5) It is not an offence to attempt to commit an offence against this section."

The Commonwealth version of this offence is in similar terms but is in two different versions. The first, s 477.1(1)-477.1(3) requires the use of a telecommunications service. If such a service is used it is an offence to intent to commit and offence against any Australian jurisdiction. However if a telecommunications service is not used, the second variation s 477.1(4)-(5) restricts the operation of the offence to an intention to commit a serious Commonwealth offence.

Under s 477.1, as long as the person causes the access, modification or impairment by means of a telecommunications service, the intention can be to commit a serious New South Wales offence. This creates a large ambit of operation for Commonwealth agencies in prosecuting any form of electronically-based crime.

The conduct

This offence is designed to make actions that would otherwise fall outside of s 478.1/s 308H, s 477.2/s 308D and s 477.3/s 308E criminal if the defendant is engaging in the conduct with intention commit a serious indictable offence. Thus unauthorised access to unrestricted information becomes an indictable offence with a penalty ranging up to life imprisonment (depending on the maximum penalty for the intended offence) and unauthorised modification is criminalised even without proof of the specific intents to impair data — as long as it is preparatory to another offence. However the section adds nothing to s 477.3/s 308E. All activities in relation to intent to impair electronic communication in s 477.1/s 308C are already prohibited in s 477.3/s 308E. This emphasises the extreme breadth of s 477.3/s 308E.

The offence therefore criminalises any form of conduct that deals with data in computers or passing between computers where that dealing is related to the commission of another serious crime. It is more than arguable that this section may prove to be all that the law needs to deal with computer offences. By referring to serious indictable offences the law manages to make the concept of the computer a transparent one. It is the underlying offence that constitutes the criminality, not the technological tool used.

However, the method of deriving the penalty is of some concern. The section of the MCCOC Report discussing this offence makes it clear that this offence was designed to fulfil a similar role to offences of going equipped to steal and other preparatory offences. Indeed, throughout the Report this offence is referred to as preparatory. The matching of the penalty to the penalty of the serious indictable offence intended by the access also emphasises the fact that the MCCOC saw the offence as akin to an offence of attempt. In other words, this offence is one that should only be prosecuted when the defendant has been interrupted prior to the realisation of their ultimate aim (the serious indictable offence).

But there is nothing in the wording of the offence that prevents a defendant having to face charges arising from both this offence and the serious indictable offence (or its attempt). Thus, the basic effect of this section is to double the penalty for any serious crime perpetrated by means of a computer. If the crime is successfully completed one can still be charged under the principal offence. If the crime does not come to fruition one can still be charged with the attempted crime, in addition to this offence. The only restriction is that one cannot be charged with an attempt to use a computer to attempt. It is hoped that prosecutors adopt a policy of seeing this offence as an alternative to the serious indictable offence intended and not as an additional offence.

Unauthorised

The requirement that the access, modification or impairment be unauthorised constitutes a narrowing of the scope of the previous s 309(2) which enacted:

> "(2) A person who, with intent:
>
> (a) to defraud any person; or
>
> (b) to dishonestly obtain for himself or herself or another person any financial advantage of any kind; or
>
> (c) to dishonestly cause loss or injury to any person,
>
> obtains access to a program or data stored in a computer is liable to imprisonment for 2 years, or to a fine of 500 penalty units, or both."[65]

This offence while specifying the crimes that the person had to intend to commit did not require that the access they effected was unauthorised. This had the effect that persons who created a misleading statement on their own home computer were not only creating false statements but also committing a computer offence. The new offence recognises that the law should not criminalise conduct that in itself is legal merely because it is on a computer and preparatory to another offence. The new offence makes clear that the criminality arises when one acts in an unlawful way in order to commit another offence. Otherwise the absurd situation of committing a crime against oneself is possible. Under the old offence, if perpetrators used their own e-mail programmes to send deceptive e-mails to others, they would be guilty of not only attempting to obtain by deception but also of using their own e-mail.

On the other hand, the removal of the restriction of the offence to intentions to commit property offences is welcome. Computerised systems are now involved in all aspects of life and therefore can be a preparatory part of almost all crimes. Crimes of sabotage, public health and safety, and personal injury can now be perpetrated through the use of computers.

Serious offence

This is defined in s 477.1(9)/s 4 as an:

> "offence that is punishable by imprisonment for life or for a term of 5 years or more."

It is also given an extraterritorial effect similar in effect to s 308. However, there is no requirement of "conduct" occurring in the other jurisdiction and so may be more easily applied.

Intention of committing or facilitating

These elements emphasise the preparatory nature of the offence in that they do not include "in the commission of" as an alternative. The aim appears to be to permit the arrest of criminals in a planning stage. This is before any attempt is made to actually commit the crime. In many ways this offence is similar to the traditional offences of going equipped to steal.

It is interesting to contrast its scope with that of s 478.3/s 308F and s 478.4/s 308G. If the obtaining of the data is unauthorised, then an intent to use that data to cause unauthorised modification or impairment within the scope of s 477.2/s 308D or s 477.3/s 308E may constitute an offence under s 477.1/s 308C. Consequently a penalty of up to 10 years would be possible.

This means that s 478.3/s 308F and s 478.4/s 308G are only likely to be prosecuted in circumstances where the data was obtained or created in a legal way — for example by the creation of a password cracking program. As mentioned in the discussion of those offences it is moot whether such situations are in fact criminal.

[65] *Crimes Act 1914* (Cth), s 76b(2) is in similar terms.

The importance of the de minimus principle, police funding and judicial discretion

The major check on the abuse or overuse of this new legislation will be financial and attitudinal. The police and public prosecutors have limited budgets and clear priorities to concentrate on serious criminal activity. These new laws constitute a more flexible regime in which they can operate to prevent and prosecute crime. But their budget constraints will likely mean that there will be a reluctance to prosecute any minor or borderline breaches of these new laws. However, in the wake of moral panics and heightened concerns over so-called "cyberterrorism" such restraint may not be forthcoming.

If such prosecutions are undertaken, or if private prosecutions become more prevalent, the attitude of the judiciary will be of importance. Magistrates and judges will not look kindly on prosecutions that waste the court's time and patience. In addition, unless serious harm or an intent to cause serious harm results, it is unlikely that sentences will involve substantial fines or imprisonment. In many cases the first offence may be deal with under sections such as s 10 of the *Crimes (Sentencing Procedures) Act 1999* (NSW), "Dismissal of charges and conditional discharge of offender".

Conclusion

The new offences are a confusing result of experience and experiment. In the access offences and modification of data offences it is clear that the offences recognise that the original offences were too broadly expressed. Thus it is now only an offence to access restricted data and issues of authorisation avoid the murky waters of ulterior motive. The modification offences now require the knowledge of the defendant that such modification or damage was inevitable or possible.

However, the new preparatory offences and the impairment offence are even broader than the old offences were. The preparatory offences rely almost entirely on proof of intention, and thus on circumstantial evidence or confession. The impairment offence rests on an untested and vague notion of impairment. It would appear that recognition of the need to wind back the scope of the existing offences did not prevent the repetition of those excesses in the creation of the new offences.

Appendix A: comparative table of offences in NSW

Current Law			*New Law*		
Section	**Offence**	**Max penalty**	**Section**	**Offence**	**Max penalty**
			308C	Cause unauthorised computer function with intention to commit serious offence (comprising unauthorised access to data, unauthorised modification of data or unauthorised impairment of electronic communication)[66]	The maximum penalty applicable for commission of serious indictable offence*
310	Damaging data in computer	10 years and/or 1,000 penalty units	308D	Unauthorised modification of data with intent to cause impairment	10 years*
			308E	Unauthorised impairment of electronic communication to or from computer	10 years*
			308F	Possession of data with intent to commit serious computer offence	3 years*
			308G	Producing, supplying or obtaining data with intent to commit serious computer offence	3 years*
309 (1)	Unlawful access to data in computer	6 months and/or 50 penalty units			
309 (2)	Unlawful access to data in computer—intent to defraud/dishonestly obtain benefit or cause loss/injury	2 years and/or 500 penalty units			
309 (3)	Unlawful access to data in computer—knowledge data is confidential	2 years and/or 500 penalty units	308H	Unauthorised access to or modification of restricted data in computer (summary offence)	2 years*
309 (4)	Continue to examine data in computer—ought reasonably to know data confidential	2 years and/or 500 penalty units			
			308I	Unauthorised impairment of data held in computer disk, credit card or other device (summary offence)	2 years*

These descriptions are sourced from the descriptions in the Explanatory Memorandum to the Crimes Amendment (Computer Offences) Bill 2001

*The court may alternatively, or in addition, impose a fine of 1,000 penalty units for an individual or 2,000 for a corporation (a penalty unit is currently $110).[67]

[66] This is more accurately described as "Cause unauthorised computer function (comprising unauthorised access to data, unauthorised modification of data or unauthorised impairment of electronic communication) with intention to commit serious offence".
[67] *Crimes (Sentencing Procedure) Act 1986*, s 15, 16.