

**MODEL
CRIMINAL
CODE**

Report

CHAPTER 4

**DAMAGE AND
COMPUTER OFFENCES**

and

**Amendments to Chapter 2:
Jurisdiction**

January 2001

This Report was prepared by the Model Criminal Code Officers Committee. It does not necessarily represent the views of the Standing Committee of Attorneys-General or an individual Attorney-General.

REPORT

MODEL CRIMINAL CODE

CHAPTER 4

DAMAGE AND COMPUTER OFFENCES

AMENDMENTS TO CHAPTER 2: JURISDICTION

Model Criminal Code Officers Committee of the
Standing Committee of Attorneys-General

January 2001

This Report was prepared by the Model Criminal Code Officers Committee. It does not necessarily represent the views of the Standing Committee of Attorneys-General or an individual Attorney-General.

ISBN 0 642 21006 3

PREFACE

Background To The Model Criminal Code Project

On 28 June 1990 the Standing Committee of Attorneys-General (“SCAG”) placed the question of the development of a national model criminal code for Australian jurisdictions on its agenda. In order to advance the concept, SCAG established a Committee consisting of an officer from each Australian jurisdiction with expertise in criminal law and criminal justice matters. That Committee was originally known as the Criminal Law Officers Committee (CLOC), but, in November 1993, the name was changed to the Model Criminal Code Officers Committee (MCCOC) in order to reflect the principal remit of the Committee directly.

The first formal meeting of the Committee took place in May 1991. In July 1992, the Committee released a discussion draft of the general principles of criminal responsibility. After a great deal of public consultation, the Committee delivered a Final Report to SCAG which was released in December 1992. With the exception of the general principles relating to intoxicated defendants, the recommendations in that Final Report formed the basis for the Commonwealth Criminal Code Bill, 1994, which was passed by the Commonwealth Parliament in March, 1995.

In 1994, both the Commonwealth Government and the State and Territory Premiers’ Leaders Forum endorsed the Model Criminal Code project as one of national significance.

In December 1995 MCCOC released its Final Report titled Theft, Fraud, Bribery and Related Offences. MCCOC has since released discussion papers on Non Fatal Offences Against the Person in August 1996 (report September 1998), Sexual Offences in November 1996 (report, June 1999), Contamination of Goods Offences in May 1997 (report March 1998), Serious Drug Offences in June 1997 (report October 1998), Administration of Justice Offences in July 1997 (report June 1998), Slavery Offences in April 1998 (report November 1998) and Fatal Offences in June 1998.

This report primarily deals with the area of the law which criminalises damaging property and breaching the security of, and harming computer systems. The damage offences have concepts linked to those already settled in Chapter 3 which deals with theft and fraud offences because both deal with property. The computer offences also deal with damage, but the intangible nature of computer technology is such that special offences are required. While they are appropriately grouped with the damage offences, the computer offences cover less tangible consequences. The Committee has always attempted to rationalise offences and strongly believes that where a general offence can be used it should be (for example, the Committee does not favour special computer fraud and forgery offences, instead the traditional offences have been modified to cover computers).

The Committee has also used this discussion paper to put forward its view on what should be the general provisions dealing with the geographic limits of State and Territory offences. Following decisions like *Catanzariti* (1995) 8 A Crim R 584 and *Isaacs* (1996) 87 A Crim R 513, it has become apparent that the existing provisions on jurisdiction, which were endorsed by SCAG in 1992, need to be reviewed. The Committee recognises it cannot complete the Code without putting forward a legislative solution to the problems raised in those cases. The proposed provisions in chapter 2 of the Model Criminal Code which deal with jurisdiction are discussed in the second part of the report.

While there are some serious offences not included in the Model Criminal Code (for example, piracy), with the completion of chapter 4, most serious offences will be in the Code. In the future it can be expected SCAG will wish to modify the Code and add offences to it as times change. No Criminal Code can remain viable without ongoing development. However, with the completion of chapter 4, Governments will have a Model Criminal Code which they can implement wholly or progressively over the next decade. The focus will now move to implementing the Code in each jurisdiction. This will no doubt be a gradual process which will require commitment to the aims of the Attorneys-General when they initiated the project in 1991 - greater national consistency.

It is therefore with great gratitude for their previous efforts that the Committee asks contributors to provide their views on this report.

As with its previous publications, MCCOC has attempted to produce a document which is comprehensive, concise and capable of being understood by the general public as well as those who have some legal expertise. In this report "Model Criminal Code" will be used to refer to the draft legislation recommended by this paper, the Bill attached to Chapters 1 and 2 as modified by the Criminal Code Act 1995 (Cth) (Appendix 2) and Chapters 3, 5, 6, 7, 8 and 9 as drafted in the reports on Theft, Fraud, Bribery and Related Offences, Sexual Offences, Non-fatal Offences, Serious Drug Offences, Administration of Justice Offences, Contamination of Goods Offences and the Slavery Offences. The Criminal Code Act 1995 (Cth) enacts the draft Bill attached to the Chapters 1 and 2 Final Report, with the exception of the provisions relating to the O'Connor defence of intoxication. The drafting of the Commonwealth Act differs slightly from that of the Draft Bill. These changes have been approved by the Standing Committee of Attorneys-General. The report is organised with the proposed Code provision on one page and a commentary explaining the Committee's reasoning and intentions about it on the facing page.

The Committee is very grateful for the assistance of the Parliamentary Counsels' Committee and, in particular, Parliamentary Counsel for New South Wales for its prompt, thoughtful and incisive drafting.

Most of the report was written by Mr Ian Leader-Elliott of the Faculty of Law, University of Adelaide, who is a consultant of the Commonwealth Government.

Mr Matthew Goode of the South Australian Attorney-General's Department wrote the segment concerning jurisdictional issues.

The Committee welcomes comments on any aspect of the proposed provisions. Comments should be sent to:

The MCCOC Secretariat
Criminal Law Division
Attorney-General's Department
Robert Garran Offices
National Circuit
BARTON ACT 2600

COMMITTEE MEMBERS

Chairperson

The Honourable Justice Rod Howie, QC
Supreme Court of New South Wales

Members

New South Wales:

Ms Chrissa Loukas
Director, Criminal Law Review Division
Attorney-General's Department

Victoria:

Mr Greg Byrne
Manager
Criminal Law Branch
Department of Justice

Western Australia:

Ms Lindy Jenkins
Senior Assistant Crown Counsel
Crown Solicitor's Office

South Australia:

Mr Matthew Goode
Managing Solicitor
Policy & Legislation Section
Attorney-General's Department

Tasmania:

Mr Nick Perks
Crown Counsel
Department of Justice

Northern Territory:

Ms Elizabeth Kelly
Director, Policy Division
Attorney-General's Department

Australian Capital Territory:

Ms Karen Greenland and Ms Amanda Casimar
Criminal Law Section
Legal Policy Division
Department of Justice and Community Safety

Commonwealth:

Mr Geoff McDonald
Assistant Secretary
Criminal Law Branch
Attorney-General's Department

Commonwealth Consultant:

Mr Ian Leader-Elliott
Faculty of Law
University of Adelaide

Adviser

Her Honour Judge Megan Latham
District Court of New South Wales
Mr Andrew Haesler
Public Defender (NSW)

Legislation

| | |
|-----|--|
| ACT | Crimes Act 1900 |
| Cth | Crimes Act 1914 Criminal Code Act 1995 |
| NSW | Crimes Act 1900 |
| NT | Criminal Code Act 1983 |
| Qld | Criminal Code Act 1899 |
| SA | Criminal Law Consolidation Act 1935 Summary Offences Act 1953 |
| Tas | Criminal Code Act 1924 |
| Vic | Crimes Act 1958 Summary Offences Act 1966 |
| WA | Criminal Code Act Compilation Act 1913 |

Table Of Contents

| | |
|---|-----------|
| Preface | i |
| Background to the Model Criminal Code Project | i |
| Committee Members | iv |
| Legislation | vi |
| Introduction | 1 |
| Chapter 4 - Part 4.1 - Property Damage Offences | 9 |
| Division 1 - Definitions | 9 |
| 4.1.1 Property | 9 |
| 4.1.2 Damage to property | 13 |
| 4.1.3 Person to whom property belong | 21 |
| 4.1.4 Threats | 25 |
| 4.1.5 Causing damage or other result | 25 |
| Division 2 - Offences | 27 |
| 4.1.6 Damaging property | 27 |
| 4.1.7 Arson | 37 |
| 4.1.8 Bushfires | 47 |
| 4.1.9 Threat to cause property damage - fear of death or serious harm | 57 |
| 4.1.10 Possession of a thing with intent to damage property | 67 |
| Division 3 -Defences | 77 |
| 4.1.11 Consent | 77 |
| 4.1.12 Claim of right | 79 |
| 4.1.13 Self-defence | 83 |

| | |
|---|------------|
| Chapter 4 - Part 4.2 - Computer Offences | 87 |
| Introduction | 87 |
| 4.2.1 General definitions | 121 |
| 4.2.2 Meaning of access to data, modification of data and impairment of electronic communications | 133 |
| 4.2.3 Meaning of unauthorised access, modification or impairment | 139 |
| 4.2.4 Unauthorised access, modification or impairment to commit a serious offence | 149 |
| 4.2.5 Unauthorised modification of data to cause impairment | 157 |
| 4.2.6 Unauthorised impairment of electronic communication | 171 |
| 4.2.7 Possession of data with intent to commit computer offence | 175 |
| 4.2.8 Obtain produce or supply data with intent to commit computer offence | 183 |
| Part 4.3 - Sabotage | 201 |
| Introduction | 201 |
| 4.3.1 Definitions | 205 |
| 4.3.2 Meaning of damage to public facility | 207 |
| 4.3.3 Sabotage | 209 |
| 4.3.4 Threaten sabotage | 213 |
| Chapter 2 - Part 2.7 - Jurisdiction | 217 |
| Introduction | 217 |
| The Territorial Principle | 218 |
| Continuing Crimes | 220 |
| The Protective Theory | 222 |
| Modern General Theories Of Jurisdiction | 224 |
| Statutory Intervention On A National Basis | 231 |

| | |
|--|------------|
| International geographical jurisdiction | 240 |
| The Proposed Model | 245 |
| Appendix 1 - Model Criminal Code Chapters 1 and 2 | 283 |
| Appendix 2 - Model Criminal Code Chapter 4 | 308 |
| Appendix 3 - Computer Misuse Act 1990 (UK) | 322 |
| Appendix 4 - United Nations International Convention for the Suppression of Terrorist Bombings (52/164) | 337 |
| Appendix 5 - Commonwealth, State and Territory Property Damage and Computer Offences Comparison Chart | 350 |

INTRODUCTION

Laws against damage were the creation of legislatures, rather than courts. Like the law of non-fatal offences against the person, in jurisdictions which have not yet cleansed their statute books of antique debris, the law of criminal damage is characterised by unnecessary proliferation of distinct offences and pointless differentiation among different kinds of damage or modes of inflicting that damage. Periodic waves of legislative concern over two centuries have resulted in the enactment of distinct criminal prohibitions aimed at individuals who might be tempted to damage crops, ships, railways, animals, aircraft and computers. The Committee's Report on *Non-Fatal Offences Against the Person* began with a criticism of laws which are patchy and underinclusive in their applications and fussily insistent on "very specific categories instead of...general offence(s) based on general and consistent principle".¹ The Report proposed a simplified code of offences differentiated according to the fault of the offender and the gravity of the harm. The same commitment to the articulation of general and consistent principles drives the proposals in this Report for reform of the law of criminal damage.

The recommendations which follow are based on the work of the United Kingdom Law Commission, whose report on property damage offences² and draft provisions provided the basis for the *Criminal Damage Act 1971*. ATH Smith, introduces his valuable commentary on the Act with the following encomium:

This codifying measure greatly simplifies the pre-existing law by abolishing distinctions based on the nature of the property damage, its situation, the circumstances in which the destruction or damage took place, the status of the offender, and, with one notable exception (arson) the means used to effect the damage. These distinctions had made the law undesirably complex.³

The Committee's reliance on British legislative precedent was largely determined by its earlier proposals for reform of the law of theft and related offences. In 1995 the Committee recommended adoption of a uniform code of offences based on the UK *Theft Act*⁴ - legislation which had been accepted and received, with local variations, in Victoria, the Australian Capital Territory and the Northern Territory. Criminal damage overlaps the crime of theft. One who takes, opens and drinks a bottle of wine from a vintner's cellar without permission is guilty of larceny of the vintner's wine and criminal damage to his property as well.

1 Model Criminal Code - Chapter 5: *Non-Fatal Offences Against the Person* Report 1998, p2

2 *Report on Offences of Damage to Property* (1970) L.Com. No29.

3 ATH Smith, *Property Offences* (1994), para 27-02.

4 Model Criminal Code - Chapter 3: *Theft, Fraud, Bribery and Related Offences*, Report 1995.

Though there is substantial common ground between these offences, the overlap is far from complete. Criminal damage requires proof of harm to tangible things but property can be stolen even though the thief does not lay a finger on the property in question. The law of theft has progressed, by slow and halting steps, to the point where it includes dishonest acquisition of rights to intangibles, as well as deprivation of physical possession.⁵ This extension of the offence of theft to include conduct which violates rights, whether or not physical interference with the property has taken place, has been facilitated by a parallel development of the concept of dishonesty. Conduct is dishonest if it violates the ordinary person's expectations or standards of honesty. In many instances, the element of dishonesty is the only thing which separates theft from a unexceptionable transaction involving a lawful exchange of property.⁶ Since standards of honesty and dishonesty are variable and evolve over time, the prosecution is required to prove that the offender was aware of the standard before a conviction can be returned.

No comparable sophistication in the definition of fault elements has been necessary in the law of criminal damage.⁷ The offence is confined to relatively crude forms of physical interference with tangible property. Some will amount to theft; many will not. A vandal who destroys the handpiece of a public telephone or snaps a motor car aerial is guilty of criminal damage but would not usually be described as dishonest.

There are other distinctions between the offences apart from those involving the concept of dishonesty. The area of common ground between the offences is nevertheless substantial. The extent of their overlap and the frequent similarity in the harms involved, when rights to tangible things are threatened, requires consistency of principle and terminology. The offences proposed in Part 1 of the Report are intended to provide a coherent and principled supplement to the Chapter 3 offences.

The need to ensure consistency of principle and conceptual vocabulary in closely related areas of law has also influenced the Committee's decision to build on the work of the Law Commission. Criminal damage and damage to data can overlap and, in either case, the prospect of dishonest gain will often provide the motive for the offence.

5 Chapter 3: *Theft, Fraud, Bribery and Related Offences* Report 1995, p35: "It is possible to assume the rights of an owner in relation to goods without touching them: to point to someone else's car and offer to sell it would amount to an appropriation. The true breadth of the term has been the subject of considerable controversy."

6 These considerations justify what might otherwise seem an inconsistency in the fault requirements for theft and criminal damage. The charge of inconsistency was made in a submission from the Commonwealth Director of Public Prosecutions March 13, 2000, per Justin McCarthy, Senior Assistant Director.

7 See, however, the potential applications of the defence of "claim of right" in s4.1.13, post.

Criminal damage is not graded by cost or value

The UK Law Commission discussed and rejected proposals to divide the offence of criminal damage into a basic and an aggravated offence by reference to the value of the property involved:

The test of the value of the property damaged has obvious disadvantages consequent upon the changing value of money. In addition, we doubt whether a valuation of the property damaged is necessarily co-extensive with the real seriousness of the offence. A man may, for example, set fire to a nearly valueless tree, knowing that there is a risk that a whole forest may be destroyed. On the other hand, a man may destroy two paintings, one valueless and the other priceless, thinking them both to be of little value.⁸

The Law Commission proposed instead a distinction between aggravated and basic offences which depend on whether criminal damage involved fire or endangering life. The Committee has followed the first of these proposals, retaining arson as an aggravated offence of property damage. There is, however, no offence of endangering people by destroying property. That would involve an unnecessary duplication of offences found elsewhere in the Code.

South Australia is exceptional among Australian jurisdictions in providing three levels of penalty for property damage, calibrated by reference to the financial cost of the damage done to the property.⁹ Australian Capital Territory legislation limits the penalty for criminal damage to 6 months imprisonment, if the property was worth less than \$1000.¹⁰ The South Australian scheme, which makes the cost of the damage determinative, suggests an additional conceptual issue. What principle determines whether penalties are graduated by reference to the value of the property damaged, as the Law Commission contemplated, or by the South Australian practice of counting the cost of the damage sustained by the property?

Apart from the likelihood of bracket creep and other considerations to which the UK Law Commission drew attention, damage to valuable property may be trivial in extent. If South Australian practice is followed, however, making the cost of repair or replacement determinative, this sum may bear no relationship to the loss imposed as a consequence of the damage or destruction. Sabotage of machinery resulting in loss of a days production can impose losses which far exceed the cost of a minor but essential repair to restore the machinery to working order. It is preferable to rely on exercise of the sentencing discretion in particular cases than attempt to discover legislative formulae which will dissolve these complexities.

8 Law Com No29, para 23.

9 *Criminal Law Consolidation Act* (SA) 1935, s85.

10 *Crimes Act* 1900 (ACT) a128(4).

Proposals for a division between aggravated and trivial offences reflect uneasiness over the sheer breadth of the offence of criminal damage and the consequential breadth of sentencing discretion required. Adoption of that principle would have far reaching effects however. If principles of fairness required discrimination between serious and less serious grades of criminal damage, those principles would apply with equal force in the law of theft, so as to require distinction between serious and less serious grades of that offence. Here as in other areas of overlapping concern, the law of property damage should be consistent with the law of theft. A drinker who pockets a beerglass in a hotel is guilty of theft and liable, under Chapter 3 of the Model Criminal Code to a maximum penalty of 10 years imprisonment. The penalty for property damage is the same. In this respect the Code reflects the law in most Australian jurisdictions. If a hotel patron who pockets a glass is liable to the standard penalty for theft, the same patron should be liable to the standard penalty for criminal damage if the beerglass was deliberately dropped and shattered on the tiled floor of the bar. In the United States, where the American Law Institute *Model Penal Code* provides the pattern for reform, the law does tie grades of liability for theft to the pecuniary value of the property which was stolen.¹¹ It is a pattern of prohibition which has not found favour in Australia and the Committee can see no reason for recommending so radical a change to existing legislative practice.

There is no doubt that the offence of criminal damage will extend to much conduct which is too trivial to merit prosecution. The Code does set some limits to the offence. The plea of consent will excuse damage to property if it was done in the belief that the owner would have consented, had the circumstances been known: [s4.1.11]. Sometimes acts of property destruction or damage are socially appropriate and accepted. There is no doubt, however, that much conduct which should never be the subject of criminal prosecution, will fall within the literal scope of the prohibition against property damage. Like offences of assault and minor theft, the enforcement of laws against criminal damage requires common sense in the exercise of prosecutorial discretion.

The proposed offences

The offence of property damage is committed whenever property is damaged or destroyed by an act which was intended to cause damage or destruction or accompanied by the realisation that there was a substantial and unjustifiable risk of damage or destruction. The prohibition applies generally to all real and personal property so long as it is tangible. Damage is defined broadly and includes, among other harms, loss of the property and impairment of its use or operation.

¹¹ *Model Penal Code* ALI 1962: See s220.3(2) Criminal Mischief; s223.1.

A range of more specific offences supplements the general offence of property damage. Arson remains an offence, though it is limited to damage caused to buildings, habitations and motorised vehicles, aircraft and motorised watercraft. The Committee accepts, here as elsewhere in the Code, that there are significant benefits in retaining public understanding and acceptance of the law, when the crimes in the Code coincide with well known and well accepted names of crimes in common usage.¹² The offence of arson proposed in the discussion paper is narrower in its applications than many current legislative formulations. The draft cleaves far more closely than existing law, however, to community understanding of the nature of the offence.

Two offences proposed by the Committee are without parallels in existing legislation. Sabotage and threatened sabotage [Part 4.3] are directed at terrorists and others who attempt or threaten to destroy public facilities, infrastructure or government offices. The second of the new offences - one with a peculiarly Australian resonance - is a prohibition against starting bushfires [4.1.8]. Like arson, both of these offences are punishable by penalties substantially exceeding the 10 year maximum for simple property damage.

Threats to cause property damage will be an offence against this Chapter if the threat was known to involve a substantial risk of causing fear of death or serious harm: [s4.1.9]. A threat to damage property, without more, will not amount to an offence against the Code, though the Committee proposes a summary offence of threatening property damage. A second summary offence of poaching wildlife is also proposed. Though domestic and captive animals are property which can be damaged, ownership of land does not confer ownership of wildlife which may be found there. The poaching offence is intended to provide a basis for prosecution of individuals who take, injure or kill wildlife on private land.

The application of each of these offences is extended by the general doctrines of attempt, complicity and conspiracy. In addition, the report retains the familiar preparatory offence of being in possession of the means of causing property damage with intent: [s4.1.10].

The boundaries of the criminal damage offences

In many ways, the offences in this Chapter are supplementary in character. They form a relatively minor province, completing a triangular terrain of prohibitions whose major parts consist of the Chapter 5 offences against the person and Chapter 3 offences of theft and other varieties of dishonest

12 See, for example, Model Criminal Code - Chapter 5: *Fatal Offences Against the Person* 1998 Discussion Paper pp9-10: "Murder". On occasion, however, significant shifts in the definition and scope of an offence will require abandonment of traditional terminology which might impose unwanted conceptual restrictions on the application of the offence: see Chapter 5: *Sexual Offences Against the Person*, Report 1999 pp55-65, on the displacement of "rape" by "unlawful sexual penetration".

acquisition. It is not necessary to include in this Chapter offences which involve property damage which endangers life. Such conduct is covered already, by general prohibitions against endangerment by any means whatever, in Chapter 5.¹³ Nor is it necessary to include offences where property is damaged or destroyed for some dishonest purpose. Destruction of property in order to effect a fraud, as for example in a fraudulent insurance claim, is an offence against this Chapter only if the property belongs to another. It is, in other words, merely an instance of the general offence of property damage. People who destroy property belonging to themselves or others for the purposes of fraud will be guilty of a Chapter 3 offence of fraudulent obtaining or, if their endeavours come to nothing, of an attempt to defraud, conspiracy or incitement to fraud.

The Code does not purport to provide a complete set of offences protecting property interests. There will remain a need for legislative provisions which regulate the ways in which particular kinds of property may be used and prohibit their misuse. Crimes of “obstruction”, “interference”, “concealment”, “disturbance”, “removal”, “rendering invisible” and “concealment” of railways, navigational aids and other specific forms of property cannot be contained within a general prohibition against damage or destruction.¹⁴

Computer misuse and damage to computer data

There is an exception to the Committee’s resolve to avoid proposals for legislation regulating the use and misuse of particular kinds of property. Part 2 of this Report proposes a code of offences dealing with the misuse of computers and damage to computer data. There are few areas of current legislative concern in which the need for uniformity of approach in the formulation of criminal offences is more desirable or more pressing.

13 Model Criminal Code - Chapter 5: *Non-Fatal Offences Against the Person* 1998, Division 7 - Endangerment.

14 The selection of examples is taken from Chapter 46 of the Queensland *Criminal Code* 1899.

PART 4.1 - PROPERTY DAMAGE OFFENCES

Division 1 - Definitions

4.1.1 Property

In this Part:

property means any real or personal property of a tangible nature, including:

- (a) a wild creature that is tamed or ordinarily kept in captivity or that is reduced (or in the course of being reduced) into the possession of a person, and
- (b) any organ or part of a human body and any blood, ova, semen or other substance extracted from the human body.

CHAPTER 3 - MODEL CRIMINAL CODE

For purposes of comparison, Chapter 3 contains the following definition of 'property':

"Property

14.4 In this Chapter:

"property" includes all real or personal property, including:

- (a) money; and
- (b) things in action or other intangible property; and
- (c) electricity; and
- (d) a wild creature that is tamed or ordinarily kept in captivity or that is reduced (or in the course of being reduced) into the possession of a person."

PART 4.1 - PROPERTY DAMAGE OFFENCES

Definitions

“Property”

The offences in Chapter 4 restrict liability for criminal damage to conduct which causes harm to *tangible* property.¹⁵ The definition of “property” in this Chapter is more limited than it is in Chapter 3: *Theft, Fraud, Bribery and Related Offences*. Offences of dishonesty, unlike criminal damage, will often involve conduct which impairs rights rather than acts of gross physical interference with physical objects. There is, however, a substantial area of common concern and though “property” is more broadly defined in Chapter 3 the definitions are meant to coincide in their application to tangible property.¹⁶

Property includes any tangible real or personal property. Offences involving property damage include harms to:

- *Land or fixtures* on land, such as buildings or fences;
- *Wild creatures* which have been tamed or kept captive and wild creatures which are in the course of being reduced to possession;
- *Human Tissue* which includes an organ or parts of a human body, foetal tissue, and substances extracted from the human body, including blood, ova and semen.¹⁷ The inclusion of human tissue

15 Two submissions took issue with the restriction of the definition to tangible property. Both submissions suggested that the accommodating definition of property employed in defining theft offences would be more appropriate. In part, at least, the suggestion appears to have been intended to bring damage to computer data within the scope of criminal damage legislation. See: Legal Aid Western Australia, 25 March 2000, per George Turnbull, Director; Victoria Police 31 March 2000, per Neil O’Loughlin Deputy Commissioner, Policy and Standards. The Committee does not accept that view. Extension of the offence of criminal damage to include impairment of rights of ownership would result in an alarming and incalculable extension of criminal liability in areas currently regulated by the civil law. Where impairment of rights to tangible property is concerned, we currently rely on the law of theft, fraud, copyright infringement and the like to delineate forms of wrongdoing and mark the boundary between civil and criminal processes. The law of criminal damage is an exceedingly blunt instrument by comparison. Protection of computer data and electronic communications does not require measures of such uncontrolled generality. Specific prohibitions directed against hackers and others are to be preferred both on grounds of principle and for their educative effect.

16 It should be noted, however, that Chapter 4 ss4.1.2(f), 4.13 departs from Chapter 5, s15.4, in extending liability for criminal damage to tenants who sever or damage plants.

17 *Compare Human Tissue Act 1983 (NSW) s4(2A)* See, in addition, *R v Kelly*[1998] 3 All ER 741, in which the English Court of Appeal held that human anatomical specimens, used in a medical school for teaching purposes, were property capable of being stolen. The Court held that the labour involved in dissecting and preserving human body parts conferred on them the attributes of property. In *obiter dicta*, at p750, the Court suggested that the common law might extend the meaning of property to include body parts though they had not been transformed by the application of labour or skill, “if they have a use or significance beyond their mere existence. This may be so if, for example, they are intended for use in an organ transplant operation, for the extraction of DNA or...as an exhibit in trial”.

Code

may go beyond the common law, which has been said to limit proprietary rights in human body parts to those which have been subjected to an exercise of skill of labour - as by dissection or preservation. The definition does not, however, extend to an entire human body, whether of a foetus or a person. Cases can be imagined - as for example an attack on an ancient mummified body in a museum - when a charge of criminal damage might appear appropriate. Such special cases aside, however, the Committee is of the view the mutilation, desecration or dismembering of an entire human body is not an appropriate subject for general legislation aimed at property damage. Instances of damage to ancient mummies are best dealt with in legislation directed to the protection of museum collections. Criminal damage legislation can play no more than a subsidiary and supplementary role in regulating conduct relating to human remains.¹⁸

The offences of theft and criminal damage overlap. The essential difference between the offences is to be found in the definition of theft as an acquisitive offence, which requires proof of dishonesty and an intention to deprive the owner permanently of property.

The offence of criminal damage proposed in Chapter 4 includes damage to real property. Here too, there is an overlap with the offence of theft. Though land cannot be stolen, the offence of theft extends to include severance and appropriation of things which form part of the land.¹⁹ Like theft, criminal damage extends to doorknobs, cultivated roses, wild or cultivated blackberries and mushrooms.²⁰ Unlike theft, criminal damage does not require proof of severance, appropriation or dishonesty.

18 See, for example, E King and R Smith, *Human Tissue Transplantation Crime: Trends and Issues in Crime and Criminal Justice*, Australian Institute of Criminology No87, 1998.

19 See s15.4 Chapter 3: *Theft, Fraud, Bribery and Related Offences* (1995). In this respect, Chapter 3 of the Model Criminal Code adopts a more extensive definition of theft than the UK *Theft Act* 1967. Section 4(3) of that Act excepts from its scope individuals who pick wild flowers, fruit, foliage or mushrooms, unless for reward, sale or other commercial purposes.

20 In Britain, *Criminal Damage Act* 1971, s10(1)(b) excludes "mushrooms growing wild on any land or flowers fruit or foliage of a plant growing wild on any land" from the scope of prohibition.

4.1.2 Damage to property

For the purposes of this Part, *damage* to property includes:

- (a) destroying the property, or
- (b) causing the physical loss of the property by interfering with the property (including by removing any restraint over the property or abandoning the property), or
- (c) causing any loss of a use or function of the property by interfering with the property, or
- (d) defacing the property, or
- (e) in the case of a document - obliterating or rendering illegible the whole or any part of the document, or
- (f) in the case of an animal— harming or killing the animal, or
- (g) in the case of a plant or other thing forming part of land— severing it from the land.

4.1.2 Damage to property

“Damage”

The offences of criminal damage are confined to destruction or damage affecting tangible property. Though the second of these expressions needs no definition, the meaning of “damage” has been the subject of debate. A leading British text opens discussion of the subject with the disarming remark that it is “difficult to lay down useful rules about what will or will not constitute damage”.²¹ Another British text²² quotes the South Australian Supreme Court decision in *Samuels v Stubbs* to emphasise the indeterminate scope of the concept of damage:²³

One must be guided in a great degree by the circumstances of each case, the nature of the article and the mode in which it is affected or treated...the word...is sufficiently wide in its meaning to embrace injury, mischief or harm done to property...in order to constitute “damage” it is unnecessary to establish such definite or actual damage as renders the property useless or prevents it from serving its normal function...

In that case the Court held that a “temporary functional derangement” of a policeman’s cap, which resulted when the defendant jumped on it, amounted to criminal damage.

Criminal damage does not require proof of complete or partial destruction of the object. In general, damage will involve “some physical harm, impairment or deterioration which can be perceived by the senses”.²⁴ It is apparent, however, that the meaning of “damage” varies according to the nature of the property and may extend to conduct which does not involve gross physical interference with the property. It is possible, for example, that all instances of damaging computer data - the primary subject of the second part of this discussion paper - will amount to simple criminal damage. The activities of hackers and others who modify data without authorisation, no matter how subtle the intrusion, will always involve some physical derangement of molecular patterns or traces which encode data in discs or other storage devices.

21 ATH Smith, *Property Offences* (1994) 27-13.

21 JC Smith and B Hogan, *Criminal Law*, (1983) 629.

22 (1972) 4 SASR 200 per Walters J at 203.

23 JC Smith and B Hogan, *op cit*, 629.

Code

Property damage resulting from omission to avoid harm

Damage to property can result from an omission or from some positive act of commission. Failure to water my neighbour's plants as I promised will kill them just as surely as dowsing them with herbicide. Though damage resulting from omission is often a matter for blame, the Code does not impose criminal liability for omission in the absence of specific provision or necessary implication: see Chapter 2: *General Principles of Criminal Responsibility*, s4.3. Though it would be possible to impose duties to preserve property belonging to others from harm, the Code does not extend to prohibit cases of property damage by omission. The clearest cases for recognition of a duty which might provide the basis for criminal liability are those in which the person is contractually obliged to preserve property. Though this may be the clearest case, it is also the one where the need for criminal penalties to enforce the duty are least persuasive. If there is liability in contract, the imposition of criminal liability as well appears unnecessary.²⁴ We do not, in general, impose prison sentences to reinforce contractual duties or other duties created by civil law.

Conduct causing loss of property

Though the concept of damage is flexible in its application to different kinds of harm to property, it does not readily extend to all forms of physical interference which impair use or enjoyment. Conduct which results in loss of the property need not involve damage or destruction. A person who cuts the painter of a launch which drifts from its moorings and is not seen again, is no doubt liable for the damage to the painter. Since the fate of the launch is unknown, liability for damage cannot be imposed. Depending on circumstances, it is quite likely that the launch is in excellent condition, having been appropriated by an unscrupulous finder.

It would be absurd, in such a case, to make liability for criminal damage depend on whether the malefactor had the wit to untie the painter, rather than cut it. The definition of damage is extended accordingly to include physical loss of the property as a consequence of physical interference with the property, such as removal of restraint over the property or abandonment of the property.

24 Compare the Canadian draft code prepared by the Canadian Law Reform Commission, which also requires specific legislative provision before liability for harm resulting from an omission is imposed. The Canadian Draft Code imposes no duties to preserve property from damage or destruction: Report: *Recodifying the Criminal Law* (No31, 1987) p87.

Code

Interference resulting in loss of use or function

Conduct which results in loss of use or function of property can amount to criminal damage. This element of the definition draws on South Australian law, which extends the meaning of “damage” to include conduct which makes property useless or inoperative.²⁵ The Code provision is more limited, however, than the South Australian definition, which will extend to some conduct which appears to be far removed from anything which would ordinarily count as damage. A person who took another’s car keys from their usual hook on the wall and hid them for a time might be said to “damage” the car, according to the extended South Australian definition.

In the Code, loss of use or function will only amount to damage if it results from physical interference with the property. The definition would exclude the case where a motor car was immobilised by taking the keys from their usual hook. The definition of damage would apply, however, if the keys were taken from the ignition, with the consequence that the car could no longer be used.

The provision will have the effect of penalising some conduct which results in temporary interruption of the use of property. Conduct of this nature is barely distinguishable from the activity of the unauthorised borrower, which the Committee declined to classify as theft in Chapter 3 of the Code.²⁶ Complete consistency between the offences of criminal damage and theft is an unattainable goal however. The law of criminal damage has no counterpart to the requirement of “intent to deprive permanently”, which excludes dishonest borrowing from the ambit of theft.

Though the Code requirement of physical interference narrows the application of the definition it is broader, in one respect, than its South Australian counterpart. The Code provision extends to instances in which any function or use of the property is lost as a consequence of the interference, though other functions or uses may remain.

Cases which call for the application of the provision will be rare. Almost always, loss of use or function will involve damage to the property in the conventional sense of the word. An Irish case in which mink breeding stock were released from captivity without authorisation provides an example. Though the mink

25 *Criminal Law Consolidation Act* 1935 s84(1). Compare the proposal of the Law Reform Commission of Canada for an offence of “vandalism” in *Recodifying the Criminal Law* (No31, 1987), pp86-88, which similarly proposed liability for physical interference with property which renders it useless or inoperative.

26 Model Criminal Code - Chapter 3: *Theft, Fraud, Bribery and Related Offences* (1995), p73: Though dishonest borrowing clearly infringes property rights, theft should be reserved for cases where the victim has suffered a permanent loss: remedies in tort provide a sufficient response for temporary takings.

Code

were recaptured and suffered no physical injury, they could not be individually identified and, lacking verifiable pedigree, were no longer of use as breeding stock. Though the court held that the mink had been damaged, the decision is probably unsustainable on the conventional meaning of damage.²⁷ The Code provision would apply, however, since release of the mink put an end to their use as breeding stock.²⁸

27 *Rexi Irish Mink Ltd v Dublin C.C.* (1972) IR 115: Held that the mink had been damaged because they were virtually worthless once they lost their identities. ATH Smith doubts the correctness of the decision that conduct which diminishes *value* amounts to damage, in the ordinary sense of the word: *Property Offences* (1994) 27 - 15.

28 One submission took issue with the conclusion that the conduct of the mink liberators would cause a loss of the "use or function" of the mink. It was suggested that physical interference which results in loss of the use or function of property should be supplemented by a reference to causing "diminution of the value of the property": Sir Harry Gibbs, 28 March 2000. The Committee is of the view that this would involve too radical a departure from the central defining elements of criminal damage, which emphasise requirements of tangible harm. Though the issue is certainly debateable, the Committee remains of the view that the liberated mink had lost their use or function as breeding stock, once their identities were lost.

4.1.3 Person to whom property belongs

- (1) For the purposes of this Part, property *belongs* to any person having possession or control of it, or having in it any proprietary right or interest (not being an equitable interest arising only from an agreement to transfer or grant an interest or from a constructive trust).
- (2) If property is subject to a trust, the persons to whom it belongs include any person having a right to enforce the trust.
- (3) If property belongs to 2 or more persons, a reference in this Part to the person to whom the property belongs is a reference to all those persons.

CHAPTER 3 - MODEL CRIMINAL CODE

For purposes of comparison, Chapter 3 contains the following definitions:

“Person to who property belongs

14.5 For the purposes of this Chapter, property belongs to any person having possession or control of it, or having in it any proprietary right or interest (not being an equitable interest arising only from an agreement to transfer or grant an interest or from a constructive trust).

Belong to another - interpretation

- 15.5(1) If property is subject to a trust, the persons to whom it belongs include any person having a right to enforce the trust. Accordingly, an intention to defeat the trust is an intention to deprive any such person of the property.
- (2) If property belongs to 2 or more persons, a reference in this Division to the person to whom the property belongs is a reference to all those persons.”

4.1.3 Person to whom property belongs

“Belonging To Another”

The definition shares common elements with the definition of the same expression in Chapter 3: *Theft, Fraud, Bribery and Related Offences*. It omits, however, provisions in that Chapter which define an owner’s interest by reference to certain obligations attaching to property.²⁹ Those provisions, which were necessary in offences aimed at dishonest usurpation of rights of ownership, are unnecessary in offences of criminal damage. In this respect, the Code follows the UK *Criminal Damage Act 1971*.³⁰ With the exception of arson (s.4.1.7), liability for criminal damage requires proof of damage to property belonging to another.

The decision to limit the offence of criminal damage to conduct which harms property belonging to another departs, in one respect, from the model provided by the *Criminal Damage Act*. Prior to the passage of that Act, English law recognised two exceptions to the rule that property which is the subject of the offence must belong to another:

- Liability was imposed for malicious damage when property was destroyed by its owner with the intention of defrauding another;
- Liability was also imposed when an owner destroyed property in circumstances where the lives of others were endangered.

Criminal damage legislation in most Australian jurisdictions preserves one or both of these exceptions to the rule that the offence is limited to conduct which damages property belonging to another.³¹ Though usual in criminal damage legislation, neither exception appears necessary.

The Law Commission concluded that the law of criminal damage was inappropriate as a vehicle for penalising fraud and, as a consequence, the UK Act contains no provision penalising owners who destroy their own property with intent to defraud.³² The same conclusion follows under the Model Criminal Code. Individuals who destroy their own property with intention to defraud are caught by the preparatory offences in Chapter 2: *General Principles of Criminal Liability*. If the conduct can be said to have passed beyond the stage of mere preparation, the owner will be liable for an attempt or a conspiracy

29 In particular, obligations to “retain and deal” with property “in a particular way” [MCC s15.5(2)] and the obligation to return property transferred by mistake [MCC s15.5(3) and (4)].

30 Discussed, ATH Smith, *Property Offences* (1994) paras 27-32.

31 Jurisdictions which preserve both exceptions, with considerable variety of form, include: New South Wales: *Crimes Act 1900* ss195, 196, 197; Queensland: *Criminal Code Act 1899* ss459(2), 469; Victoria: *Crimes Act 1958* s197(2), (3); Tasmania: *Criminal Code Act 1924* ss267, 269A; ACT: *Crimes Act 1900* s128(2), (3). The Northern Territory *Criminal Code Act 1983*, s238 preserves the rule that the offence of criminal damage extends to individuals who destroy their own property with intent to defraud. By contrast, the criminal damage provisions of the South Australian *Criminal Law Consolidation Act 1935* restrict liability to damage caused to property belonging to another.

32 Law Commission No.27, paras 19-20.

Code

| |
|--|
| |
|--|

to commit one or more of the offences in Chapter 3: *Theft, Fraud, Bribery and Related Offences*. If the owner has not reached the point where conduct could be said to amount to an attempt or conspiracy, there is no more justification for imposing criminal liability in this instance than in any other instance of conduct which is merely preparatory to fraud.

The Law Commission took a different view, however, of conduct which damages property in circumstances where the offender recklessly endangers life. The *Criminal Damage Act 1971* declares that ownership of the property is irrelevant in such a case. The Law Commission recommendation on this point appears, however, to have been provisional. The Commission remarked that the inclusion of the special endangerment offence might be reconsidered when reform of the law of offences against the person was further advanced. In the event, the law of offences against the person remains uncodified in Britain³³ and the endangerment offence was included when the *Criminal Damage Act* was passed in 1971.³⁴ It is unnecessary to deal with conduct which endangers life in this Chapter. Model Criminal Code - Chapter 5: *Non Fatal Offences Against the Person* imposes liability for recklessly endangering others: see Division 7 - Endangerment. There is no need for an additional provision in Chapter 4, which could only apply when the conduct which endangered others did so by causing damage to property.

Property is taken to belong to any person who has possession or control or a proprietary interest in it. A disgruntled mortgagor who damages or destroys property to satisfy a grudge against a mortgagee will be liable for offences under the Code.³⁵

The offence of arson [4.1.7] is an exception among the criminal damage offences in not requiring proof that any other person had possession, control or a proprietary interest in the property.

Shared ownership

Section 4.1.3(3) is identical in effect to s15.5(6) of Chapter 3: *Theft, Fraud, Bribery and Related Offences*. These provisions ensure that criminal damage and offences of dishonest acquisition impose liability on part owners who violate the rights of other part owners by damage or dishonest acquisition of jointly owned property.

33 For a brief account of the British path to reform and a discussion of recent developments, see Smith, "Offences Against the Person: The Home Office Consultation Paper" [1998] Crim LR 317.

34 See s1(2) *Criminal Damage Act 1971* (UK). ATH Smith, *Property Offences* (1994) 27-74 remarks that the "offence is more properly classifiable as an offence against the person".

35 Compare *Holden* (1998) 103 A Crim R 70.

4.1.4 Threats

For the purposes of this Part:

- (a) a threat may be made by any conduct, and may be explicit or implicit and conditional or unconditional, and
- (b) a threat to a person includes a threat to a group of persons, and
- (c) fear that a threat will be carried out includes apprehension that it will be carried out.

4.1.5 Causing damage or other result

For the purpose of an offence under this Part, a person causes damages or any other result if the person's conduct substantially contributes to the damage or other result.

4.1.4 Threats

Chapter 4 proposes offences of threatened sabotage [Part 4.3] and an offence of threatening property damage in circumstances involving a substantial risk of causing fear of serious personal injury [s4.1.9]. In addition to these Code offences, the Committee proposes a summary offence of threatening injury to property. The law of unlawful threats to harm property intersects with offences proposed in Chapter 5: *Non-Fatal Offences Against the Person*.³⁶

In view of the complementary intersection of the threat offences in Chapter 5 and related threat offences in Chapter 4, the definitions are identical in substance. Threats may be explicit or implied from conduct and the problems which have occasionally arisen concerning the status of conditional threats are avoided.³⁷ Fear includes “apprehension”, so ensuring that the offence is committed even though the nominal victim of the offence may face the threatened danger with icy detachment or nerves of steel.

4.1.5 Causing damage or other result

The legal concept of causation coincides, for the most part, with the commonsense application of the concept.³⁸ The occasion for an explanation of causation arises most commonly in cases involving homicide or infliction of personal injury. In these cases Australian courts accept the view that the prosecution can prove the existence of a sufficient causal link if it can be shown that the conduct of the accused made a substantial causal contribution to death or injury. It is not necessary to establish that the defendant’s conduct was the sole cause.³⁹ The provision makes it clear that the same rule applies to the offences involving property damage.

A similar provision defining the causal element in the Part 4.2 computer offences is included in s4.2.3(3).

³⁶ See Division 6 - Threats and Stalking.

³⁷ *Rosza v Samuels* [1969] SASR 205.

³⁸ *Royall* (1990-1991) 172 CLR 378.

³⁹ The requirement of causation in offences against the person is discussed at greater length in Model Criminal Code - Chapter 5: *Fatal Offences Against the Person* (Discussion Paper, June 1998) 25-31

Division 2 - Offences

4.1.6 Damaging property

(1) A person who:

- (a) causes damage to property belonging to another person, and
- (b) intends to cause or is reckless as to causing damage to that or any other such property,

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 4.2.5 (Unauthorised modification of data to cause impairment), or
- (b) an offence against section 4.2.6 (Unauthorised impairment of electronic communications).

Note. Section 4.1.11 provides for persons who damage property with consent. The defence applies to other offences against this Part.

Division 2 Offences

4.1.6 Damaging Property

Elements of the offence

Physical elements

- Conduct causing damage to property:
- Property is damaged if it is:
 - (1) destroyed;
 - (2) physically lost as a consequence of interference with the property, including any removal or restraint over the property or abandonment of the property.⁴⁰
 - (3) diminished by a loss of use or function;
 - (4) defaced⁴¹ or, in the case of a document or writing, obliterated or rendered illegible in whole or in part;⁴²
 - (5) in the case of an animal, harmed or killed and in the case of a plant or other thing forming part of the land, severed from the land.

Fault elements

- intention to cause or recklessness as to a risk of causing damage to property belonging to another person.⁴³ The fault elements for the property damage, like those for the Chapter 5 offence against the person, follow the common law convention of transferred malice. A vandal who throws a stone with the intention of breaking a streetlight will be guilty of criminal damage though the stone misses its target and breaks a window instead.

40 Compare *Criminal Code Act* (NT) s242 which seems to be an attempt to solve a similar problem: "does an act that tends to the immediate loss...of a ship in distress." To damage or destroy property requires an act which directly causes one or other consequence. A prohibition against causing loss requires a comparable restriction.

41 Compare *Crimes Act* 1900 (ACT) s131, "defacing premises".

42 Compare *Criminal Code Act* (NT) 1983 s1 "'damages'... when used in relation to a document or writing, includes obliterating and rendering it illegible either in whole or in part".

43 It was suggested in one submission that specification of the fault required for the offence is unnecessary in view of s5.6(2) of the Criminal Code, which requires proof of recklessness in the absence of a legislative specification of fault: see Commonwealth Director of Public Prosecutions 13 March 2000, per Justin McCarthy, Senior Assistant Director. The Committee concedes the logic of the submission but remains of the view that the benefits of informative redundancy outweigh the virtues of austerity in this context.

Code

Penalty

- Imprisonment for 10 years.

Nature and rationale of the offence

Criminal damage is distinguished from the Chapter 3 offences of theft and fraud primarily by the absence of any acquisitive motive prompting the harm to another's interest in property. The offence is committed though the damage to the property may be slight or repairable and though the owner's use and enjoyment of the property may be only marginally impaired.⁴⁴ In that sense, criminal damage extends to a broader range of harms to property than theft, which is limited by the requirement that appropriation must be done with an intention to deprive the owner permanently of the property. When criminal damage results in destruction of property or permanent loss, however, the offences can overlap. In the old case of *Cabbage*,⁴⁵ the offender was convicted of stealing a horse which he took and killed in order to destroy evidence against a friend.

The offence of theft, which began as an offence requiring proof of physical violation of another's right to possession of property, now includes dishonest usurpation of rights of ownership to intangible property. By comparison, the law of property damage remains far closer to its roots as crime of physical interference with tangible property. Though the Code proposes an extension of liability for conduct which causes loss of property, rather than damage in its more usual sense, the provision still requires proof of an act of interference which results in physical loss.⁴⁶ That restriction is meant to ensure that the offence does not extend to instances of mismanagement, involving no physical interference with the property, which might result in a loss of rights, title or value. Harm of that nature is regulated by Chapter 3: *Theft, Fraud, Bribery and Related Offences*, which requires proof of dishonesty before conviction.

Liability is not graded by reference to financial loss

The offence of criminal damage, like theft and obtaining by deception, does not divide into serious and less serious grades of offending. Though Chapter 4 does make provision for the more serious offences of arson [4.1.7], bushfire [4.1.8] and sabotage [Part 4.3], these prohibitions are aimed at distinctive kinds of wrongdoing. They are not aggravated forms of a basic offence of criminal damage.

44 British cases touching the question whether there is a level of damage so trivial as not to incur criminal liability are inconclusive: see ATH Smith, *Criminal Damage* (1994) 27-18.

45 (1815) 168 ER 809.

46 "Interference" requires "tampering" or other activity involving some direct physical contact with the object of interference: see *Galvin* (1998) 102 A Crim R 568 at 575.

Code

| |
|--|
| |
|--|

Australian jurisdictions vary in their approach to the question whether criminal damage legislation should grade levels of liability by reference to the financial loss resulting from the offence.⁴⁷ On this issue, as on others, the Committee has been influenced in its decision to propose a single, unified offence of criminal damage by the close relationship between criminal damage and theft. In the absence of any distinction among different grades of stealing by reference to the value of the property stolen, no reason is apparent for treating criminal damage differently in this respect.⁴⁸ In practice, actual or potential losses involved in offences of criminal damage, theft or obtaining by deception will play a significant role in determining penalties. Cases involving minor damage or loss will be tried summarily and, in any event, the extent of actual or potential harm will be taken into account in determining a proportionate sentence for these offences.

Fault - Intention and Recklessness

No distinction is drawn between damage intentionally inflicted and damage recklessly inflicted. Nor is liability imposed for damage resulting from negligent conduct. The law of criminal damage is markedly different, in this respect, from the offences against the person in Chapter 5. Offences involving harm to persons assume the existence of the principle that all persons are equal, where violations of the right to physical integrity are concerned. Damage to property is different. There is no underlying, monolithic idea of a right to inviolability of property, which corresponds to the idea that each person has an equal right to respect for their physical integrity. It would be incongruous if a person who destroyed an aircraft by recklessness were to be liable to a lesser penalty than a bar patron who smashed a beer glass intentionally.

The Principle of Transferred Malice

An offender who throws a stone at an ornamental gaslamp and smashes a window instead commits the offence of criminal damage though the possibility of smashing the window was unforeseen. The same principle of transferred malice applies in offences against the person, when conduct meant to cause injury to one person unexpectedly injures another.⁴⁹ When the intended target and the unintended object of destruction are of roughly equivalent value, as will often be the case in cases of criminal damage, there is no reason to distinguish between the culpability of those who hit their intended target and those who fail to do so. Distinctions will have to be drawn, of course, when an act intended to cause minor harm misses its intended target and causes catastrophic and

⁴⁷ See pages 2 - 4 for more detail.

⁴⁸ Compare the approach taken in the American *Model Penal Code* ALI 1962 ss220.3 and 223.1, which grade the offences of "criminal mischief" by reference to the financial loss resulting from the mischief and theft by reference to the value of the property which is stolen.

⁴⁹ Compare Model Criminal Code, Chapter 5 - *Non-Fatal Offences Against the Person* ss5.1.14, 5.1.15, 5.1.16, all of which relate the fault element to the person injured or "any other person".

Code

| |
|--|
| |
|--|

unforeseen damage to other property. In general, penalties for criminal damage, like the penalties for physical injury, are aggravated when the damage is severe. But proof that the actual damage far exceeded the offender's expectations will mitigate the penalty, which might otherwise be imposed for harm of such magnitude.⁵⁰ The case is no different, in essence, from one in which unexpectedly severe damage is caused to the intended target of the offender's destructive endeavour.

In England, the *Criminal Damage Act 1971* accepts the principle of transferred malice, though the issue has been the subject of controversy.⁵¹

Though there is an undeniable element of constructive liability in provisions which utilise the principle of transferred malice, the Committee is of the view that reliance on the principle is justified by the consequential economy and simplicity achieved in the definition of the offences of criminal damage.⁵²

Damage is a physical element of the offence, objectively defined

Damage is not in the eye of the beholder. Property is damaged if any ordinary person would consider it to have been damaged.⁵³ If Donald paints Donna's house purple, with yellow polka pots in the misguided belief that she will be surprised and pleased by his officious meddling, he damages her house.⁵⁴ Conviction is not automatic in such a case. Though Donald's mistake does not affect the objective quality of his act as damage he may escape conviction, on the ground that he believed that Donna would have consented to his colour scheme, had she known of his plans: see s4.1.11.

50 See *Storey* (1996) 89 A Crim R 519; *Olbrich* (1999) 108 A Crim R 464 on proof of actors which aggravate or mitigate punishment.

51 Section 1(1) of the Act, which imposes liability for damaging property when a person intends or consciously risks damage to "any such property" was intended to import the principle of transferred malice. Law Commission, No 29 (1970), *Report on Offences Against Property*, para 45; Ashworth, "Transferred Malice and Punishment for Unforeseen Consequences" in *Reshaping Criminal Law* (1978 ed PR Glazebrook) 77 at 91-92. Glanville Williams, who conceded that the Act achieves this result, thought the application of the principle in offences of criminal damage unwarranted: see his *Textbook of Criminal Law* (2ed 1983) 908; and "Convictions and Fair Labelling" (1983) 42 Cambridge LJ 89.

52 Compare Ashworth's defence of transferred malice, *ibid*, 93 - the economy and simplicity achieved by recourse to the principle "can be regarded as outweighing the occasional case of injustice in which liability is in substance constructive - particularly as any injustice can be minimised by proper sentencing policy".

53 Compare *Fancy* [1980] Crim LR 735; discussed ATH Smith, *Property Offences* (1994) 27-23.

54 One submission made the point that Donald could not be said to have intended damage or to have caused damage *recklessly*, if he believed the house much improved by his bizarre decorative scheme: see Commonwealth Director of Public Prosecutions 13 March 2000, per Justin McCarthy, Senior Assistant Director.

Code

| |
|--|
| |
|--|

Penalty

The ten year penalty for the offence is the same as the penalties for the Chapter 5 offence of intentionally causing harm to a person and the Chapter 6 offence of trafficking in a small quantity of a controlled drug. The offence of criminal damage is most nearly comparable, however, to the Chapter 3 offence of theft, which is also punishable by imprisonment for ten years.⁵⁵

⁵⁵ Though the offences are nominally distinguished by the requirement, among others, that theft requires proof of an intention to deprive permanently, neither property damage nor theft need involve destruction or permanent loss of the property. An intention to deprive a person permanently of a limited interest, such as possession under a bailment, will amount to theft, though the offender has no intention to retain the property permanently. Moreover the meaning of intention to deprive permanently is extended, by s15.6, to include circumstances where there is no intention to cause permanent loss of “the thing itself”. In terms of fault elements, theft and property damage deal with moral wrongdoing of a comparable order.

4.1.7 Arson

(1) A person who:

- (a) causes damage to a building or conveyance by means of fire or explosive, and
- (b) intends to cause or is reckless as to causing, damage to that or any other building or conveyance,

is guilty of an offence.

Maximum penalty: Imprisonment for 15 years.

(2) A person who:

- (a) makes to another person a threat to damage any building or conveyance belonging to that other person or a third person by means of fire or explosives, and
- (b) intends that other person to fear that the threat will be carried out or is reckless as to causing that other person to fear that the threat will be carried out,

is guilty of an offence.

Maximum penalty: Imprisonment for 7 years.

(3) In the prosecution of an offence against subsection (2) it is not necessary to prove that the person threatened actually feared that the threat would be carried out.

(4) In this section:

building includes:

- (a) a part of a building, or
- (b) a structure (whether or not movable) that is used, designed or adapted for residential purposes.

conveyance means motor vehicle, motorised vessel or aircraft.

4.1.7 Arson

Physical elements:

- cause damage;
- by fire or explosive;⁵⁶
- to any building, dwelling, airplane, motor vehicle or motorised vessel.

Fault elements:

- intention or recklessness

Penalty:

- 15 years imprisonment

Nature and rationale of the offence

Arson is a crime with a “splendidly evocative” name⁵⁷ in search of a coherent rationale for its existence. Penalties for arson invariably exceed the penalties for criminal damage. Yet the only difference between arson and criminal damage, in many jurisdictions, is that arson requires proof of damage by fire or explosives. A number of jurisdictions do not restrict the application of the offence to any particular kind of property.⁵⁸ New South Wales legislation is typical in its definition of arson as property damage of any kind caused by fire or explosives and in the increased penalty imposed for arson.

A variety of reasons have been given for distinct offences of criminal damage and arson. Two, in particular, capture the essence of the case for retaining the offence:

- Arson has always been regarded with particular abhorrence,⁵⁹ and
- Uncontrolled fire is an inherently unpredictable means of destruction.⁶⁰

56 Most Australian jurisdictions couple fire and explosive. For exceptions, see *Criminal Code Act* 1983 (NT), ss239, 241, 251(3).

57 JC Smith & B Hogan, *Criminal Law* (5 ed 1983) 649.

58 Compare *Criminal Code* (Qld) s461 which prohibits setting fire to buildings, structures, vessels, stacks of cultivated vegetable produce, stacks of mineral or vegetable oil, mines or their fittings, aircraft or motor vehicles. Succeeding sections prohibit setting fire to crops and growing plants and the use of explosives to damage property. For similar schemes, see: *Criminal Code Act* (Tas) s269A, *Criminal Code Act* 1983 (NT) ss239, 241, 251(3).

59 See ATH Smith, *Property Offences* (1994) 27-81, relating the reasons which led the UK Law Commission to recommend retention of a distinct offence of arson. The Commission was also concerned to ensure the indefinite detention of mentally disturbed arsonists. Since the *Criminal Damage Act* 1971 (UK) makes arson punishable by life imprisonment, retention of the offence allowed the mentally disturbed arsonist to be kept in detention indefinitely for psychiatric treatment, pursuant to an order under the *Mental Health Act* 1959.

60 *Ibid.*

Code

| |
|--|
| |
|--|

Granting the persuasive effect of these considerations, the distinction between arson and criminal damage, in New South Wales and jurisdictions with similar legislation, is crudely lacking in discrimination. There is no justification for imposing sharply augmented penalties simply because my documents, furniture, camera or clothing are consumed in a bonfire rather than obliterated, smashed, or torn to shreds.

The Committee is of the view that the offence of “arson” - a well understood and evocative term of criminal condemnation - should be retained in the Code. But the offence should be brought into closer alignment with ordinary, lay understanding of the scope of the offence.

The core meaning of the offence is apparent from dictionary definitions of ordinary usage:

- Shorter Oxford English Dictionary: “Arson...The act of wilfully and maliciously setting fire to another man’s house, ship, forest, etc...”
- Macquarie Dictionary: “Arson...the malicious burning of a house or outbuilding belonging to another...”

A separate offence of arson, with a higher penalty than the basic offence of criminal damage, possesses the virtues of familiarity and public support. The justification for retaining the offence is essentially the same as the justification for retaining a distinct offence of burglary. The fact that a compound offence could be eliminated by dissecting its parts and enacting distinct offences does not necessarily justify such an exercise. The advantages of retaining legal definitions of crime which match commonsense categories of wrongdoing should not be abandoned lightly.

The Code provision is limited to fire raising which involves specified forms of property. In this respect the proposed Code provision departs from existing prohibitions in some jurisdictions which would permit, on a literal reading, life imprisonment for setting fire to another person’s cigar without consent.⁶¹

61 The proposal to restrict the offence elicited fewer responses than expected. The Law Society of New South Wales agreed with the proposal: submission 22 June 2000, per John North, President. Two submissions took issue with the proposal. Both suggested that arson should extend to damage caused by fire or explosion to any form of tangible property: Model Criminal Code Review Committee, Western Australia, 20 March 2000, per Hon Justice Scott; Australian Institute of Criminology, 6 April 2000, per Dr Russell Smith. Both asserted that arson is ordinarily taken to include damage to items of personal property, if they are consumed by fire. The assertion is contradicted by Australian and English dictionary definitions. Neither submission took issue with the reasons advanced by the Committee for its restrictive definition of the offence. A submission by Sir Harry Gibbs, 31 March 2000, proposed a limited extension of the offence to include fire damage to haystacks, crops and timber. Though arson traditionally extended to haystacks, crops and timber, the Committee preferred the narrower version of the offence proposed in the Discussion Paper. Most instances of fire damage to standing crops or standing timber will be caught by the new offence of Bushfire, in s4.1.8. In a post agricultural society, there is no particular reason why the law of criminal damage to property should single out, for especially condign penalties, fire damage to felled timber or harvested agricultural produce.

Code

| |
|--|
| |
|--|

The core of the offence is the prohibition of setting fire to a dwelling or workplace.⁶² Liability is extended to cases involving fire or explosive damage to motor vehicles, aircraft and motorised vessels.

The place of arson in the Model Criminal Code

The risks of catastrophic spread of fire and of consequential injury to persons explain, to a considerable extent, the demand for special offences or special penalties when property damage results from fire. Code provisions in Chapter 5 which impose liability for conduct which risks injury to persons and the proposed bushfire offence [4.1.8], support and complement the case for a more discriminating definition of the offence of arson.

Arson may involve danger of injury or death. It is, however, both unnecessary and confusing to enact special provisions in criminal damage legislation which would penalise conduct which causes or risks death or personal injury from fire. Offences of reckless endangerment in Chapter 5: *Non Fatal Offences Against the Person*, propose severe penalties for offenders who endanger life, whether by lighting fires or by other dangerous conduct.

There is an obvious need, in all Australian States and Territories, for legislation which strikes at intentional, reckless and even negligent conduct which causes or risks bushfire or other forms of wildfire. The harm which results from bushfire or wildfire is not limited to damage or destruction of buildings, plant and crops, which are the concern of criminal damage legislation. The destruction of fauna, habitat and flora may be no less deplorable, even though there is no damage to property which belongs to another person.

The Code proposes an offence, described simply as “bushfire”, in s4.1.8. It carries the same penalty as arson.

Arson and property ownership

The offence is exceptional in its extension of liability to owners who damage or destroy their own buildings, vehicles, vessels or aircraft by fire or explosives. Existing legislation tends to confine the offence to fire or explosive damage to property belonging to another.⁶³

Two considerations persuaded the Committee to disregard ownership in defining the elements of the offence. The Code limits arson to a restricted range of property and liability is qualified by the provision of a defence of claim of right: see s4.1.12. As to the first of these considerations, the uncontrolled or capricious use of fire or explosives to destroy or damage buildings, vehicles, vessels or aircraft is

⁶² Originally, it would seem, an agricultural building such as a barn.

⁶³ *Criminal Damage Act 1971* (UK) s1(3); *Crimes Act 1958* (Vic) s197(6); *Crimes Act 1900* (NSW) s195; *Crimes Act 1900* (ACT) s128(4), s129. Special provision is made, in each of these jurisdictions, for augmented penalties when owners use fire or explosives to destroy their own property in the knowledge that life will be endangered or in order to defraud.

Code

| |
|--|
| |
|--|

highly likely to cause public alarm, public expense and public nuisance. Those harmful consequences will often follow, regardless of the fact that the person who does the damage happens to own the property in question. Harm or potential harm to the public at large, consequent on the nature of the property affected and the means employed, are more significant elements in this offence than they are in the lesser, general offence of property damage.

There are occasions, of course, when demolition or destruction by fire or explosives are unexceptionable. Section 4.1.12, in Division 3 allows a defence of claim of right, which will justify or excuse any reasonable work of demolition or destruction by fire or explosives. The defence, in common with other Code defences, requires a person accused of the offence to point to some evidence which suggests the possibility that the conduct was justified or excused. There is no blanket immunity for owners which would allow them an unqualified right to damage or destroy their own property by fire or explosives.⁶⁴

Claim of right requires evidence that the defendant believed that their proprietary right or interest authorised the use of fire or explosives as the means of causing damage or destruction. The owner's right to damage or destroy the property by other, less alarming, methods is not in issue.

To avoid misunderstanding, the committee emphasises that owners who use explosives or fire to destroy their own property remain potentially liable to penalties for a range of offences if they threaten⁶⁵ or endanger the well being of others.⁶⁶ They are also liable for offences of dishonesty if the damage was done in order to defraud.

Consent and Damage by Fire or Explosives

A person who uses fire or explosives to damage or destroy a building or conveyance may do so with the consent of the owner or another person entitled to authorise the use of those means. Section 4.1.11 supplies a defence of consent in such cases. Since the owner's right to use force or explosives is not absolute, the defence of consent extends to instances of mistaken belief that the person who gave the consent was entitled to do so.

64 One submission expressed concern that an owner who used fire or explosives to destroy or damage a building or conveyance without intent to defraud or other improper motive would be required to justify or excuse their conduct: Sir Harry Gibbs, 31 March 2000. In this respect, the offence places the owner in a more onerous position than existing law. The issue is whether legislation should attempt to specify in advance the range of improper motives which would make the owner's use of fire or explosives to destroy buildings or conveyances unlawful. Plain cases of demolition or disposal aside, the destruction of buildings or conveyances by fire or explosives seems a sufficient cause for social concern and a requirement of some account from the owner of the reasons for resort to those means. The burden of explanation is not heavy, the defence of claim of right is broadly drawn. An honest belief that ownership entitled the person to destroy or damage the property by fire or explosives is sufficient to excuse their use and the prosecution will bear the burden of proving the absence of that honest belief.

65 Model Criminal Code - Chapter 4, s4.1.9 Threat to cause property damage - fear of death or serious harm.

66 *Ibid*, Chapter 5, s5.1.25, Recklessly endangering life; s5.1.26, Recklessly endangering serious harm.

Code

Penalty

The penalty of 15 years imprisonment accords with penalties imposed by legislation in the Australian Capital Territory and Victoria.⁶⁷ Elsewhere, penalties vary in severity.⁶⁸

67 *Crimes Act 1958* (Vic) s197, *Crimes Act 1900* (ACT) s129.

68 *Criminal Law Consolidation Act 1935* (SA) s85, life imprisonment for damage exceeding \$25,000; *Criminal Code Act* (NT) s239 - life imprisonment, s241 - 14 years imprisonment; *Criminal Code Act 1899* (Qld) s461, life imprisonment; *Criminal Code Act Compilation Act 1913* (WA) s444, 14 years imprisonment; *Criminal Code Act* (Tas) s268, 21 years imprisonment.

4.1.8 Bushfires

(1) A person:

- (a) who causes a fire, and
- (b) who intends or is reckless as to causing a fire, and
- (c) who is reckless as to the spread of the fire to vegetation on property belonging to another,

is guilty of an offence.

Maximum penalty: Imprisonment for 15 years.

(2) In this section:

causing a fire includes:

- (a) lighting a fire,
- (b) maintaining a fire,
- (c) failing to contain a fire, except where the fire was lit by another person or the fire is beyond the control of the person who lit the fire.

spread of a fire means spread of a fire beyond the capacity of the person who caused the fire to extinguish it.

4.1.8 Bushfires

Elements

Physical elements:

- lighting a fire; or
- maintaining a fire; or
- failing to contain a fire lit by the person - unless the fire was beyond control
- substantial risk of spread to vegetation
- on property belonging to another

Fault elements:

- intentional or reckless lighting, maintaining or failure to exercise control; and
- recklessness as to a substantial risk of spread to vegetation on property belonging to another.

Penalty:

- 15 years imprisonment

Nature and rationale of the offence

Arson is an aggravated form of criminal damage and limited, like criminal damage, to conduct which harms the property rights of particular individuals. With the exception of the Western Australian *Bushfires Act 1954*, existing legislation appears to make no provision for a crime of comparable gravity directed at individuals who start bushfires.⁶⁹ Offences of criminal damage, which are concerned with harm to individual property interests, do not adequately reflect the harm to collective or community interests involved in bushfires.

Bushfires Act 1954 (WA)

s32 Offences of lighting or attempting to light a fire likely to injure

A person who -

- (a) wilfully lights or causes to be lit or attempts to light a fire; or

⁶⁹ State and Territorial legislation dealing with bushfires tends to impose comparatively light penalties for specific prohibitions against behaviour likely to cause bushfire, grassfire or other rural wildfires or lighting fires which might endanger person or property. See, for example: *Bushfires Act 1936* (ACT), Part V; *Rural Fires Act 1997* (NSW), s100; *Country Fires Act 1989* (SA) s52; *Bushfires Act 1996* (NT, Part III).

Code

- (b) places a match or other inflammable or combustible substance, matter or thing in a position so that it may directly or indirectly be ignited by the rays of the sun or by friction or other means, or be exploded or set on fire, or whereby a fire may be lit or caused and with the intent to cause a fire,

under such circumstances as to be likely to injure or damage a person or property, whether the fire be caused or not, is guilty of an indictable offence.

Penalty: \$250,000 or 14 years imprisonment or both

Context aside, there is nothing in the Western Australian Act to confine the operation of the provision to bushfires. Unlike the proposed Code offence, the Western Australian provision requires proof of a risk of injury or damage to person or property. The Code offence, which imposes liability when there is a substantial risk of fire spreading to vegetation on land belonging to another, does not require proof that injury or damage was likely. Unlike the Western Australian offence, which appears to impose strict or absolute liability with respect to the risk of damage to person or property, the Code offence requires proof of recklessness with respect to the risk that the fire will spread.

The proposal for an offence of causing a bushfire was among the more controversial recommendations made in the Discussion Paper. A submission by the Victorian Police argued in favour of a general offence of property damage, with aggravated penalties when damage is caused by fire or explosives.⁷⁰ It was suggested that the provision of distinct offences of criminal damage, arson and bushfire “complicates policing”. Complication is unavoidable, however, if aggravated penalties are attached to distinct physical elements of an offence. In principle, liability to an aggravated penalty on proof of different physical elements is the primary ground for distinguishing between offences: see *Courtie* [1984] AC 463.⁷¹ The Law Society of New South Wales, which agreed on the need for a distinct offence, argued in favour of a restriction to cases where the offender caused the fire to spread maliciously.⁷² It is unlikely, however, that a requirement of “malice” would affect the ambit of prohibition of the offence, which requires proof of recklessness with respect to the risk. In current jurisprudence, concepts of recklessness and malice are usually taken to be equivalent in meaning and references to “malice” are best

70 Victoria Police 5 April 2000, per s Neil O’Loughlin Deputy Commissioner, Policy and Standards.

71 See, in addition, appellate proceedings in the High Court, consequent on the decision of the South Australian Court of Criminal Appeal in *Cheng* (1999) SAS 175, *Cheng v R* [2000] HCA 53 (5 October 2000).

72 Law Society of NSW 16 June 2000, per John North, President.

Code

| |
|--|
| |
|--|

avoided in view of the long and unhappy history of legal disputes over the meaning of the term. On the other hand, a requirement of *intention* to cause the fire to spread would impose unwarranted limitation on the scope of the offence. A submission from the Australian Institute of Criminology urged expansion of the offence, to include cases in which a person created a risk of fire, as for example by depositing a large quantity of petrol on grassland near a roadway.⁷³ If the petrol was deposited with the intention of starting a fire, the case would fall within the reach of the law of attempt (see Chapter 2, Model Criminal Code - *General Principles of Criminal Responsibility* s 11.1). In the absence of such an intention, this hypothetical scenario and others which might be imagined, are appropriate targets for regulatory legislation dealing with particular forms of risk taking behaviour.

After consideration of the alternatives, the Committee concluded that the essence of the offence is to be found in conduct which creates a risk of an uncontrolled spread of fire to vegetation on land which is not owned or occupied by the offender. Damage to vegetation may be of great or little moment. For some species of Australian flora, fire is beneficial to procreation of the species. The real gravamen of the offence is the creation of a risk, which may or may not eventuate, of catastrophic damage to property, life or environment.

The primary subjects of the prohibition are those individuals who start fires on property over which they have no proprietary interest. A person who lights a fire on land owned and occupied by another commits the offence if there is a substantial risk that the fire will spread to vegetation *on that land or adjoining land* and the person is reckless with respect to that risk.

Liability is also incurred by occupiers or owners who light fires on their own land in the realisation that there is a substantial risk of spread to neighbouring properties. The penalty for the offence is severe but justifiable, in worst case scenarios involving owners or occupiers. Moreover they face comparable liability to punishment for arson, if fire started on their own property escapes and damages their neighbours' buildings or vehicles.

An offence of reckless endangerment

Unlike arson and criminal damage, the bushfire offence is predicated on the creation of risk rather than the infliction of harm. The reason for the offence is the a risk of catastrophe, unpredictable in extent and consequences, rather than injury to individual rights of ownership over vegetation.

⁷³ Australian Institute of Criminology 6 April 2000, per Dr Russell Smith.

Code

| |
|--|
| |
|--|

The fault element

The bushfire offence requires proof of intentional or reckless causation of the fire and recklessness, at the least, as to the spread of the fire on property belonging to another. Unlike most offences in the Model Criminal Code, there is a latent element of constructive fault in the definition of the offence. Though it is necessary to prove that the offender was aware that fire might spread, there is no need to prove awareness of the substantial risk of catastrophic consequences. There is a similar discrepancy between the fault elements which must be proved and the severe penalty for the offence.⁷⁴ Compare, for example, the difference between the 10 year penalty for endangering life in Chapter 5 and the 15 year penalty for this offence, which does *not* require proof of recklessness with respect to the risks of harm to life or property involved in starting bushfires. So long as the offender realises the risk that the fire will spread, there is no need for proof of realisation of the extent of the horror which may follow.⁷⁵ This offence has a very particular connection to Australian ecology and the commemoration of Australian rural history in Black Mondays, Black Thursdays and Black Fridays. The balance among the elements which go to the proof of guilt and imposition of punishment differentiate this offence from almost all others in the Code.

The defence of consent

Consent is a general defence to the property damage offences: see 4.1.11. The defence is expressed in terms of consent by “the person entitled to consent to the damage to the property concerned.” The defence is equally applicable to the bushfire offence, though it is an offence of endangerment rather than of damage to property. The person entitled to consent to damage to property is also a person entitled to consent to a risk of fire spreading to their property.

Owners and occupiers can be expected to act from self interest in preserving their properties from fire. If consent was given to the lighting of the fire - as will usually be the case when employees, contractors etc are working on the owner or occupier’s property - no liability should result even though the firefighter realises that there is a risk that the fire will spread beyond control.

It is the consent of those whose properties are endangered by spread of the fire which provides the evidential basis for the defence. Owner A’s consent will not protect an offender who realises that there is a risk that a fire lit on A’s property will spread to owner B’s property.

74 The range between the worst case and the least is far broader here than in most other offences. That breadth of application reflects the incalculable risks associated with bushfires.

75 One submission proposed an even heavier penalty, of 25 years imprisonment, to match the penalty for arson: Australian Federal Police 28 April 2000, per John Guerts, Director Technical Operations. The pronounced difference in fault elements between the offences suggests that equivalent penalties would breach the principles of proportionality in punishment. Bushfire offences which cause injury to persons or damage to buildings or conveyances should be prosecuted as offences against the person or arson, in addition to the instant offence.

Code

| |
|--|
| |
|--|

Consent of an owner or occupier will not, of course, displace the liability of workers or contractors for offences committed against regulatory legislation imposing fire bans or other fire controls.

4.1.9 Threat to cause property damage—fear of death or serious harm

- (1) A person who:
- (a) makes to another person a threat to damage property, and
 - (b) is reckless as to causing that other person to fear that the carrying out of the threat will kill or cause serious harm to that other person or a third person,

is guilty of an offence.

Maximum penalty: Imprisonment for 7 years.

- (2) In the prosecution of an offence against this section it is not necessary to prove that the person threatened actually feared that the threat would be carried out.
- (3) In this section, serious harm has the same meaning as it has in Part 5.1.

Division 2 - Offences

4.1.9 Threat to Cause Property Damage - fear of death or serious harm

Physical Elements

- Threat to another person
- To damage property

Fault Elements

- Intention to make a threat; and
- Recklessness as to the risk that the person to whom the threat is made will fear that the threat will be carried out, resulting in death or serious harm to another person.⁷⁶

Penalty

Imprisonment for 7 years

Nature and rationale of the offence

Though this offence takes the form of a prohibition involving threatened damage to property, its primary role is to supplement Chapter 5: *Non Fatal Offences Against the Person*. The Chapter 5 offences of threatening serious harm [Division 6] and endangerment [Division 7] do not extend to cases where the defendant threatened harm to *property* in circumstances involving recklessness to the risk that the person to whom the threat is made will fear injury to that person or to another.⁷⁷ Threats to set fire to dwellings are the most obvious examples of such conduct. Apart from the fact that the offence is limited to threats to damage property, it is expressed in very similar terms to the Chapter 5 offences of threatening death or serious harm: see ss5.1.20, 5.1.21. Like the offence of arson, this prohibition draws no distinction between threats to destroy property which belongs to another and property which belongs to the offender. The essence of the offence is the creation of a substantial risk that the person to whom the threat is made will fear that someone will die or suffer serious harm.

Each of the three Chapter 4 offences which involve threats is directed against significant and serious criminality. Threatened arson [s4.1.7] and threatened sabotage [Part 4.3] are primarily concerned with threats to cause major property damage. This offence will extend to threats of minor property damage, if the

⁷⁶ Section 5.4(4), Model Criminal Code - Chapter 2: *General Principles of Criminal Liability*, ensures that the offence will extend to cases in which the offender intends to induce fear.

⁷⁷ Compare *Criminal Damage Act 1971* (UK) s1(2), which creates the offence of dangerous damage, which covers conduct which would fall within Model Criminal Code - Chapter 5. In *Property Offences* (1994) 27 - 72, ATH Smith remarks that the British offence "could quite properly be classified as [an offence] against the person".

Code

| |
|--|
| |
|--|

threatened action involves a risk of serious harm or death. So, for example, a threat to damage safety devices or alarms by a quite minor act of interference might induce the most serious concern for public safety.

The draft offence is more discriminating in its effect than the corresponding offence in the UK *Criminal Damage Act 1971*, versions of which has been adopted in Victoria, New South Wales and ACT⁷⁸ and other Australian jurisdictions. The UK provision combines, in a single offence, threats to destroy property belonging to another and threats to destroy the offender's own property in a way which is likely to endanger another person.⁷⁹ The combination yokes together conduct involving trivial wrongdoing with serious criminality. The penalty of 10 years imprisonment for threats was no doubt intended for cases in which the threat would endanger life, if it was carried out.⁸⁰

The Committee is of the view that the British offence of threatened property damage is over inclusive in its effects. There is a significant difference between mere threats and conduct which causes actual property damage.⁸¹ Though the Committee accepts the necessity for an offence of threatening to damage property, in circumstances which do not involve sabotage, arson or potential danger to other people, the offence should be summary rather than a Code offence.

Threats

Like other Chapter 4 offences involving threatening conduct, s.4.1.9 does not require proof that the person to whom the threat was made feared that it would be carried out. The offence is committed even if the person to whom the threat is made knows very well that safety precautions have been taken which effectively disarm the offender's threats.

As in other offences involving threats, "fear" does not require proof that the victim panicked, suffered personal distress or disquiet or that the offender intended to produce these effects. The offence may be committed by an offender who intends to induce a state of rational and calm apprehension that serious harm could follow if the threat was carried out. Often the threats will be made to individuals whose duties or employment will require just such a cool appreciation of the risks and a rational deployment of preventive measures: see s4.1.4(c).

78 See *Criminal Damage Act 1971* (UK), s2; *Crimes Act 1958* (Vic), s198; *Crimes Act 1900* (NSW) s199; *Crimes Act 1900* (ACT) s132.

79 *Criminal Damage Act 1971*, s2.

80 Compare *Crimes Act 1958* (Vic), which substantially adopts the UK scheme of offences. The Victorian provision distinguishes between the penalties for the s197(1) offence of criminal damage [level 5 imprisonment] and s198 offence of threatening damage [level 6 imprisonment].

81 Section 11.1(1) Model Criminal Code - Chapter 2: *General Principles of Criminal Liability*, imposes the same penalty for attempted and completed offences.

Code

| |
|--|
| |
|--|

Fault element

Though proof of threat to damage property is required, it is not necessary to prove an intention to carry out the threat. Nor is it necessary to prove that the offender intended to induce fear that the threat will be carried out or that lives may be endangered. Recklessness to the risk that the other person might fear death or serious harm, as a consequence of the threatened conduct, is sufficient. In this respect, the offence is more inclusive than its British counterpart, which does require proof of an intention to induce fear.⁸²

The expansive scope of the Code offence is justifiable. Individuals who make serious threats may claim, in retrospect, that it was all a joke and not seriously meant. Some jokes are, indeed, transparent. A threat to paint Sydney Harbour Bridge pink, unless the Olympic Games include an event for marching bands, is harmless hyperbole. But jokes and hoaxes are close kin and the consequences of hoaxes involving threats of serious harm can be expensive and disruptive.⁸³ The Code requires those who realise the risk that hyperbole might be taken seriously to desist or face the possibility of criminal prosecution.

Serious harm

The definition of “serious harm” in this offence is drawn from Chapter 5. It means harm that “endangers, or is likely to endanger a person’s life”; or harm that “is or is likely to be significant and longstanding”. Unlike the corresponding offence in the UK *Criminal Damage Act 1971*, the Code provision does not require proof that anyone would have been injured had the threat been carried out.⁸⁴

Penalty

The penalty of seven years imprisonment is the same as the penalty for the closely related Chapter 5 offence of threatening to cause serious harm: see s5.1.2.

82 See s2, *Criminal Damage Act 1971* (UK): Making a threat, “intending that the other would fear it would be carried out”. So also in *Crimes Act 1958* (Vic) s198; *Crimes Act 1900* (NSW) s199. Compare *Crimes Act 1900* (ACT) s132, which resembles the proposed Code offence in the absence of any requirement for proof of an intention to cause fear.

83 Existing offences in some jurisdictions create offences of making false reports of danger to property or person: see *Crimes Act 1900* (NSW) s203; of the *Criminal Code Act 1924* (Tas) s276AA.

84 *Criminal Damage Act 1971* (UK) Section 2 imposes liability for threats to damage property in a way which the offender “knows is likely to endanger life”. The literal effect of this reference to “knowledge” is to require proof that the threatened act would in fact endanger another. See ATH Smith, *Property Offences* (1994) 27-91.

Summary offence

Threat to cause property damage

- (1) A person who:
 - (a) makes to another person a threat to damage property belonging to that other person or a third person, and
 - (b) intends that other person to fear that the threat will be carried out,is guilty of an offence.
Maximum penalty: Imprisonment for 2 years.
- (2) In the prosecution of an offence against this section it is not necessary to prove that the person threatened actually feared that the threat would be carried out.

Summary Offence

Threat to cause property damage

Elements of the offence

Physical Elements

- Threat to another person;
- to damage property;
- belonging to any other person.

Fault Elements

- Intention to make a threat; and
- Intention to induce the other person to fear that the threat will be carried out.

Penalty

Imprisonment for 2 years

Nature and rationale of the offence

The summary offence of threatened property damage is intended to supplement a range of serious Code offences which impose criminal liability for threatening arson [4.1.7(2)] or sabotage of public infrastructure [Part 4.3], endangering physical safety or well being by property damage [4.1.9]. Though any threat of damage to property belonging to another will fall within the scope of the offence, it is intended for use against minor offenders, whose threats exceed socially acceptable levels of hyperbole.

Sensible exercise of prosecutorial discretion is obviously necessary in enforcement of the prohibition. Circumstances might possibly justify prosecution of an irate householder who threatens to kill the neighbour's barking dalmation unless it is silenced. It is more difficult to imagine circumstances which would justify prosecution of the same irate householder for a threat to burn the neighbour's football if it lands among his roses just one more time.

The offence should be distinguished from existing indictable offences of threatened property damage in Victoria, New South Wales and Australian Capital Territory,⁸⁵ all of which were intended to extend to threats which could induce fear of personal injury associated with property damage.

⁸⁵ *Crimes Act 1958* (Vic) s198; *Crimes Act 1900* (NSW) ss199; *Crimes Act 1900* (ACT) s132. See also *Criminal Code Act* (Tas) s276, *Criminal Code Act 1983* (NT) s257 and *Criminal Code Act 1899* (Qld) s478, which create offences of sending a letter &c threatening to burn or destroy property.

Code

| |
|--|
| |
|--|

Fault elements

The offender must intend to induce fear. The summary offence is different, in this respect, from the indictable offences of threatened arson [s4.1.7(2)] and threatened property damage involving risk of personal injury [4.1.9]. In these offences, recklessness as to the effect of the threat on the victim is sufficient: the potential harm associated with the victim's apprehension of the threatened harm may be distressing to individuals and require costly precautions to avert the threatened harm. In this offence, which is directed at threats of a less serious nature, a requirement of proof of intention to induce fear will have the effect of excluding some conduct too trivial for criminal penalties.

A person who makes a threat to damage property belonging to another may or may not intend to be taken seriously. The threat may have been meant to be taken as a joke or as hyperbole. There is good reason to impose criminal liability even on jokesters and hoaxers, if the threats are of very serious harm and they are made in the realisation that they could be taken seriously by the person to whom they are made: see the discussion of s4.1.9. The same need to protect against the risk of causing unintended alarm or apprehension is not apparent when the threat is minor. The Committee is of the view that the summary offence should be restricted in its application to circumstances in which the threat was meant to be taken seriously or the person by whom it was made knew that it would be taken seriously.⁸⁶

Penalty

The penalty of 2 years imprisonment is appropriate for the comparatively lesser harm likely to result from the commission of this offence.

86 Model Criminal Code - Chapter 2: *General Principles of Criminal Responsibility*(1992) s5.2 equates realisation that a consequence of one's act is certain with intention to cause that consequence. Opinions vary on where the boundary should be drawn between criminal harms and conduct which is too trivial to warrant criminal prohibition. One submission argued in favour of liability for threats if the threatener realised that the person to whom the threat was made would take it seriously: Legal Aid Western Australia 31 March 2000, per George Turnbull, Director.

4.1.10 Possession of a thing with intent to damage property

- (1) A person who possesses any thing, with the intention that the person or another person will use it to damage property belonging to another, is guilty of an offence.

Maximum penalty: Imprisonment for 3 years.

- (2) In this section:

possession of a thing includes:

- (a) having control over the disposition of the thing (whether or not the thing is in the custody of the person), or
- (b) having joint possession of the thing.

4.1.10 Possession of a thing with intent to damage property

Elements of the Offence

Physical Elements

- Possess a thing

Fault Elements

- With the intention that it will be used by the person in possession, or another, to damage property which belongs to another.

Penalty

Three years imprisonment.

Nature and rationale of the offence

The prohibition against possession with intent is a preparatory offence and akin to similar offences proposed elsewhere in the Code. Chapter 6, which deals with serious drug offences, imposes criminal liability on anyone who is found in possession of things intended to be used for unauthorised manufacture of controlled drugs [s.6.3.8] or unauthorised cultivation of controlled plants [s6.3.16].⁸⁷ The closest analogy, however, is the offence of going equipped for theft, in Chapter 3 of the Code.

Offences of this nature are well known in existing law.⁸⁸ They are designed to impose criminal liability when the conduct of the accused falls short even of an attempt to steal, defraud or damage property. The essential element for guilt is the intention to commit the principal offence. Though the Code, like existing legislation, makes no attempt to specify the nature of the property intended for use in damaging property, proof of the offender's intention will normally depend on possession of some object or artefact which is peculiarly adapted to causing some particular form of damage.

Possession for use by the offender or another

The definition of possession has been drawn from Chapter 6: *Serious Drug Offences*.⁸⁹ It is intended to reflect common legal usage in existing case law. As an element in the definition of this offence, "possession" will rarely be problematic. The things which are commonly used to damage property are not exotic and possession of such objects or implements for lawful purposes is far more common than possession for an unlawful purpose. Only a tiny minority

⁸⁷ Model Criminal Code - Chapter 6: *Serious Drug Offences* (1998).

⁸⁸ See *Criminal Damage Act* 1971 (UK) s3 and Australian provisions which follow the same pattern: See *Crimes Act* 1958 (Vic) s199; *Crimes Act* 1900 (NSW) ss200; *Crimes Act* 1900 (ACT) s133; *Criminal Law Consolidation Act* 1935 (SA) s86.

⁸⁹ Model Criminal Code - Chapter 6: *Serious Drug Offences* (1998) s6.1.4.

Code

among those who possess sledgehammers will intend to use them to damage property belonging to another. The answer to the question whether possession of a sledgehammer will incriminate a suspect depends entirely on the circumstances attending possession. The question whether the suspect could be said to possess the sledgehammer is unlikely to arise. But disputes over the meaning and scope of possession can arise when the alleged means of destruction are more obviously incriminating or when possession of the thing is prohibited by other laws. In those circumstances, offenders can be expected to take steps to distance themselves from the source of incrimination. So, for example, cases involving allegations of possession of explosives with intent are likely to involve issues very similar to those which arise in the flourishing case law on possession of drugs.

Comparison with the offence of going equipped to steal

Though the offence of possession of a thing with intent is related in policy to the Chapter 3 offence of going equipped to steal, it is far broader in scope. Section 16.7 of Chapter 3: *Theft, Fraud, Bribery and Related Offences*, had its distant origins in offences of being in possession of picklocks, jemmies and other tools of the burglar's trade. Though the Chapter 3 of the Code avoids specifying the incriminating objects, the offence of going equipped to steal is restricted to things which the offender "when not at home, has with him."

There is, of course, a large area of overlap between the offences. An offender equipped with a sledgehammer and explosives for the purpose of forcing a door and cracking a safe can be convicted of either offence. Possession of a thing with intent to damage property is far less restricted in its applications, however, than going equipped for stealing. The comparative breadth of the offence is consequence of the fact that artefacts used for destruction are more various and more likely to be dangerous than the things which are used for the purpose of dishonest acquisition.⁹⁰

Possession on behalf of another

The offence is committed though the offender does not intend to use the thing personally. The provision is particularly likely to find application in these circumstances where explosives are involved in the plan to destroy property. If the intended destruction does eventuate, a person who supplied the means of destruction, knowing of its intended purpose, would be guilty as an accomplice. There is no liability, however, for an attempt to become an accomplice. The offence of possession with intent supplements the law of complicity and preparatory offences, catching those who intend others to do the dirty work.

Penalty

The penalty of three years imprisonment matches the penalty for the Chapter 3 offences of going equipped for stealing.

⁹⁰ The offence is supplemented by prohibitions against possession of false documents and devices for making false documents: See Model Criminal Code - Chapter 3: *Theft, Fraud, Bribery and Related Offences*, ss19.6, 19.7.

Summary Offence

Poaching

- (1) A person who intentionally takes, kills or injures any wild creature on land belonging to another is guilty of an offence.

Maximum penalty: Imprisonment for 2 years.

- (2) A person is not criminally responsible for an offence against this section if:
 - (a) the person engaged in conduct constituting the offence with the consent of the owner or occupier of the land;
 - (b) at the time of the conduct constituting the offence, the person believed that he or she had a right or interest in the wild creatures which authorised the person to engage in that conduct; or
 - (c) the person's conduct constituting the offence is justified or excused by any Act or other law.
- (3) In this section, wild creature means any live bird, mammal, fish (including crustacean) or amphibian that is not tamed or ordinarily kept in captivity or not reduced (or in the course of being reduced) into the possession of a person.

Summary Offence

Poaching

Elements of the Offence

Physical elements

- Take, kill or injure;
- On land belonging to another;
- a live bird, mammal, fish, crustacean or amphibian that is not:
 - (1) tamed or ordinarily kept in captivity; or
 - (2) reduced (or in the course of being reduced) into the possession of a person;
- Absence of authorisation whether by consent of the landowner or by lawful authority.

Fault Elements

- Intention to take, kill or injure;⁹¹
- Recklessness⁹² as to ownership of the land, absence of authorisation or the status of the creature.

Penalty

Imprisonment for two years.

Nature and rationale of the offence

Criminal damage, like theft and related offences, always involves an invasion of the rights of a property owner. Though the summary offence of poaching protects the interests of landowners, it is exceptional in its focus on creatures which are not owned by anyone.

The concept of “property” in Chapter 3 and Chapter 4 of the Code includes domestic animals⁹³ and wild animals if they are tamed, ordinarily kept in captivity,⁹⁴ in possession or in the course of being reduced to possession. So,

91 Model Criminal Code - Chapter 2: *General Principles of Criminal Responsibility* (1992) s5.6(1) declares that intention is the fault element for a physical element of an offence that consists of conduct.

92 *Ibid*, 5.6(2) requires proof of recklessness as to circumstantial elements of the offence unless contrary provision is made. Imposition of strict and absolute liability requires specific provision: see ss6.1, 6.2.

94 ATH Smith, *Property Offences* (1994), 3-52.

94 The definition in s14.4(d) MCC Chapter 3: Theft Fraud...&c is apt to include wild animals which escape from a circus or zoo, for they are “ordinarily kept in captivity” even if not “tamed”.

Code

for example, when fish and marron are farmed in special ponds, they are property belonging to the owner of the pond and they can be stolen. Unauthorised conduct which injures or kills them will amount to criminal damage. By contrast, fish and crustaceans taken from the wild are not covered by the offences of theft or criminal damage. Nor are wild kangaroos, goats, possums, foxes and rabbits.

POACHING: THE ENGLISH EXPERIENCE

In Britain, the *Theft Act* 1967, like the property offences in Chapter 3 of the Code, excludes liability for theft of wild creatures. Special provision was made for an offence of taking or destroying fish, however, in a schedule to the Act. This was intended as a temporary expedient, pending a more systematic review of the law relating to poaching. The English poaching offence, which still forms part of the Act, is as follows:

Theft Act 1967: Para 2(1), Schedule 1

[A] person who unlawfully takes or destroys or attempts to take or destroy any fish in water which is private property or in which there is any private right of fishing shall on summary conviction be liable to imprisonment for a term not exceeding three months....

Proof of an intention to keep the fish and the prohibition against “taking” fish extends to one who catches a fish, even if it is returned to the water alive.⁹⁵ Western Australia copied the UK provision in 1996⁹⁶ and extended the term “fish” to include crustaceans. Wild marron are, accordingly, protected in Western Australia. Under s437 of the *Criminal Code*, taking fish unlawfully is a summary offence, punishable by two years imprisonment or a fine of \$8000.

In Britain, a similar development occurred in relation to deer. A special summary offence of taking or destroying deer was included in the schedule to the *Theft Act*. Unlike the prohibition against taking or destroying fish, however, this provision has since been repealed. The *Deer Act* 1991 now prohibits pursuit or poaching deer on land belonging to another. That *Act* also introduced licensing schemes governing the trade in venison. Penalties are imposed for trafficking in meat which has been taken unlawfully.⁹⁷

95 ATH Smith, *Property Offences* (1994), 13.13. The prohibition is supplemented by special legislation directed at salmon poachers: *Salmon Act* 1981 (UK).

96 Act No 36 of 1996.

97 See also *Salmon Act* 1981 (UK), which introduced a similar scheme of licensed trade and prohibitions against unlicensed traffickers.

Code

| |
|--|
| |
|--|

The offence of poaching supplements theft and criminal damage by making it an offence to take, kill or injure wild creatures on another's land though they are not owned by anyone. This motley band of creatures includes animals native to Australia as well as wild buffalo, foxes, starlings, rats, rabbits, feral pigs and cats. It will include fish and crustaceans, whether native or introduced. In a jurisdiction which has fully developed legislation dealing with commercial exploitation of wild creatures and protection of native fauna, the poaching offence will play a marginal role. But even a marginal role is sufficient justification for imposing a minor criminal sanction for poaching. Schemes for the commercial exploitation of wild creatures are likely to develop long before detailed legislation to regulate the trade are enacted.

Quite apart from protection of nascent commercial enterprises, the contemplation of wild creatures on one's own property, the enjoyment of their company and, if that is one's bent, the pleasures of the hunt, are not trivial human goods. It is arguable that they are worth the protection, at least, of a summary offence. However a number of those who made submissions disagreed with the Committee on this issue.⁹⁸ The offence remains in the draft as a model which may be adopted in some jurisdictions. As a summary offence, it does not play a significant role in the scheme of Chapter 4 offences.

98 The proposal for an offence of poaching elicited sharp disagreement on the question whether such an offence was necessary: Victoria Police 5 April 2000, per Neil O'Loughlin Deputy Commissioner Policy and Standards; Law Society of NSW 16 June 2000, per John North, President; Legal Aid Western Australia 31 March 2000, per George Turnbull, Director.

Division 3 - Defences

4.1.11 Consent

A person is not criminally responsible for an offence against this Part if, at the time of the conduct constituting the offence:

- (a) the person entitled to consent to the damage to the property concerned had so consented, or
- (b) he or she believed that the person whom he or she believed was entitled to consent to the damage to the property concerned had so consented, or
- (c) he or she believed that that person would have so consented if that person had known about the damage to the property and its circumstances.

4.1.12 Claim of right

- (1) A person is not criminally responsible for an offence against this Part if, at the time of the conduct constituting the offence, the person believed that he or she had a right or interest in the property concerned which authorised the person to engage in that conduct.
- (2) In this section, a right or interest in property includes a right or privilege in or over land or waters, whether created by grant, licence or otherwise.

4.1.14 Self-defence

To avoid doubt, section 10.4 of Chapter 2 (Self-defence) applies to an offence against this Part.

Division 3 - Defences

4.1.11 Consent

Absence of consent is not an element of any of the offences in Chapter 4. The prosecution is not required to prove that the act was done without consent unless there is some evidence of consent or of mistaken belief in consent. In this respect, the role of consent in offences involving property damage is markedly different from its role in defining the Chapter 5 sexual offences against the person,⁹⁹ where absence of consent is an element of the offence forming part of the prosecution case.

The provision reproduces, in essentials, elements of the plea of “lawful excuse” in s5 of the UK *Criminal Damage Act* 1971, which have been adopted in Victorian and ACT legislation.¹⁰⁰

Absence of consent in property damage offences plays a role closely related to that of dishonesty in theft.¹⁰¹ Whether damage to property or appropriation of property is in issue, there is no criminal liability if the defendant’s conduct was actuated by a sincere belief that the person to whom the property belongs had consented or would consent, if the circumstances were known. As in the case of theft, an honest though plainly unreasonable belief defeats the charge of criminal damage.

99 Model Criminal Code - Chapter 5: *Sexual Offences Against the Person* (1999) Division 2 - Sexual Acts Committed without consent.

100 See *Criminal Damage Act* 1971 (UK) s5(2)(a) and Australian provisions which follow the same pattern: *Crimes Act* 1958 (Vic) s201(2)(b); *Crimes Act* 1900 (ACT) s130(1).

101 The *Theft Act* 1968 (UK) s2(1)(b) defines dishonesty by reference to absence of belief in consent. The Model Criminal Code makes no specific reference to consent in provisions defining dishonesty: see ss14.2, 15.2. Discussed: Chapter 3: *Theft, Fraud, Bribery and Related Offences* (1995) p15. The Committee is of the view that the rules relating to consent are implicit in the concept of dishonesty and do not require specific articulation in the Chapter 3 offences.

4.1.12 Claim of right

- (1) A person is not criminally responsible for an offence against this Part if, at the time of the conduct constituting the offence, the person believed that he or she had a right or interest in the property concerned which authorised the person to engage in that conduct.
- (2) In this section, a right or interest in property includes a right or privilege in or over land or waters, whether created by grant, licence or otherwise.

4.1.12 Claim of right

Chapter 2 of the Model Criminal Code allows a defence of honest, though mistaken, claim of right to property offences if the mistaken belief contradicts the fault required for the offence: see s9.5 of Chapter 2. So for example, it is not theft to take property belonging to another if it was taken in the sincere belief that it really belongs to the taker. Claim of right is equally available as a defence to a charge of criminal damage. A muddled property developer who confuses allotment numbers and begins to demolish the wrong house will face the prospect of a civil damages suit but not prosecution for an offence. Criminal sanctions for merely negligent conduct, which causes property damage, are unnecessarily draconic.

In most instances, the claim of right merely makes explicit what was implicit in the definition of the offence. The offences of damaging property [s4.1.5], bushfire [s4.1.8] and possession with intent [s4.1.10] all require proof that the accused was aware of the fact that the property in question belonged, or might belong, to another person. Arson [s4.1.7] is an exception to the general rule however. People who destroy or damage their own buildings or motor vehicles by fire or explosives can be convicted of the Code offence of arson. The range of perils, public nuisance and public alarm resulting from major fires or explosions requires something more in the way of excuse or justification than a mere claim to ownership of the affected property. Special provision is accordingly necessary in Chapter 4 to supplement the general defence of claim of right in Chapter 2 of the Code.

Owners who destroy their buildings, vehicles, vessels or aircraft by fire or explosives can rely on s4.1.12 to justify or excuse their conduct if they acted in the belief that they had “a right or interest in the property concerned which authorised...that conduct.” The excuse consists of two elements:

- A belief, which may be true or false, that the defendant had a right or interest in the property; and
- A belief, which may be true or false, that the right or interest authorised the person to engage in that conduct.

The second of these elements is of critical importance. In Chapter 4, the claim of right excuse is dependent on the defendant’s beliefs about the consequences which flow from ownership rather than on the fact of ownership itself.¹⁰² Where liability for arson is concerned, claim of right requires evidence of a belief that the defendant’s proprietary right or interest authorised the use of fire or explosives.

¹⁰² There is a parallel in the application of claim of right to the offences in Model Criminal Code Chapter 3, *Theft, Fraud, Bribery and Related Offence*. Section 9.5(1) of Chapter 2, *General Principles of Criminal Responsibility* requires a mistaken belief concerning possessory or a proprietary rights which “would negate a fault element” of dishonesty. Mere belief in a proprietary or possessory right, whether true or mistaken, will not immunise the accused from conviction for an offence of dishonesty. It is a commonplace of the law of theft that owners can be convicted of stealing their own property. The claim of right defence requires evidence that the accused believed that the proprietary or possessory right to the property conferred the right to do the act which is the subject of the criminal charge.

4.1.12 Claim of right

- (1) A person is not criminally responsible for an offence against this Part if, at the time of the conduct constituting the offence, the person believed that he or she had a right or interest in the property concerned which authorised the person to engage in that conduct.
- (2) In this section, a right or interest in property includes a right or privilege in or over land or waters, whether created by grant, licence or otherwise.

The defence also has potential application in cases where proprietary interests are divided. Criminal damage is committed when a part owner destroys or damages property without the consent of other part owners. Chapter 4, like Chapter 3: *Theft, Fraud, Bribery and Related Offences* (1995) defines with generous amplitude the expression, “belonging to another.” Property is taken to belong to any person who has possession, control or a proprietary right or interest in it. Individuals who may be aware that another person has an interest in the property may mistake the extent of their own rights to alter the property. Conflicts between part owners are particularly likely to arise in circumstances where one part owner’s attempts to improve, renovate or rehabilitate property are rejected by another part owner as vandalism. Individuals who act on a mistaken view of the extent of legal rights or powers conferred by their part ownership cannot avoid civil liability. But criminal penalties would be inappropriate in such a case.

Burden of proof

Claim of right does not arise for consideration unless there is evidence that the accused acted in the belief that the conduct was authorised by some right or interest in the property. Once the issue is raised, however, it is for the prosecution to prove beyond reasonable doubt that the accused did not hold the exculpatory belief. Part 2.4 of the Code, which deals with proof of criminal responsibility, governs the Chapter 4 defences. The general rules relating to proof are discussed in Part 6, Chapter 2: *General Principles of Criminal Responsibility* (1992).

4.1.13 Self-defence

To avoid doubt, section 10.4 of Chapter 2 (Self-defence) applies to an offence against this Part.

4.1.13 Self-defence

Situations in which damage or destruction of property may be justified or excused by the necessities of self defence are incalculable in their range and variety. Dog attacks may be met with whatever degree of force is reasonable to repel the attack and the terrorist's lethal device may be destroyed with impunity. Section 10.4 of the Code provides a general defence of self defence which applies alike to the Chapter 5 offences against the person and Chapter 4 offences of criminal damage. The elements of the s.10.4 defence are discussed in more detail in Chapter 2: *General Principles of Criminal Responsibility*.¹⁰³ The plea results in acquittal if the defendant acted in the belief that the response was necessary to defend person or property and if the response was reasonable, in the circumstances as the defendant believed them to be.

The application of self defence to the criminal damage offences involves, however, some idiosyncratic points which deserve mention:

- *Self defence includes destruction of property in order to avoid an attack which threatens personal injury*:¹⁰⁴ The Lone Ranger is excused if he must shoot Red Ryder in order to avoid being shot himself. It is better, however, if he can shoot Red's pistol from his hand, though the pistol will be irremediably damaged. The plea of self defence covers injury to Red Ryder and damage to his pistol as well.
- *Self defence includes defence of property from a threat of unlawful harm by a human agent*. A landowner who uses force against a trespasser to protect a lamb from slaughter, is justified or excused if reasonable force is used.¹⁰⁵ This provision avoids the anomaly apparent in Britain, Victoria and the Australian Capital Territory,¹⁰⁶ where the law takes a more humane attitude to misjudgments in the heat of the moment when property is at risk than it does when personal injury is threatened.¹⁰⁷
- *Self defence of property is limited to responses to threats of unlawful action by a human agent*. If the irate landowner kills the neighbour's dog to protect a lamb from slaughter, the plea of self defence is of no avail. The landowner must look instead to the defence of

103 *Ibid*, 66-69.

104 *Model Criminal Code* s10.4(2)(a) Conduct "to defend himself herself or another person".

105 *Ibid*, s10.4(2)(c) Conduct "to protect property from unlawful appropriation, destruction, damage or interference."

106 *Criminal Damage Act* 1971 (UK) s5(2)(b); *Crimes Act* 1958 (Vic) s201(2)(b); *Crimes Act* 1900 (ACT) s130(1)(c)(d)(e). In New South Wales, which adopted much of the British Act, conduct undertaken in defence of property falls within the inarticulate embrace of "lawful excuse": see, for example, s198 *Crimes Act* 1900 (NSW).

107 The anomaly is discussed at length in ATH Smith, *Property Offences* (1994) paras 27-68 - 27-71.

Code

| |
|--|
| |
|--|

sudden or extraordinary emergency: Chapter 2: *General Principles of Criminal Responsibility* s10.3(1). So also when property is destroyed to create a firebreak.

In most circumstances, justification or excuse for defensive action will require evidence of honest belief in the need for defensive action and reasonable response to the perceived threat, whether property damage or personal injury is threatened.

Burden of proof

Like all Code defences, self defence does not arise unless there is evidence that the accused did believe that the conduct was authorised by some right or interest in the property. Once the issue is raised, however, it is for the prosecution to prove beyond reasonable doubt that the accused did not act in defence of person or property. Part 2.4 of the Code, which deals with proof of criminal responsibility, governs the Chapter 4 defences. The general rules relating to proof are discussed in Part 6, Chapter 2: *General Principles of Criminal Responsibility* (1992).

PART 4.2 - COMPUTER OFFENCES

INTRODUCTION

State and Commonwealth laws dealing with computer crime are diverse in policy and partial in their application. Though the desirability of uniform legislation was recognised by the Standing Committee of Attorneys General in 1987, disagreements over the form which legislation might take have, until now, precluded any concerted approach to reform.¹⁰⁸

Two areas of concern in particular provided a focus for legislative concern. A number of jurisdictions have enacted special provisions aimed at those who use computers as a means to the commission of crime, usually crimes involving dishonest acquisition of money or financial advantage. Victorian legislation provides what is perhaps the most elaborate Australian example of legislation aimed at computer fraud.¹⁰⁹ Apart from fraud, legislative concern has been focused on the need to protect data and programs in computers from predators. The primary concern here is security of the system itself from unauthorised access, corruption or sabotage, rather than prevention of predatory gain or access to confidential information.

Though there is a diversity of approaches, four jurisdictions - the Commonwealth, New South Wales, Tasmanian and Australian Capital Territory - have enacted legislation which approaches uniformity. *The Review of Commonwealth Criminal Law: Interim Report on Computer Crime of 1988* conducted by Sir Harry Gibbs [*Gibbs Report*] provided the template for legislation in these jurisdictions. The original concern of the *Gibbs Report*, reflected in the Commonwealth legislation which implemented its recommendations,¹¹⁰ was the protection of data or programs “stored in [a Commonwealth] computer” from disclosure or corruption. New South Wales, Tasmania and ACT adopted the pattern proposed in the Gibbs Report, though the ambit or prohibition is broadened to include conduct which secures access to any computer data or programs, whether owned by government or a private citizen. Each of these jurisdictions has enacted special offences of causing damage to computer data or programs or obstructing the lawful use of computers.

108 Sullivan, “*The Response of the Criminal Law in Australia to Computer Abuse*” (1988) 12 Crim LJ provides a valuable critical survey of legislation prior to the Review of Commonwealth Criminal Law Interim Report on Computer Crime 1988 (Gibbs Report). See also S Krishcock, *The Criminalisation of the Unauthorised Accessing of Computer Systems* (1993), unpublished LLB Hons dissertation, University of Adelaide Law Library, Chap 3 for critical analysis of Australian legislation and proposals for reform.

109 *Crimes (Computers) Act* 1988 (Vic), inserting ss74(2), 80A, 81(4) and 83A in the *Crimes Act* 1958 (Vic), and inserting s9A in the *Summary Offences Act* 1966 (Vic).

110 *Crimes Act* 1914 (Cth) ss76Aff. Compare *Computer Fraud and Abuse Act* 1986 (US) 18 USC 1030.

In general, existing Australian legislation is aimed at conduct involving unauthorised access or use of data or programs. Though the Tasmanian Law Reform Commission once proposed an offence of unauthorised use of a computer, no Australian legislature has so far adopted the recommendation.¹¹¹

The UK *Computer Misuse Act 1990*, based on the UK Law Commission report, *Computer Misuse*,¹¹² provides a useful comparison with the Australian legislation. The Law Commission distinguished three areas for potential legislative action:

- *Protection of computerised data and programs from unauthorised access:* The British Act makes it a summary offence, punishable by 6 months imprisonment, if a person “causes a computer to perform any function with intent to secure [unauthorised] access to any program or data held in any computer.”¹¹³
- *Prevention of crime consequential on unauthorised access:* The basic offence of unauthorised access is aggravated when an offender obtains unauthorised access with intent to commit or facilitate commission of an offence punishable by five or more years imprisonment.¹¹⁴ This offence carries a penalty of five years imprisonment.
- *Protection of data and programs from corruption, whether by hackers or by persons who put virus infected discs or worms into circulation:* A person who causes “an unauthorised modification of the contents of any computer” is guilty of an offence punishable with five years imprisonment.¹¹⁵

The Law Commission made no specific recommendations with respect to legislation against computer fraud.¹¹⁶ Nor was the Commission particularly concerned to protect privacy. Such protection as the legislation affords to the preservation of secrets was no more than an incidental effect of measures enacted to preserve the integrity of the computer system from unauthorised access or attack.

111 *Report on Computer Misuse*, Law Reform Commission of Tasmania, Report No47 of 1986, recommendation 3(iii).

112 *Criminal, Law: Computer Misuse* Law Com No186, 1989.

113 *Computer Misuse Act 1990* (UK) s1(1)(a).

114 *Computer Misuse Act 1990* (UK) s2(1).

115 *Computer Misuse Act 1990* (UK) s3(1)(a).

116 *Ibid*, paras 2.5-2.7: The Law Commission considered it desirable to introduce measures which would deal with problems which arise when offenders “deceive” machines in order to obtain a commercial benefit or inflict a commercial loss. In view of the complexity of the issues involved, however, the Commission deferred consideration of the issue.

Though there are significant differences and variations, the proposals which follow are substantially derived from the Law Commission report and *Computer Misuse Act* 1990. That is a consequence, in the main, of the fact that the Committee was asked by the Standing Committee of Attorneys-General to base its proposals for reform of the law of theft and fraud in Chapter 3, *Theft, Fraud, Bribery and Related Offences* (1995), on the provisions of the UK *Theft Act* 1968. The *Theft Act*, together with the *Criminal Damage Act* 1971 and the *Computer Misuse Act* 1990 comprise a complementary scheme of legislation, with interlocking parts. Misuse of a computer or electronic communications for purposes of dishonest gain falls within the scope of the *Theft Act*, which deals with offences of dishonesty. Crimes involving unauthorised modification of computer data merge with offences of criminal damage. So, for example, it is at least possible that a hacker who causes a computer program failure by introducing a virus or worm might be caught by a simple prohibition against criminal damage to property. Care has been taken in the draft provisions to ensure that the computer offences and criminal damage are alternative bases for conviction in marginal cases: [ss4.1.6(2); 4.2.5(2); 4.2.6(2)].

In view of the interdependence of codes dealing with offences of dishonesty; criminal damage and computer offences, the Committee concluded that the UK *Computer Misuse Act* 1990 provided an appropriate basis for reform of Australian law. Though many changes have been made in adapting the United Kingdom model, the essential premises of that legislation remain unchanged. The draft provisions dealing with computer crime which follow, like the criminal damage offences in the preceding part of the Report, are intended to complement Model Criminal Code - Chapter 3, *Theft, Fraud, Bribery and Related Offences* (1995).

The *Computer Misuse Act* is now a decade old. The Council of Europe is currently engaged in formulating a Convention on Cyber-Crime¹¹⁷ which prescribes a scheme of computer offences for adoption by Council members. In the rapidly changing environment of cyberspace regulation, it was necessary to ensure that the United Kingdom Act had not been overtaken by more recent developments. Enquiries of the Law Commission elicited the information that no changes are currently proposed for the United Kingdom legislation. It should be noted, however, that the *Computer Misuse Act* does not extend to some of the preparatory offences proposed in the Draft Convention. The Committee's proposals go beyond the scope of the United Kingdom Act in certain respects. Those extensions include the preparatory offences of ss4.2.7 and 4.2.8. The offence of unauthorised access &c with intent to commit a serious offence (s4.2.4) goes well beyond its counterpart in the United Kingdom Act and the Part 4.3 offences dealing with sabotage, which extend to cyberterrorism, have no counterpart in the *Computer Misuse Act*.

117 Draft *Convention on Cyber-crime*, Draft No22, Revision 2, October 2, 2000. <<http://conventions.coe.int/treaty/en/projets/cybercrime.htm>>

The Committee also considered recent legislative initiatives in other jurisdictions. The New Zealand Law Commission reported in mid 1999,¹¹⁸ recommending a range of offences. In addition to proposals for offences of impairing computer data or security, the NZ Law Commission recommends measures intended to reform the law of telecommunications interception and offences of fraud, forgery and dishonest acquisition. The Committee's concerns are less expansive. Telecommunications offences are the subject of Commonwealth legislation and Chapter 3 of the Model Criminal Code, *Theft, Fraud, Bribery and Related Offences* (1995), makes provision for frauds involving computer misuse. In areas of common concern, involving unauthorised access and damage to data, the Committee has derived considerable benefit from consideration of the New Zealand report, though our conclusions are markedly different at some points.

In India, the *Information Technology Act of 2000*¹¹⁹ is primarily concerned to establish a regime in which electronic documents and communications are recognised in commerce and government. Though the primary concern of the Act is directed to regulation of commerce, it does contain "hacking" offences in addition to a range of statutory torts, allowing claims for civil compensation, by individuals who suffer loss as a consequence of unauthorised access to data or unauthorised data modification. These statutory torts, in Chapter IX of the Act, provide a more complete and detailed set of prohibitions than the criminal offences of Chapter XI. A person who suffers loss as a consequence of unauthorised access; hacker attack; unauthorised copying of confidential electronic information; denial of access; disruption of computer operations, impairment of data or certain frauds is entitled to recover compensatory damages up to a stated limit. The Indian legislation possesses considerable interest for its blending of civil and criminal modes of enforcement of strictures against hackers and others who gain unauthorised access, destroy data or impede communications. Since civil enforcement is geared to the recovery of provable loss, the statutory torts hold the promise of a more extensive coverage of categories of harm, coupled with greater discrimination in the application of prohibitions to particular instances of wrongdoing. Legislation which blends civil and criminal enforcement is, of course, familiar to Australian eyes. The great majority of legal actions for enforcement of prohibitions in Commonwealth trade practices legislation and State fair trading legislation involve civil actions for damages, rather than criminal prosecution. Similar developments in blended civil and criminal enforcement can be expected as Australian legislatures begin to elaborate schemes of regulation for electronic commerce.¹²⁰

118 *Computer Misuse*, Law Commission (NZ) No 54, May 1999.

119 Act no 21 of 2000. The Act and discussion of its contents can be viewed on the Ministry of Information Technology website: <<http://www.mit.gov.in>>.

120 Though the Commonwealth, New South Wales and Victoria have enacted electronic transactions legislation, in pursuance of a uniform scheme of legislation, the Acts are enabling rather than regulatory and do not make provision for civil or criminal enforcement of conventions governing electronic communications technology. See: *Electronic Transactions Act 1999*; (Cth); *Electronic Transactions Act 2000* (NSW); *Electronic Transactions Act 2000* (Vic).

Outline of Proposed Offences

It will be apparent that the Committee proposes a departure, sharp though far from radical, from the prevailing pattern of Australian legislation dealing with computer crime. In some respects, the *Gibbs Report* provided an inappropriate model for general State and Territorial legislation. The Gibbs Committee was concerned to recommend legislation which would protect *Commonwealth* computer and telecommunication systems from abuse for purposes of sabotage or gain. The focus on the protection of governmental interests inevitably biased the formulation of criminal offences. Factors which might justify the imposition of criminal penalties for unauthorised interference with governmental facilities will often be absent when private property is the target of interference. A prohibition against “use of a *Commonwealth* facility” to obstruct the lawful use of computer¹²¹ can be justified as a protection of governmental computer data. It is inappropriate, however, as a model for a general offence, under State law, of obstructing the lawful use of any computer by any means whatsoever.¹²² The explosive growth in the number of people using computers, the variety of uses to which they are put, coupled with the intractable problems of defining what is and what is not a computer, should preclude blunderbuss prohibitions of this nature. One might just as well argue for offences of impeding the lawful use of a television set or record player.

Though Chapter 4 offences are broadly equivalent to those in the UK *Computer Misuse Act* 1990, they are considerably more extensive in coverage and application.

- 4.2.4 - *Unauthorised access, modification or impairment to commit a serious offence*: A preparatory offence, penalising individuals who engage in unauthorised misuse of computer data with the object of committing another offence;
- 4.2.5 - *Unauthorised modification of data to cause impairment*: The offence prohibits unauthorised alteration or erasure of computer data.
- 4.2.6 - *Unauthorised impairment of electronic communications*: The prohibition is aimed at denial of service attacks.
- 4.2.7 *Possession of data with intent to commit computer offence*: A preparatory offence, akin to the more familiar offences of “going equipped for stealing” or possession of an offensive weapon.
- 4.2.8 *Supply of data with intent to commit a computer offence*: A preparatory offence, aimed at those who devise or traffic in programs which enable damage or unauthorised access to computer networks.

121 *Crimes Act* 1914 (Cth) s76E(b).

122 *Crimes Act* 1900 (NSW) s310B; *Crimes Act* 1900 (ACT) s135K(b).

- *Summary offence:* Unauthorised access to restricted data.
- *Summary offence:* Unauthorised impairment of data held in a computer disk, credit card, &c.

This code of prohibitions is supplemented by the sabotage offences of Part 4.3, which impose severe penalties for conduct which is intended to cause major damage or major disruption to government facilities and public infrastructure. These offences, which were developed from international proposals for anti-terrorism legislation, extend across the saboteur's destructive gamut, from bombs to computer viruses. The range of harms caught by the offences is equally broad, ranging from physical destruction of government buildings to major disruption of communications systems, as for example an attack, by electronic means, on the Australian Stock Exchange.

The Council of Europe Draft Cyber-Crime Convention

The Council of Europe is an international organisation made up of representatives of 41 European nations. In 1997 the Council constituted a "Committee of Experts on Crime in Cyberspace" to prepare a model code of offences involving computers and electronic communications. The outcome of their deliberations - the Draft *Convention on Cyber crime* was released in April 2000 and a revised version appeared in October of that year.¹²³ Nations which have participated in preparation of the draft include many which are not COE members. Most notable among them, perhaps, the United States. Substantial parts of the draft were prepared by the Computer Crime Division of the US Department of Justice. When completed, the convention will be open to signature by other nations, some of which participated in formulating its provisions, (for example, the United States).

Title 1 of the Convention provides a set of prescriptive requirements for a comprehensive code of "offences against the confidentiality, integrity and availability of computer data and systems". Chapter 4 of the Model Penal Code draws on the prescriptions of the Convention at a number of points. The preparatory offences of possess data with intent (s4.2.7) and supply data with intent (s4.2.8) are intended to match the requirements of Article 6 - *Illegal Devices*. With one exception, the computer offences proposed in Chapter 4 of the Model Criminal Code match the proposals of the Draft Convention. Though many forms of communications interception will be caught by Chapter 4, interceptions of communications by external means, which do not involve the execution of any function of the computer, are not. These fall more appropriately within the scope of legislation directed at unlawful interception of communications.

¹²³ Draft *Convention on Cyber-crime*, Draft No22, Revision 2, October 2 2000

<<http://conventions.coe.int/treaty/en/projects/cybercrime.htm>>

**DRAFT CONVENTION ON CYBER-CRIME 2000:
THE COMPUTER OFFENCES**

Title 1: Offences Against The Confidentiality, Integrity and availability of Computer Data and Systems

Under this heading, the Convention proposes the following offences:

- *Article 2: Illegal access to a computer system;*
- *Article 3: Illegal interception of transmissions of computer data;*
- *Article 4: Data interference, by damage, alteration &c or suppression¹²⁴ of computer data;*
- *Article 5: System interference, by “seriously hindering” the functioning of a computer system by data input, damage &c to data or suppression of data;*
- *Article 6: Illegal Devices - dissemination and possession: The offence is directed at devices which enable commission of an Article 2 or Article 5 offence.*

The Draft is not restricted to proposals for substantive offences: the titles which follow include provisions on jurisdiction, international co-operation and law enforcement. The Draft also proposes two offences which are intended to control the content of electronic communications. Child pornography and copyright breach are the subject of proposed prohibitions.

A proliferation of potential cyber-crimes

The computer offences of Chapter 4 extend familiar concepts of criminal damage or destruction of chattels to conduct which impairs computer data or electronic communication between computers. The evolution of the computer offences from the matrix of criminal damage is comparable to the evolution of modern offences of dishonesty from the gross physicalities of larceny, embezzlement and fraudulent conversion. Though the computer offences have evolved in this way to include wrongs to intangibles, the interests protected remain the same or closely analogous to those harmed by the more familiar instances of criminal damage. The primary purpose of the Code offences, in Chapter 4 and elsewhere, is to preserve what the *Report of the President’s Working Group on*

124 Notes to the Convention explain the concept of “suppression” as an amalgamation of two kinds of harm:

- deletion of data so that it ceases to exist; or
- “rendering data inaccessible” so that a person can no longer gain access to it, though it still exists.

*Unlawful Conduct on the Internet*¹²⁵ called “online-offline consistency.” In principle, “substantive regulation of unlawful conduct...should, as a rule, apply in the same way to conduct in the cyberworld as it does to conduct in the physical world.”¹²⁶

Adaptation of physical world legal concepts to the cyberworld generates the need for new applications of familiar concepts. There is a more difficult challenge ahead however. The expansion of communicative technologies will generate as well, demands for new forms of civil and criminal liability in the cyberworld which have no counterparts in the physical world. The Report of the President’s Working Group outlines the issues posed by the unprecedented communicative power of the Internet.

Although there are proposals to build identification mechanisms into Internet protocols...such proposals are controversial, because there are strong reasons to allow anonymity in communications networks. For example, whistleblowers may wish to remain anonymous, as may a group of rape victims who wish to convene an electronic meeting to discuss their experiences without revealing their identities.

[T]he differences between...traditional means of communication and the Internet is significant and attempts to solve Internet problems only by drawing analogies to existing technologies will often fail.... For example, the telephone and mail systems...allow predominantly one-to-one communications. Although someone wishing to defame a public figure anonymously or harass others can, in theory, call thousands of people anonymously, the time and cost make this impractical. By contrast, the cost free, simple, one to many nature of the Internet dramatically alters the scope and impact of communications....Given the complexity of the issue, balancing the need for accountability with the need for anonymity may be one of the greatest policy challenges in the years ahead.¹²⁷

125 *The Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet: A Report of the President’s Working Group on Unlawful Conduct on the Internet*(March 2000) <<http://www.usdoj.gov/criminal/cybercrime/unlawful/htm>>.

126 *Ibid*, at II.B.1, p13. There are limits, however, to imaginative exercises in constructing analogies: see Kaplan, “Treat Ebay Listings as Property? Lawyers See a Threat” *Cyberlaw Journal*, 28 July 2000 on the question whether a California court was right to extend the common law wrong of trespass to chattels to permit action against an online auction house which used a software robot to search a competitor’s auction listings: <<http://www.nytimes.com/2000/07/28/technology/28law.html>>

127 *Ibid*, at II.D.1, p23.

As the Report mentions elsewhere, drawing on a military analogy, the Internet is a “force multiplier.” The key elements in the mix are the potential for virtually cost free access to a mass audience, by individuals who can maintain anonymity or promulgate communications via assumed identities. The potentiality for disguise, encryption and anonymity have obvious implications for law enforcement. They give rise as well to demands for recognition of new forms of criminal behaviour. Several submissions drew on a report by the National Police Research Unit in support of the suggestion that there is need for specialised offences of cyberworld impersonation or identity theft.¹²⁸ Other submissions suggested an offence of “spam for an improper purpose”¹²⁹ Further afield, a section in the Report of President Clinton’s Working Group opens with the question: “Page Jacking - A New Type of Computer Crime?”. Page jacking is described as the appropriation of website descriptions, key words, or metatags¹³⁰ from other sites”.¹³¹

It is important to emphasise, however, that techniques and tactics involving encryption, the use of trademarks in metatags, bulk spam, anonymity and disguised identity are all capable of legitimate use. Legitimate resort to these techniques and tactics may, indeed, be more common than illegitimate use. None of these practices can be banned outright nor do they indicate that the individual is engaged in some nefarious enterprise. As Australian law stands at present, none identifies a course of conduct which could provide the basis for a criminal offence. In jurisdictions which have introduced specialised computer offences, the first step is the promulgation of a regulatory code which specifies permissible and impermissible modes of communication before imposing criminal penalties or civil liability for breaches of that code. The role of legislatures in establishing or maintaining Internet conventions of communication may prove to be relatively insignificant. Many current problems and opportunities for subterfuge will be rectified by technological development, driven by the competitive demands of the electronic market place. In commercial transactions the offences of misleading or deceptive conduct in trade practices and fair trading legislation will extend to many, if not all, appropriations of another’s trade marks or identities.¹³² To date, Australian legislatures have exercised a remarkable degree of restraint. With the exception of longstanding provisions dealing with interception of telecommunications, few if any attempts

128 Commonwealth DPP, 24 March 2000, per Geoff Gray, Assistant Director, adopting a report prepared by the National Police Research Unit, *Minimum Provisions for the Investigation of Computer Based Offences*, Report Series No 129.1; Police Commissioner’s Conference: Electronic Crime Steering Committee 2 May 2000, per MJ Palmer, Chair.

129 Submission, Australian Securities & Investment Commission, 27 April 2000, per Joseph P Longo, National Director, Enforcement; Police Commissioners’ Conference Electronic Crime Steering Committee, 2 May 2000, per MJ Palmer, Chair.

130 On metatag abuse, see B Allgrove, *Meta Tag Abuse: Where to Turn When the Law Falls Short* (2000), LLB honours dissertation, University of Adelaide Law Library.

131 *The Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet*, *op cit*.

132 The argument for regulatory restraint is advanced persuasively and in detail by B Allgrove, *Meta Tag Abuse: Where to Turn When the Law Falls Short*, *op cit*.

have been made to crystallise the conventions of electronic communications and subject those who violate them to criminal or civil sanctions. Recent electronic transactions legislation¹³³ is intended to facilitate the shift from paper communication to electronic communication in commercial and administrative relationships. No provision is made for sanctions or rules sustained by civil or criminal sanctions. The question whether Internet specific offences are necessary was raised directly in two submissions which proposed an offence of “spam for an illegal or improper purpose”. The proposal is discussed below.

Legislation against offensive content

The COE Draft *Convention on Cyber-crime* proposes legislative measures against child pornography. Two submissions argued in favour of a substantially broader set of prohibitions which would make it an offence to use the Internet to produce, possess or supply child pornography or material which promotes or depicts racial hatred, cruelty or violence.¹³⁴

The Committee makes no recommendation with respect to control over Internet content or possession of objectionable material on computer data bases. The arguments for and against legislative control of content are the subject of intense and continuing political debate.¹³⁵ The issues involved - whether of technology, morality or policy - are not issues on which the Committee can claim either special expertise or representative status. There is no lack of informed voices on these issues. In the circumstances, the Committee is of the view that entry into the arena of debate is unlikely to be productive.

Harassment and Cyberstalking

The offence of stalking, now accorded legal recognition in most Australian jurisdictions, is a comparatively recent conceptualisation of a distinct form of criminal conduct.¹³⁶ The conceptual novelty of the offence and its unusually

133 *Electronic Transactions Act* 1999 (Cth). The Act is intended to form part of a comprehensive uniform scheme with matching State and Territorial legislation. To date, two States have enacted matching legislation: *Electronic Transactions Act* 2000 (NSW); *Electronic Transactions Act* 2000 (Vic). The genesis of the legislation is discussed in depth on the Commonwealth Attorney General's website: <<http://www.law.gov.au/publications/e-commerce/legal.html>>. The United Kingdom has recently enacted similar legislation, *Electronic Communications Act* 2000, as has Singapore, see *Electronic Transactions Act* 1998.

134 Australian Federal Police, 28 April 2000, per John Geurts, Director Technical Operations; Commonwealth DPP, 24 March 2000, per Geoff Gray, Assistant Director, adopting a report prepared by the National Police Research Unit, *Minimum Provisions for the Investigation of Computer Based Offences*, Report Series No 129.1.

135 See *Broadcasting Services Amendment (Online Services) Act* 1999 (Cth). Academic criticism can be found in Scott, “The Dawn of a New Dark Age? Amendments to the *Broadcasting Services Act* (1999) 2 *Internet Law Bulletin*, 32; Penfold, “Censorship Legislation - Wrecking the Internet?” (2000) *National LR* 4.

136 Model Criminal Code - Chapter 5: *Non Fatal Offences Against the Person*, Report 1998 51ff provides a succinct account of the development of Australian laws against stalking.

evocative name can tend to obscure the fact that stalking, in its more serious manifestations, is a supplement to the more central and familiar offences of threatening death or injury. There is no need to resort to a charge of stalking when one person threatens to kill or injure another whether the threat is made orally, in writing or via the Internet.¹³⁷ The need to legislate against stalking was a consequence of the recognition that there are situations in which a person of ordinary fortitude would regard another's conduct as implicitly menacing, though no threat of any particular kind of injury is communicated.¹³⁸ Model Criminal Code - Chapter 5: *Offences Against the Person*, ss5.1.22 - 5.1.23 provides a canonical formulation of the offence. It requires proof that the defendant intended to induce fear that another person would be harmed, physically or mentally,¹³⁹ by conduct which can be described as "stalking" another. The definition of conduct which can amount to stalking lists a number of specific activities. None of them is necessarily objectionable even though they may be repeated on a number of occasions. It is the stalker's intention that the conduct should induce fear of physical or mental harm which transforms conduct which might otherwise appear innocuous, into a criminal offence. The activities include: following a person; loitering outside a place frequented by that person; telephoning the person; entry on another's property or interference with their property; exposing another person to offensive material or maintaining surveillance over them. To amount to stalking, the conduct must occur on at least two occasions. This itemisation of the typical repertoire of the stalker is supplemented by a sweeper provision which includes within the definition of stalking a repetition, on two or more occasions, of "acts...that could be expected to arouse a reasonable person's fear" of harm.¹⁴⁰

The Committee received one submission suggesting that Chapter 4 should include an offence of cyberstalking, as an element in a comprehensive coverage of crimes committed by means of computer technology.¹⁴¹ In the United States a number of jurisdictions have enacted offences which are specifically directed to Internet stalking or harassment.¹⁴² Media reports suggest that the

137 *Ibid*, ss5.1.19 - 5.1.21 and discussion at pp49ff.

138 Model Criminal Code - Chapter 5: *Non Fatal Offences Against the Person* (1998) p53: In its criticism of existing law, the report states that it does not cover the case where a "person causes another a degree of fear or trepidation by behaviour which is on the surface innocent but which, taken in context, assumes an importance beyond its immediate significance. Where a person does not explicitly threaten another, but silently follows them round, or sits outside their dwelling, it may be difficult to find the appropriate criminal sanction."

139 The concept of "harm" is defined expansively in Chapter 5, *ibid*, s5.1.2. The offence of stalking in s5.1.22 is committed where the conduct of the offender causes a person to fear for their own safety or the safety of a third person.

140 *Ibid*, s5.1.23(2).

141 Mark Williams JP, 12 March 2000.

142 A comprehensive selection of US harassment, stalking and cyberstalking laws can be found on WHOA [Working to Halt Online Abuse] <<http://www.haltabuse.org/laws.html>>.

phenomenon is both a cause for public concern and the subject of campaigns, by various interested groups, to intensify that level of public concern.¹⁴³

Should the Model Criminal Code make specific provision for an offence of cyberstalking? The question appears to involve three subsidiary issues:

1. Do the existing Code offences of threatening conduct and the supplementary offence of stalking adequately cover the range of activities which may be undertaken with the intention of inducing fear of injury?
2. Should liability be extended beyond conduct intended to induce fear of injury to harassment intended to induce fear of other kinds of harm; or conduct intended to cause significant levels of annoyance, embarrassment, shame or resentment?
3. If extension of existing Code offences dealing with threats is necessary, should the extension be restricted to conduct involving electronic communication?

Though the Code offences of threats and stalking cover a broad range of intimidatory conduct, they might be outflanked by human ingenuity in devising new forms of harassment and threatening behaviour. The *Report of the President's Working Group on Unlawful Conduct on the Internet*¹⁴⁴ provides the following example in support of its assertion that the Internet "provides new avenues for would-be stalkers to pursue their victims":¹⁴⁵

A rejected suitor impersonated his victim in various Internet chat rooms and online bulletin boards, where he posted, along with her telephone number and address, messages that she fantasised about being raped. On at least six occasions, sometimes in the middle of the night, men knocked on the victim's door, saying that they wanted to rape her. The offender pleaded guilty to a charge of stalking under California law and charges of inciting sexual assault.

The example is revealing on a number of levels. It is not a case in which human ingenuity outflanks the provisions of the Model Criminal Code. The conduct of the rejected suitor would fall within the scope of the offence of

143 "Personal cyber-attacks rise", Australian 7 November 2000.

144 *The Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet: A Report of the President's Working Group on Unlawful Conduct on the Internet* (March 2000) <<http://www.usdoj.gov/criminal/cybercrime/unlawful/htm>>. The Report draws on an earlier and more extensive consideration of the issues by the US Attorney General in *Cyberstalking: A New Challenge for Law Enforcement and Industry* (August 1999) <www.usdoj.gov/criminal/cybercrime/>.

145 *Ibid*, section IIA(3), at p12.

threatening serious harm.¹⁴⁶ That is not to say, of course, that it is impossible to imagine forms of menace which do fall outside the Code. Nor is it a case in which the menace takes a form which is peculiar to the Internet, though the communicative power of the medium must have increased the chances of locating men who would take the chat room messages seriously. The Californian scenario is, in fact, a sadistic variant on a well known form of urban harassment in which a practical joker induces undertakers, florists or real estate agents to deluge the victim with unwanted offers of their services.

The fact that threats may be made by electronic means provides no reason for enlarging the offences of threatening death or harm to individuals. These offences are quite general and apply no matter what the means chosen to make the threat.¹⁴⁷ The Code offence of stalking might well be improved, however, by explicit reference to Internet stalking. It makes specific mention of stalking by means of repeated telephone messages and it should be equally specific in relation to repeated electronic messages. Though stalking by Internet would be caught by the concluding sweeper clause, there are educative advantages in making the prohibition explicit.

Should provision be made for criminal penalties to be imposed where conduct is intended to cause annoyance, embarrassment, shame or resentment? In 1997 the United Kingdom enacted the *Protection from Harassment Act*, which creates a summary offence of "harassment."¹⁴⁸ The concept is not defined in the Act, beyond the requirement that a reasonable person would consider the conduct to be harassment. Nor is there any specification of the circumstances in which harassment can give rise to liability, though it is a defence to show that the conduct was reasonable in the circumstances. The arguments against indiscriminate prohibitions of this nature were canvassed in the Committee's Report, *Non Fatal Offences Against the Person*¹⁴⁹ and it is unnecessary to repeat them here. If a summary offence of this nature were to be introduced - an initiative which the Committee does not recommend - no reason is apparent why it should be limited in its effects to harassment by electronic communication.

146 Model Criminal Code - Chapter 5, s5.1.15. See, in addition, the summary offence of threatening harm, recommended in the Code Chapter 5: *Non Fatal Offences Against the Person*, Report 1998, p50. The offender, whose conduct induced the men to threaten to rape the victim, is liable for their acts under Chapter 2: *General Principles of Criminal Responsibility*, s11.2 Complicity or s11.3 Innocent Agency.

147 It is arguable, however, that explicit provision should be made to ensure that a threat to rape is equivalent to the Chapter 5, s5.1.21 offence of threatening serious harm.

148 The summary offence of harassment in s1 is supplemented by the s4 indictable offence of putting another in fear of violence on two or more occasions.

149 Model Criminal Code - Chapter 5: *Non Fatal Offences Against the Person* (1998) 57.

Fraud and forgery on the Internet

A number of submissions suggested the need for offences of fraud or forgery particularly directed to the use of computers or electronic communications for dishonest gain.¹⁵⁰ In general, the fact that a computer or electronic communications system is used as a means of fraud or blackmail will not affect the application of the general offences of dishonesty. Chapter 3 of the Model Criminal Code: *Theft, Fraud, Bribery and Related Offences*, extends the definition of forgery and deception,¹⁵¹ to ensure that conduct remains an offence though the transaction is accomplished by electronic communication or accomplished by dealing with an electronic rather than a human agent. The recently passed *Commonwealth Criminal Code Amendment (Theft, Fraud, Bribery and Related Offences) Act 2000* incorporates these provisions from the Model Criminal Code and makes additional provision in the offences of obtaining by deception and receiving for dishonest conduct inducing automated electronic money transfers.¹⁵²

Chapter 4, s4.2.4, imposes liability on offenders who obtain unauthorised access to data, modify data or impair electronic communications, in order to commit a “serious” offence. Any offence punishable with more than five years imprisonment counts as “serious”. Though s4.2.4 is not restricted in its application to offences of dishonesty, they are likely to provide the most common basis for prosecution. The penalty for breach of s4.2.4 is equal to that of the serious offence contemplated by the offender.

Though the Code extends the general offences of dishonesty to dishonest use of computers or electronic communications, there is no doubt that particularised offences, aimed at specific kinds of fraud involving misuse of electronic communications or transactions technology will be necessary. Formulation of these offences will require, however, the emergence and legislative crystallisation of rules and conventions regulating trade and transactions on the Internet.

Civil and criminal enforcement of emergent cyber-conventions: the case of spam

In telecommunications parlance, “spam” is the electronic equivalent of postbox junk mail. The term is usually taken to apply to email communication. Systems of delivery of spam are, as one might expect, far more various and sophisticated than those involved in postbox delivery of junk mail.¹⁵³ Unsolicited fax

150 Australian Federal Police, 28 April 2000, per John Guerts, Director Technical Operations; Police Commissioner's Conference: Electronic Crime Steering Committee 2 May 2000, per MJ Palmer, Chair.

151 Model Criminal Code Chapter 3, *Theft, Fraud, Bribery and Related Offences*, ss17.1, 19.1(1).

152 *Criminal Code Amendment Theft, Fraud, Bribery and Related Offences) Act 1999* (Cth), Obtaining property by deception 134.1(9), (10), (11), (12); Receiving, s132.1(8).

153 Prior to spam Email there was spam fax. This was the subject of a legislative ban in the United States: see the “junk fax law” of 47 USC 227, which makes it an offence to “send an unsolicited advertisement to a telephone facsimile machine”.

messages, which prompted “junk fax” laws in the United States, represent a intermediate step in the technology of uninvited commercial solicitation.

A submission from the Australian Securities and Investments Commission [ASIC] recommended extension of the offences in Chapter 4 to include an offence of “spamming for a price manipulative, illegal or improper purpose.” The Commission took, as its particular focus of concern, the practice of “making false or misleading statements affecting the price of a security...by making postings of the statement on the internet (via discussion forums, news groups, web pages and emails)”.¹⁵⁴ It was suggested that there is need for a “specific offence encompassing the actual means used to achieve the crime [as] communicating the method and an understanding of the extent of criminality involved and helping contribute to a body of knowledge that becomes readily understood by all.” An analogy was drawn with other offences which select the particular means employed by the offender as basis for prohibition. The introduction of crimes of dangerous driving causing death or injury during the second half of the twentieth century are obvious examples. Criminal law clearly has an educative role to play in controlling the misuse of new technologies.

Though the argument is persuasive in general terms, it does not follow that Chapter 4 of the Model Criminal Code provides an appropriate vehicle for the concerns which prompted the ASIC submission. The Committee recognises that legislation to outlaw the use of electronic communications in share market scams may be desirable. It does not follow, however, that a general offence of “spamming for an illegal or improper purpose” should supplement the existing offences in Chapter 4. The Committee is of the view that there is a gulf of principle and policy between the problems associated with unsolicited electronic communications and the issues addressed by the Chapter 4 offences.

The nature of the problems associated with the proposal for a general offence is more readily apparent from consideration of a progression from the simplest varieties of spamming through more sophisticated and in some cases, fraudulent, activity.

- *The activity of spamming involves transmission of an unsolicited electronic communication for a commercial purpose. Though there are many reasons why one might want to achieve electronic contact with a stranger, the term “spam” is usually restricted to communications made with some commercial objective.*¹⁵⁵

154 Submission, Australian Securities & Investment Commission, 27 April 2000, per Joseph P Longo, National Director, Enforcement. A submission from the Police Commissioners’s Conference Electronic Crime Steering Committee, 2 May 2000, per MJ Palmer, Chair, also expressed concern that offences proposed in Chapter 4 might not extend to spam based frauds or other harms.

155 Compare, for example, the use of unsolicited email for purposes of political or religious propaganda.

- *Bulk spamming:* Isolated unsolicited messages are of relatively small concern. United States jurisdictions which have legislated against the practice characteristically restrict their prohibitions to bulk spam. Transmission of bulk spam requires access to address lists. There is a thriving Internet market in electronic address lists garnered from web pages and other sources by lawful means. But proliferation of the message is frequently achieved by more objectionable means.
- *Relay rape and the anonymity of the spam merchant:* Though bulk spamming is possible without violating electronic barriers, spam attacks will often route messages through an unwitting and unwilling internet mail service provider [ISP]. The practice has been described as “relay rape”. The message may pass through dozens of service providers, colonising their address lists as it proliferates. In these circumstances, relay rape will almost certainly involve unauthorised data modification, since most service providers erect barriers against spam. The source of the message is characteristically concealed and the epidemic spread of the message may overtax the capacities of internet service providers resulting in significant impairment of electronic communications. Impairment may, indeed, be the object of the exercise or the spamster may be reckless to the risk that impairment of communications will result from flooding networks with unsolicited messages.¹⁵⁶
- *Fraudulent spam:* The possible motives of the mass spamster are barely foreseeable in their possible variety: the object may be to spread a religious or political message, promote a hoax, share a joke or sow panic. In general, however, most attention has been paid to spam for gain, which will frequently involve the promotion of fraudulent schemes. The ASIC submission proposing a spam offence was based in part on criminal proceedings taken against fraudsters in May 2000.¹⁵⁷ They disseminated more than 4 million spam messages predicting a spectacular rise in the price of Rentech stock, with the object of stimulating a surge in market activity resulting in profit on sale of their own holdings.

¹⁵⁶ Section 4.2.6, prohibiting conduct which impairs electronic communication, extends to include reckless as well as intentional impairments.

¹⁵⁷ ASIC media release, May 2, 2000. S Hourmouzis and W Loughnan, principals in the alleged scam, were charged with various offences of disseminating fraudulent information relating to securities and offences against Commonwealth telecommunications legislation. On 30 October, 2000 Steven Hourmouzis who pleaded guilty to the charges of disseminating fraudulent information, was sentenced to two years gaol: “Internet share swindler jailed”, “The Age” 31 October, 2000.

It is apparent that the varieties of objectionable behaviour associated with spam range from nuisance to outright fraud. As one might expect, legislative responses are equally varied in form. United States jurisdictions have been particularly active in their responses. No serious attempt has been made to impose an outright ban. In all of the examples considered by the Committee, statutory provisions recognised the legitimacy of unsolicited commercial email, provided senders do not falsify or hide their identity, the commercial nature of their communications or their point of origin.¹⁵⁸ A Federal Bill, currently under consideration, titled, *Internet Integrity and Critical Infrastructure Protection Act* of 2000, provides a typical and concise formulation. Under the Act it will be an offence if a person:

intentionally and without consent or authorisation of the recipient initiates the transmission of an unsolicited commercial electronic mail advertisement to one or more protected computers with knowledge that such advertisement falsifies an Internet domain, header information, date or time stamp, originating electronic mail address, or other identifier.¹⁵⁹

Aggravated forms of these offences can be charged when damage or loss occurs as a consequence and many jurisdictions permit civil action for punitive damages.

Most instances of spam are a nuisance, rather than a significant harm or threat of harm. The measures taken in various United States jurisdictions are devoted primarily to regulating electronic hucksters, rather than prohibiting their activities outright. The pressure for regulation of spam appears to have been generated by consumers and, more particularly, service providers, whose systems face overload from the proliferation of unsolicited commercial communications. Since the receiver bears the cost, the opportunities for commercial exploitation of virtually costless transmission of information to mass audiences results in escalating demands on service providers to increase their capacity to cope with the traffic. In more extreme instances, a communication designed to multiply itself over the Internet will overload mail systems to the point of catastrophic breakdown.¹⁶⁰

158 See, for example Washington House Bill 2752 (1998) enacted 25/3/98; California, *Business and Professions Code*, ss17511.1, 17538.4; 17538.45; *Criminal Code*, s502; Virginia, *Computer Crimes Act*, Chapter 886, approved 29/3/99.

159 Senate Bill s2448, 106th Congress 2d Session, Title II - Anti Fraud Protections.

160 Compare *US v Morris* (1991) 928 F.2d 504, in which a self replicating worm was released on the Internet, causing significant and widespread computer breakdown in universities, military sites and medical research facilities. Morris, who was a graduate student at Cornell University, said he released the worm to demonstrate the inadequacies of current security measures on computer networks. He denied that he meant to cause system breakdown. Like the sorcerer's apprentice, Morris failed to realise the full consequences of the worm's capacity for self replication. He was convicted of an offence of unauthorised access, contrary to the *Computer Fraud and Abuse Act* 1986 18 U.S.C.

The ASIC proposal for a general offence of spamming for an illegal or improper purpose, would impose a form of preparatory liability, additional to offences of attempt, conspiracy and the like. If it were to be adopted, the offence would supplement the existing offences in Chapter 4. Section 4.2.4 of the Code prohibits unauthorised impairment of electronic communications, access or modification of data, with intent to commit a serious offence. The requirement of a “serious” offence is generously inclusive: any offence punishable by imprisonment for five years or more is “serious”. Breach of the prohibition is punishable with the same degree of severity as the serious offence which was intended by the offender. It is, essentially, a specialised offence of attempt. Unlike the general doctrine of attempt, however, s4.2.4 specifies the proximate acts required for liability. The offence proposed by ASIC is superficially similar in form. Its claim to a place in Chapter 4 can be tested by asking whether the offence would deal with harms of a similar order to those prohibited by s4.2.4. Should it be an offence to initiate unsolicited electronic communications with intent to commit a serious crime? Consideration of the proposal in this light suggests that adoption of the ASIC proposal would be inadvisable.

The proximate acts which will result in liability under s4.2.4, in its present form, all involve outright violation of fundamental prohibitions against subversion of computer data or electronic communications systems. The offender has gained access to data or modified data without authorisation or engaged in unauthorised activity which impairs electronic communications. Spamsters who subvert security systems, engaging in relay rape and like activities, will fall within the scope of these prohibitions against unauthorised access,¹⁶¹ unauthorised modification of data¹⁶² or unauthorised impairment of communications.¹⁶³ If any of these prohibited activities are undertaken with intent to commit a serious offence, the offender’s conduct falls within the scope of s4.2.4, which has the potential to impose aggravated penalties for the offence.¹⁶⁴ Since so much is covered already, the practical effects of the ASIC proposal for an offence of spamming for an illegal or improper purpose would be restricted to those cases in which the spamster did not seek unauthorised access, did not modify data so as to cause impairment and did not impair communications. The Committee is of the view that the activity of spamming, in these residual cases does not warrant the creation of a general criminal offence under the Code. If the object of the exercise is fraud, the appropriate course is to prosecute for one of the offences of dishonesty in Chapter 3 of the Model Criminal Code or, in cases of more specialised fraud, of particularised offences in regulatory legislation.

161 *Summary offence*: unauthorised access to or modification of restricted computer data (p???)

162 Unauthorised modification of data to cause impairment, s4.2.5.

163 Unauthorised impairment of electronic communications, s4.2.6.

164 See, too, the offences of unauthorised modification of data, s4.2.5

The elements which define the conduct of spamming, whether in its colloquial or legal sense, have no natural or obvious connection with ulterior criminal objectives. In most instances the object of the spamster is to take advantage of a virtually cost free method of promulgating a commercial message. The limits imposed on the practice, in jurisdictions which have legislated against spam, are meant to provide workable regulation of an essentially law abiding populations of traders engaged in legitimate commerce. The United States legislation considered by the Committee displays considerable variations of form and content, as legislatures have sought to accommodate the competing interests of consumers, mail service providers, traders and other commercial interests. The development of anti-spam legislation closely resembles earlier developments, familiar in the Australian context, in the evolution of legislative controls over trade practices. The US legislation on spamming displays the same structure of detailed regulation, coupled with provision for enforcement of the regulatory provisions which may take the form of state initiated criminal prosecution or civil action by individuals for an award of damages. It is highly desirable, in the borderless world of trade, that regulatory schemes of this nature avoid conflict and variation across jurisdictions. Any determination of the accommodations which must be made if Australian legislatures are to impose legal sanctions against spam will require an investment of resources, consultation with service providers and affected commercial interests. A legislative programme of this nature will require time for consideration and resources well beyond the capacities of the Model Criminal Code project, which is rapidly nearing its conclusion.

The Committee is of the view that concept of spamming is too ill defined, at this time, to serve as the basis for a special preparatory offence in addition to those proposed in the Model Criminal Code. The Chapter 4 offences cover conduct which impairs data or communications. If the communication is fraudulent, the case can be dealt with under the general law of fraud or attempted fraud. If threats are made with a view to wrongful gain, the law of blackmail will cover the case. The proposal fares no better if one adds to the requirement of unsolicited commercial communication those further requirements which make the activities of the spamster unlawful in US jurisdictions which have legislated against the practice. Violation of requirements that the sender disclose identity or routing information still provides no basis for a specialised preparatory offence in the absence of a detailed regulatory scheme creating a system of agreed conventions governing cyberspace identities and identification.

Though the ASIC submission is primarily concerned with advocacy of a general offence of spamming for an illegal or improper purpose, passing reference is made to the securities fraud involving internet communications. As to the latter, the Committee is of the view that Chapter 4 of the Code should not include specific provisions aimed at the misuse of electronic communications in fraudulent or improper schemes involving trade in securities. Fraud or

impropriety of this nature calls for specialised prohibitions which will go well beyond schemes involving the misuse of computer data, electronic communications or the activities of spamsters.¹⁶⁵ The Committee concedes the point that electronic communication introduces a new dimension to familiar frauds and scams. The fact remains, however, that security fraud is a highly specialised form of criminal wrongdoing and one which is inappropriate for inclusion in a general criminal code.

Confidentiality and specially protected classes of computer data and computers

As in Britain and most Australian jurisdictions, the computer offences in this Chapter are not concerned directly with the protection of privacy or secret information. The Committee could discern no principle or basis for a distinction between secrets held in locked rooms, bureaux or filing cabinets and secret or private information stored in computer programs. If criminal legislation protecting privacy or data secrecy is desirable, it will have to be far more general in its application than the specific proposals for computer offences in this Chapter can encompass.

Legislation of this nature would also require a statement of principled limits which are specific to the protection of secrets and privacy, rather than the protection of computer security, which is the primary concern of the present chapter.¹⁶⁶

165 See, for example, the use of counterfeit web sites to inflate security prices: *The Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet*, A Report of the President's Working Group on Unlawful Conduct on the Internet, March 2000, pp5-6, US Department of Justice <<http://www.usdoj.gov.criminal/cybercrime/unlawful.htm>>

166 Compare the report of the New Zealand Law Commission, *Computer Misuse* (No54, 1999) paras 20-21, 92. The Commission rejected proposals for a simple offence of unauthorised access. Instead, offences of damage to data consequent on unauthorised access and use of information consequent on unauthorised access, were proposed. Liability for use of information gained by unauthorised access would follow the information, in much the same way as liability for receiving stolen goods follows the goods until they are restored to lawful custody. The New Zealand proposal appears to risk the creation of opportunities for oppressive prosecution of journalists and others who use information originally obtained by unauthorised access to a computer. There will be few documents of importance or interest in future, which are not generated and stored on computers at some stage in their composition or transmission. It is one thing to punish those who obtain unauthorised access to the computer. It is quite another to propose that information is to be treated as the poisonous fruit of a poisoned tree simply because it was once obtained as a consequence of unauthorised access. Some cats should not, and some cats cannot, be put back in the bag once they are out. These considerations reinforce the conclusion that legislation concerned with the security of computer systems does not provide an appropriate vehicle for the difficult policy issues involved in creating a defensible regime of protection for privacy and secrets.

Protection of Confidential Information

The Northern Territory Criminal Code is exceptional in its concern with confidentiality.¹⁶⁷ Section 222 of the Code, enacted in 1983, provides:

Any person who unlawfully abstracts any confidential information from any register, document, computer or other repository of information with intent to cause loss to a person or with intent to publish the same to a person who is not lawfully entitled to have or receive it, or with intent to use it to obtain a benefit or advantage for himself or another, is guilty of a crime...

[3 years imprisonment]

The provision has no application to information which is not “confidential”. In *Snell v Pryce* [(1990) 99 FLR 213] the Northern Territory Supreme Court held that the provision had no application to a computer operator employed by the police force, who took names, addresses and dates of birth from a departmental computer and passed them on to a private inquiry agent.

As Scott Krishcock remarks,¹⁶⁸ the “prime object [was] the protection of confidential, information, not computers, to which it only incidentally relates.” Another five years were to pass “before concerns over computer hacking reached the level at which the protection of computer systems and computer-held data became matters for the legislative agenda”.

Several submissions took issue with the absence of offences particularly directed to the preservation of confidentiality of information stored in electronic form.¹⁶⁹ Concern was expressed, particularly, over the possibility of misuse of government information concerning citizens and industrial espionage. The Committee concedes the necessity for more precisely targeted legislation protecting confidentiality and security of certain categories of information held by governments. Existing Commonwealth legislation prohibits unauthorised access to information held in a Commonwealth computer if it relates to security,

¹⁶⁷ But see also Magistrate’s Court Act 1989 (Vic) s124I, which protects the security of information relating to the collection of fines and enforcement of infringement notices.

¹⁶⁸ The *Criminalisation of the Unauthorised Accessing of Computer Systems* 1993 [Unpublished LLB Hons Thesis, University of Adelaide Law School] 73-74. Krishcock’s thesis provides a particularly helpful and an acute analysis of the issues involved in unauthorised access.

¹⁶⁹ Mark Williams, JP, 12 March 2000; New South Wales Police Service, 31 March 2000, per Michael Holmes, General Manager; Police Commissioner’s Conference: Electronic Crime Steering Committee 2 May 2000, per MJ Palmer, Chair.

defence, international relations and other categories of sensitive information.¹⁷⁰ Legislation of this nature, which restricts access to government information, can be extended to apply to certain categories of sensitive or secret information held by private enterprise. In the United States, for example, the *Computer Fraud and Abuse Act*¹⁷¹ extends the protection given to government information to the financial records of financial institutions.¹⁷² Though special or sectional interests may require protection by criminal offences which protect some categories of confidential information, offences of this nature have no place in a general criminal code.

Though the Chapter 4 offences are not directed to the protection of confidential information, those who obtain unauthorised access to data on a computer which is protected by an access control system, such as a password, will be guilty of a summary offence. However a person who is authorised to obtain access to confidential data will not commit the offence by passing that data on to another.

Self defence, self help and “strikeback” against hacker attack

United States sources report a growing trend for major corporations to install computer software which will enable a counterattack to be launched against the hacker’s computer. Strikeback programs range from systems which collect information identifying intruders to those which disable the intruder’s system.¹⁷³

Counterattack against hackers is analogous to self defence and defence of property, discussed in Part 1 of this paper: s4.1.13. It is possible that the defence of self defence in Chapter 2, s10.4 of the Model Criminal Code might extend to some instances of computerised counterattack against cybernet intruders. Self defence includes conduct which is undertaken “to protect property from unlawful appropriation, destruction, damage or interference”. It is possible, though far from certain, that a strikeback response to the hacker’s attack could be characterised in this way.

In practice, counterattack involves serious risks since hackers are likely to adopt precautions which divert the counterattack to innocent third parties.

It is apparent that principles of self defence of persons, which extend without undue strain to include protection of tangible property, are inadequate for the purpose of regulating computerised counterattack against hackers. The familiar concepts of necessity and reasonable response, which excuse or justify counterattack against physical threats, are next to useless as guides in this field.

170 See subsection 76A(2), *Crimes Act*.

171 1986 (US) 18 USC 1030(a)(2).

172 Financial institutions include registered or accredited banks, credit unions, brokers &c: see *ibid*, 1030(a)(2).

173 See Rutrell Yasin, “Think Twice Before Becoming a Hacker Attacker” <<http://infowar.com>>.

The Discussion Paper concluded that legislative intervention would be “premature,” in the current state of uncertainty over the permissible limits of defensive and deterrent strategies against hackers. In the absence of legislative provision for a right of counterattack against a hacker, the counterattack would itself amount to an offence against this Part of the Code. Individuals who resorted to self help in these circumstances would be left to the uncertain promise of a merciful exercise of prosecutorial discretion. Three submissions were received which spanned the range of possible responses to the dilemma. Reconsideration of the issue in the light of the submissions reinforced the Committee in its conclusion that any attempt to state legislative principles of justification or excuse would be premature. The Western Australian Model Criminal Code Review Committee suggested a distinction between lawful “protective counterattacks” and unlawful counterattacks which are designed to destroy the hacker’s computer system.¹⁷⁴ Another submission recommended provision for “reasonable” counterattack,¹⁷⁵ whilst the Australian Federal Police submission appeared to take the view that counterattack should not be permitted under any circumstances.¹⁷⁶

The Code makes provision for a defence of necessity in circumstances of emergency.¹⁷⁷ Any attempt to go beyond the defence of necessity to formulate a principle of justification or excuse would necessarily involve reliance on a distinction between reasonable and unreasonable retaliation. In self defence against physical attack, a requirement of reasonableness refers implicitly to criteria which are relatively robust and relatively well understood by courts and jurors alike. The case is quite different when the question involves counterattack via a telecommunications system against a hacker. The familiar criteria of necessity and proportionality which govern self defence in other applications have no obvious application here. Reliance on a test of what is or is not reasonable in the way of counterattack against hackers would place an inappropriate legislative burden on courts to determine issues of telecommunications policy.¹⁷⁸

174 Judges’ Committee of the Supreme and District Courts of Western Australia; Model Criminal Code Review Committee, 15 March 2000, per Justice Scott, chairman.

175 Australian Institute of Criminology, 3 April 2000, per Dr Russell Smith, Senior Research Analyst: Absence of a right of self defence would place “undue restrictions on the ability of computer users to protect themselves...Arguably some codification of the need for counterattacks to be ‘reasonable’ should be undertaken.”

176 Australian Federal Police, 28 April 2000, per John Guerts, Director Technical Operations: “Self-defence would necessarily involve the use of the telecommunications system to ‘retaliate’. This constitutes an offence under s76E *Crimes Act* 1914 and should not be permitted under any proposed code.” The issue is less clear, however, than the submission suggests. Though s76E forbids use of the telecommunications system to alter data on another computer or in any way impede the use of another computer without authorisation, the provision does permit reliance on a defence of “lawful excuse”. On the meaning of “lawful excuse”, see *Taikato* (1996) 186 CLR 454 at p464.

177 Model Criminal Code - Chapter 2: *General Principles of Criminal Responsibility* s10.3.

178 Compare the strictures of the High Court against the proliferation of defences of “reasonable excuse” in lieu of legislative statement of policy: *Taikato* (1996) 186 CLR 454.

Jurisdiction

The final section of this Report provides an exhaustive discussion of the present unsatisfactory state of the law governing State, Territorial and Commonwealth jurisdiction over criminal conduct. Significant changes are proposed to existing State and Territorial legislation on jurisdiction.¹⁷⁹ These changes are incorporated in Part 2.7 of the Model Criminal Code - Chapter 2: *General Principles of Criminal Responsibility*. The Model Criminal Code jurisdictional provisions, which are intended to displace existing State and Territorial law, are quite distinct from those governing Commonwealth jurisdiction, which are now to be found in the *Criminal Code Act 1995*.¹⁸⁰ The Model Criminal Code provisions will govern the application of State and Territorial criminal laws within Australia and overseas. Though state and territorial laws will apply, on occasion, to crimes committed overseas, it is likely that the Model Criminal Code provisions on jurisdiction will have their primary field of application within Australia. The State and Territorial provisions will have their primary field of application within Australia, in cases involving uncertainty over the reach and interrelationships of domestic laws. By contrast, the primary application of Commonwealth provisions will be found in the extension of Commonwealth criminal law to conduct and consequential harms occurring wholly or partly beyond Australian territorial boundaries. This practical difference in their respective fields of application explains the differences of principle between the Model Criminal Code provisions on jurisdiction and their Commonwealth counterparts.

Since the application of legislation creating computer offences to conduct occurring in other states or countries is a matter of some considerable interest, a brief account of the jurisdictional issues is appropriate at this point. The more general issues and conundrums which prompted formulation of the Code provisions on jurisdiction are discussed in depth and detail in the final section of the Report.

The Model Criminal Code and Commonwealth provisions both take as their starting point the unexceptionable principle that criminal prohibitions apply to offences which occur wholly or partly within the boundaries of the state which enacted the prohibition. In the *Criminal Code Act*, this is called “standard geographical jurisdiction”. Commonwealth law applies if the proscribed conduct or proscribed result occur wholly or partly” in Australia or wholly or partly on board an Australian ship or aircraft.¹⁸¹

179 Several Australian jurisdictions have adopted a substantially uniform set of jurisdictional provisions recommended by the Standing Committee of Solicitors General and approved by the Standing Committee of Attorneys General in the wake of the High Court decision in *Thompson* (1989) 169 CLR 1. The legislation and its interpretation in the courts is discussed in this Report in the segment on Part 2.7 of *Criminal Code* (starting p.215).

180 *Criminal Code Act 1995* (Cth), as amended by the *Criminal Code Amendment (Theft, Fraud, Bribery and Related Offences) Act 2000*.

181 The expressions “Australian ship” and “Australian aircraft” are defined in the “The Dictionary in the Criminal Code”, Chapter 11 - *Miscellaneous Interpretive Provisions*. On the problem of defining satellites, see COE: *Draft Convention on Cyber-Crime* (October 2000); *Criminal Code Act 1995* (Cth); s16.3 ‘Meaning of Australia’.

In most applications, the principles of standard geographical jurisdiction tend to permit no more than a limited extension of criminal legislation beyond territorial limits. When computer crime is in issue, however, standard geographical jurisdiction has the potential to confer an uncontrolled amplitude of jurisdiction. Rules designed to determine which state has jurisdiction over a murder when the bullet from a killer's gun hits a victim on the other side of a riverine border have unexpected consequences in their potential application to these offences. Legislation which makes it an offence to attack communications facilities is potentially capable of application if a linked computerised receiving facility is located within territorial limits, no matter where in the world the offender is located or the criminal conduct took place. This expansive effect of standard geographical jurisdiction is not limited, of course, to offences which penalise attacks on electronic communications or electronic data. The principles of standard geographical jurisdiction can be equally expansive in their operation when computerised facilities are employed to commit offences of fraud, conspiracy, transmission of forbidden material or other crimes in which the essence of the offender's wrongdoing consists in misuse of electronic communications.

The differences between the Model Criminal Code and Commonwealth provisions only become apparent when there is a question whether their laws apply to offences which do *not* occur within the jurisdiction. Jurisdiction over offences which do not occur within territorial limits - designated "extended geographical jurisdiction" in Part 2.7 of the *Criminal Code Act 1995*, is discussed below.

Standard geographical jurisdiction

Application of the principle that a state has jurisdiction over offences which occur within its territory depends on rules which determine where an offence occurs. To put it shortly, an offence is taken to occur in the place where one or more of the physical elements¹⁸² which comprise the offence occurs.¹⁸³ With the exception of the preparatory offences of possession of data with intent (4.2.7) and supply of data with intent (4.2.8) the computer offences share two common elements. The offender must *cause* the prohibited harm, whether it be impairment of data or impairment of communications and that harm must relate to a *computer*.

182 Model Criminal Code - Chapter 2: *General Principles of Criminal Responsibility* Part 2.2 defines the physical elements of an offence. These provisions correspond exactly with provisions in Part 2.2 of the *Criminal Code Act 1995-1999* (Cth).

183 Though there are differences in formulation of standard geographical jurisdiction and the Model Criminal Code does not use that terminology, Part 2.7 of the Model Criminal Code - Chapter 2: *General Principles of Criminal Responsibility* ss2.7.1(2); 2.7.2(1) & (2); 2.7.3(2)(a) duplicates the effect of *Criminal Code Act 1995-1999* (Cth), s14.1.

Offences in the Code are analysed in terms of physical elements and fault elements. Physical elements include “conduct” - the acts or omissions of the offender - “circumstances” and “results”. The distinction between act and result can lead to pointless exercises in casuistry. Very often it is possible to find equally appropriate descriptions of an act by reference to the act which initiates a consequence or by reference to the consequence itself. The act of “breaking a window” can be equally well described as an act of “throwing a stone”, with the consequence that a window was broken. References in the computer offences to the requirement that the offender *cause* unauthorised impairment &c of data makes it clear that they require analysis in terms of an “act” which initiates a causal sequence which results in an impairment of data or other specified consequence.

Acts which cause the forbidden result are unlimited in their variety. The most familiar, in the current state of technology, will involve some manipulation of a keyboard but commission of an offence may involve more circuitous means. The offender may have caused a computer system to crash by sending a virus infected disk through the mail to the owner of the computer who is the unwitting agent of harm to her own programs.¹⁸⁴ The act is located where the offender was located at the time the causal sequence was initiated. The result specified in the offence, whether of impairment of data, impairment of communication or unauthorised access, is located where the damaged computer data is located. Of course, in cases where the harm results from proliferation of a virus or worm, the harm may be worldwide - but it is, nevertheless, a catastrophic aggregation of a multitude of particular harms, each of which has a precise geographical location. Though it is data, not computers, which form the true subject of the prohibitions the discussion which follows adopts the convenient term “target computer” to indicate the location of the prohibited result.

As the preceding discussion indicates, computer offences involving geographical separation of the offender and target computer are always capable of analysis by reference to the location of the offender at the time the act was done and the location of the target computer where the harmful result occurred. That need not exhaust the possibilities however. The concept of an act which causes a consequence is not limited to physical movements of the offender. Much of what we do, in a world of modern communications, involves action at a distance. It is perfectly possible for a father residing in Sydney to *buy* a book in London and *give* it to his daughter in Los Angeles. In the same way, the offender’s conduct may involve some physical act at place A, resulting in an act occurring at place B, which results in a consequence at place C. A Londoner may operate a keyboard in Wimbledon, which activates a cyberbot in the United States, which results in harm to a target computer in Sydney. In terms of jurisdictional analysis, there seems no reason to restrict the location of the causative act to the place where the offender is located.

¹⁸⁴ See Model Criminal Code, *ibid*, s11.3; *Criminal Code Act*, *ibid*, s11.3 of the Code; on liability for the acts of innocent agents.

Section 4.2.7 - possession of data with intent - is the sole exception to the pattern of definition in terms of act and consequence. The offence includes a special jurisdictional rule which declares that a person has possession or control of data in the place where the person is located.¹⁸⁵

Jurisdiction And The Undefined Concept of a Computer

The Code offences which prohibited unauthorised modification or unauthorised access to data only apply to data “held in a computer”. The offence of impairing communications similarly refers to communications to or from a computer. The territorial application of these offences depends, ultimately, on what is to count as a “computer”. The Council of Europe Draft *Convention on Cyber-crime* proposes a definition which introduces a jurisdictional conundrum. It refers not to a “computer”, but to a “computer system”, which is defined as “any device or a group of interconnected devices, which pursuant to a program performs automatic processing of data [or any other function].”

If the term “computer” is taken to refer to a set of interconnected devices, the set may span a number of jurisdictions. It is, indeed, not apparent what limits there might be to the “group of interconnected devices”. The World Wide Web might be considered to be a single computer, effectively conferring universal jurisdiction on any state which enacts computer crime legislation. The Convention provides the following tantalising explanation of the definition:

“[A] ‘computer system’ refers to the function of data processing and therefore may include any system that is based on such a function, eg. Telecom systems...the “interconnection” referred to in the definition encompasses radio and logical connections.”

Explanatory notes accompanying earlier drafts of the Convention expressed concern over the extent to which “States will be able to claim jurisdiction over acts occurring in the whole or part of such a ‘computer system’”: Draft *Convention on Cybercrime* April 2000, fn2. In the most recent draft (October 2000), the definition of “computer system” is unchanged but the expression of concern over jurisdiction has been, perhaps surprisingly, dropped.

Chapter 4 makes no reference to “computer networks”. In the absence of such a reference, it seems clear that references to a “computer” in the Code include computers which are linked to other computers and unlinked computers. Application of standard geographical jurisdiction

¹⁸⁵ Note too the jurisdictional effects of the Chapter 4 definition of “computer offence” in s4.2.1 on the application of ss4.2.7 and 4.2.8.

to the Chapter 4 offences will result in the potential application of their prohibitions to conduct which targets, say, the interconnected computers of one of the United States telecommunications carriers. If it is accepted that the more sophisticated mobile 'phones are computers, the fact that communications to and from that 'phone are blocked by a Canadian hacker's attack on the US telecommunications carrier, while the owner of the 'phone is holidaying in Surfers Paradise, will be sufficient to confer jurisdiction on Australian courts, for there is a computer located in Australia, which has suffered an impairment of communications. Though the epicentre of the harm is in the United States and the hacker is remote from these shores, a "physical element" of the Canadian hacker's crime is manifest in Surfers Paradise. So also with other portable computers, such as smart cards, linked to networks. The location of a particular device which is affected by unauthorised impairment of data or impairment of electronic communications, which may be one among millions of such devices, scattered throughout the world, provides the jurisdictional link.

Extended geographical jurisdiction: the Commonwealth scheme

Part 2.7 of the *Criminal Code Act* 1995 sets out a five stage scheme of progressively widening jurisdictional regimes. The elaboration of the Commonwealth scheme is in marked contrast with the Model Criminal Code provisions. State and Territorial jurisdictional criteria are less elaborate, less restrictive and their meaning will depend, to a far larger extent, on judicial exegesis and the development of a body of precedent.

The first and least expansive of the Commonwealth jurisdictional regimes is "standard geographical jurisdiction." The last, designated "extended geographical jurisdiction - category D," confers jurisdiction unlimited by any territorial consideration. Standard geographical jurisdiction governs the application of Commonwealth laws unless the legislature specifies the application of one of the more expansive regimes.

The salient factors on which jurisdiction depends in the Commonwealth scheme are few and simple.

- **The location of "the conduct constituting the...offence" [CCA ss14.1,15.1, 15.2];**
- **The location of a "result of the conduct" [CCA s14.1 ss15.1, 15.2];**
- **Citizenship of the offender [CCA ss15.1, 15.2];**
- **Residence of the offender [CCA s15.2].**

The references to “conduct” and “result” refer in turn to the “physical elements” of the offence in question, defined in s4.1 of the *Criminal Code Act 1995*. We can match the salient jurisdictional factors in a comparative table with the physical elements involved in the computer offences.

| COMMONWEALTH JURISDICTION FACTORS | PHYSICAL ELEMENTS OF COMPUTER CRIMES |
|--|--|
| 1. Location of “conduct constituting the... offence” | 1. Location of the act of the offender which caused impairment of data, impairment of communications, unauthorised access...&c |
| 2. Location of a “result of the conduct” | 2. Location of the target computer. |
| 3. Citizenship of the offender | 3. Not a physical element of any computer crime |
| 4. Residence of the offender | 4. Not a physical element of any computer crime |

The jurisdictional provisions of the COE Draft *Convention on Cyber-crime* would require the parties to the Convention to extend the application of the offences beyond those committed wholly or in part within geographical boundaries to offences committed “by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence was committed outside the territorial jurisdiction of any state.” That requirement matches the Commonwealth’s *CCA* s15.1 *Extended Geographical Jurisdiction - Category A*, which extends the application of offences to Australian citizens.

Extended Geographical Jurisdiction: The Model Criminal Code

Part 2.7 of the Model Criminal Code will extend the application of State and Territorial criminal prohibitions to conduct which occurs outside territorial limits if the conduct threatens the peace, welfare or good government of the State or Territory.¹⁸⁶ It is sufficient if the threat is potential, rather than actual: State or Territorial criminal law applies if the offender’s criminal activity would have threatened peace, order or good government had it been carried through to completion.

Extended Geographical Jurisdiction and preparatory or “ancillary” crimes

The principles governing standard geographical jurisdiction confer an extravagant breadth of application on the computer offences. That is a consequence of the proliferation of portable computers in a bewildering variety

¹⁸⁶ Model Criminal Code - Chapter 2: *General Principles of Criminal Responsibility*, s2.7.3(2)(b) & 2.7.2(3).

of sizes, shapes, forms and functions. There is jurisdiction if the act which causes the prohibited result or the result itself occurs within territorial limits. Often when computer offences have an international dimension, the location of a computer used to initiate a harmful consequence or the location of a computer which suffers some impairment of function will provide alternative bases for the jurisdictional nexus.

In preparatory crimes of attempt, incitement and conspiracy, however, there is typically no “result” to provide a territorial basis for jurisdiction. Provision is made, however, for extension of the principle of standard geographical jurisdiction to the preparatory crimes when the conduct of those involved occurs outside Australia. In the Commonwealth *Criminal Code Act 1995*, attempt, incitement and conspiracy are designated “ancillary offences.”¹⁸⁷ Individuals who plot crimes whilst abroad are liable under Australian law for ancillary offences which are intended to culminate in criminal conduct or criminal consequences in Australia, though their attempts fail, their incitement falls on deaf ears or their conspiracies are aborted before the harm is done. So, for example, if a band of foreign nationals in Transylvania conspire to make an electronic communications attack on the computer system controlling the Sydney rail system, with the object of paralysing public transport in that city, the offence of conspiracy to engage in sabotage extends to their activities.

The jurisdictional provisions of the Model Criminal Code achieve essentially the same effect, though they have potentially far wider application. State or Territorial criminal law will apply if the offender’s criminal activity would have threatened peace, order or good government in the State or Territory, had it been carried through to completion.

Law enforcement and cybercrime

In common with other chapters of the Model Criminal Code, Chapter 4 makes no provision for enforcement.¹⁸⁸ There appears to be pressing need for specialised enforcement provisions. The issues involved are both difficult on a technical level and controversial in relation to the protection of individual human rights and the rights of corporate entities. The COE Draft *Convention on Cyber-crime* proposes extensive powers of search of electronic databases. These proposals include requirements of co-operation in aid of search as, for example requirements: of disclosure; of compliance in preservation of data; of assistance in decryption or recovery of data and other measures to facilitate search computer

¹⁸⁷ Defined, *Criminal Code Act 1995-1999* (Cth), The Dictionary in the *Criminal Code*. The definition includes as well liability as an accomplice (s11.2) and liability for the acts of innocent agents (s11.3).

¹⁸⁸ Concern was expressed over the absence of proposals for an extension of enforcement powers by AUSTRAC [Australian Transaction Reports and Analysis Centre] in a brief submission which drew attention to the need to ensure that enforcement agencies have the “capacity to continue to investigate and prosecute crimes committed in an electronic environment...”; 20 April 2000,. Per Elizabeth Montano, Chair, AGEC.

systems for evidence of crime.¹⁸⁹ Among recent legislative models, the UK *Regulation of Investigatory Powers Act 2000*, is of particular interest as an attempt to ensure adequate powers of enforcement which will be consistent with the requirements of the *Human Rights Act 1998*.

Commonwealth and State/Territory offences: overlaps between computer crime and telecommunications crime

Most business computers and possibly the majority of computers used for domestic purposes, are connected to other computers. Unauthorised access or impairment of data may be more likely to occur via a telecommunications link than by gross physical intrusion. As a consequence of technological convergence, the distinction between a telephone and a computer is fading with each passing month. Commonwealth legislation dealing with telecommunications, which includes specialised prohibitions aimed at unauthorised interception or impairment of telecommunications, will overlap state and territorial computer offences. Provision is necessary to ensure that state or territorial legislation, aimed at computer crimes, are not deprived of effect by s109 of the Commonwealth Constitution, which confers pre-emptive effect on Commonwealth laws.

Limited provision is made in existing law to preserve the operation of state and territorial laws dealing with computer crime. Section 76F of the Commonwealth *Crimes Act 1914* declares that the Commonwealth computer offences in the Act do not exclude or limit the concurrent operation of state and territorial laws.

The expanded range of offences proposed in the Code requires similar provision to be made elsewhere in Commonwealth law to avoid the potentially disabling effects of overlapping state and federal offences. The most obvious of these involves the proposed Code offence in s4.2.6 of unauthorised impairment of electronic communications. This will overlap s85ZG of the *Crimes Act 1914*, which makes it an offence to use a device or facility so as to “hinder the normal operation of a carriage service.”

Other instances of overlap with Commonwealth telecommunications legislation are possible. The offences of unlawful access to computer data and unauthorised modification so as to impair data [s.4.2.6] proposed in this Report, and similar offences which already exist in state or territorial law, may overlap the Commonwealth offence of intercepting a communication in s7 of the *Telecommunications (Interception) Act 1979*. The risk of overlap is less obvious here, since the offences proposed in the Report are only concerned to protect data “held in any computer”. It might be thought that there is no possibility of overlap with the offence in s7, which prohibits interception of “a communication passing over a telecommunications system”. Current caselaw dealing with interception of telephone communications suggests, however, that this may be

189 Article 14 - Search and Seizure; Article 15 - Production order; Article 16 - Expedited preservation of data stored in a computer system; Article 17 - Expedited preservation and disclosure of traffic data; Article 18 - interception: see *Cybercrime Convention*, Draft No22, Revision 2, October 2, 2000.

too simple a view to take.¹⁹⁰ In view of the absence of any definition of “computer” and the anticipated dissolution of any functional distinction between computers, computer networks and the telecommunications system, it is advisable to make provision for concurrent operation of Commonwealth interception offences with state and territorial computer offences.

¹⁹⁰ See section 85 2C *Crimes Act 1914* (Cth) adopts the definition of this and other technical terminology from the *Telecommunications Act 1997*. For ‘carriage service’ and ‘carriage providers’ see s. 87 of that Act.

4.2.1 General definitions

In this Part

Computer offence means:

- (a) an offence against this Part; or
- (b) conduct in another jurisdiction that is an offence against this Part if the conduct occurred in this jurisdiction

data includes:

- (a) information in any form, or
- (b) any program (or part of a program).

data held in a computer includes:

- (a) data entered or copied into the computer, 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.

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.

4.2.1 GENERAL DEFINITIONS

The Code adopts a minimalist approach to definition of the elements of computer systems.

“Computer Offence”

This is necessary for the offences at sections 4.2.7 and 4.2.8 (pages 174-185) and provides for extended geographical jurisdiction.

“Data”

The concept of “data” encompasses information in any form, programs or parts of programs, which have been entered into a computer which forms part of the operating system of a computer. The terminology is essentially the same as existing provisions in the Commonwealth *Crimes Act 1914*.¹⁹¹

“Data storage device” and “electronic communications”

The terminology of “data storage device” and “electronic communications” and essential elements of their definitions have been drawn from the *Electronic Transactions Act 1999* (Cth).

“Data held in a computer”

The definition is inclusive and it extends to any data or programs held in the computer, whether they form part of the operating system of the computer or have been entered into the computer for reference or use. Data or programs held on a disk or other removable storage device become “data held in a computer” when the disk is in a computer. This element of the definition is of particular significance to the application of s4.2.5, which prohibits unauthorised impairment of computer data. The offence extends to impairment of data held on discs or other removable data storage devices. Once the device is electronically accessible by a computer, the data held on the device comes within the protective scope of the provisions. If modification of the data is unauthorised, liability follows, though the offender may own the particular computer which effects the modification.

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.

¹⁹¹ Crimes Act 1914 (Cth) s76A:

(1) In this Part, unless a contrary intention appears: ... “data” includes information, a computer program or part of a computer program .

(2) In this Part...a reference to data stored...in a computer includes a reference to data entered or copied into the computer.

4.2.1 General definitions

In this Part:

Computer offence means:

- (a) an offence against this Part; or
- (b) conduct in another jurisdiction that is an offence against this Part if the conduct occurred in this jurisdiction

data includes:

- (a) information in any form, or
- (b) any program (or part of a program).

data held in a computer includes:

- (a) data entered or copied into the computer, 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.

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.

Conduct which impairs data held in a data storage device when the device is not in a computer or electronically accessible by a computer does not fall within the scope of the prohibition. The Discussion Paper proposes a summary offence of impairment of electronic data on a computer disc, credit card or other storage device.

Computers - the undefined subject of the legislative proposals

The obvious question to ask, in legislation dealing with the unfamiliar concept of computer crime, is why no attempt has been made to fix the meaning of the word computer itself. Why, for that matter, does the Code make no attempt to define “data” or “program”? In his monograph on computer crime, Martin Wasik notes that British *Computer Misuse Act 1990*, similarly leaves these terms undefined and concludes that they “should therefore be given their ordinary meaning by the courts.”¹⁹² He supports the omission on the ground that statutory definitions are likely to prove both under inclusive and over inclusive. Under inclusive, because today’s definition may be overtaken by developments in technology, so that a new generation of devices, which perform all the functions of a computer, may fall outside the scope of the statutory definition. Over-inclusive, because computerised components are increasingly used in household appliances, tools, vehicles and other artefacts manufactured for use or amusement. The standard legislative definition adopted in many American states during the eighties, a version of which was once proposed for adoption in Tasmania,¹⁹³ displays the faults of both under and over inclusiveness:

[A computer is] an electronic device that performs logical, arithmetic, and memory functions by the manipulation of electronic or magnetic impulses and includes all input, output, processing, storage, computer software and communication facilities that are connected or related to a computer.

The definition would extend to a mobile telephones, poker machines and portable calculators,¹⁹⁴ but might not cover non-electronic, optical computers.

The alternative suggested by Martin Wasik and adopted in practice in the UK and Australia, is to avoid definition: legislative references to “computer” are to be given “their ordinary meaning.”¹⁹⁵ It is apparent, however, that the determination of “ordinary meaning” is to be determined by the evolutionary

192 M. Wasik, *Crime and Computer* (1991) Appendix 4.

193 Report on *Computer Misuse*, Law Reform Commission of Tasmania, Report No47 of 1986.

194 Compare the United States *Computer Fraud and Abuse Act 1986* (US) 18 USC s1030(e), which attempts to limit the ambit of the term: “[C]omputer” means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device.

195 *Op cit* p4.

Code

| |
|--|
| |
|--|

processes of judicial interpretation. The alternative, that juries might determine whether or not a particular machine is or is not a computer, appears quite unacceptable. Though juries are perfectly capable of giving ordinary meanings to ordinary words,¹⁹⁶ it is far from clear that “computer” has an “ordinary meaning”. 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” suggest 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.

In 1991, when Martin Wasik recommended recourse to ordinary meanings, the task which he assigned to courts might have seemed more manageable than it does now. 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 in this way. 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 problem of overcriminalisation

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.¹⁹⁷

There are grounds for disquiet when criminal prohibitions extend to trivial misconduct. In Model Criminal Code Chapter 3: *Theft, Fraud, Bribery and Related Offences*,¹⁹⁸ the Committee accepted the principle that a mere borrowing of property belonging to another should not be a Code offence. The sanctions of the criminal law should be reserved for more serious misconduct: “remedies in tort provide a sufficient response for temporary takings”.¹⁹⁹ There is no reason to reverse that policy simply because a temporary taking involves unauthorised use of a computer. The Committee is of the view that the same principle should apply to unauthorised use of computer data or programs. The

196 *Brutus v Cozens* [1973] AC 854.

197 The Tasmanian Law Reform Commission, which did attempt a definition of “computer”, proposed to limit the ambit of the expression by adding a regulatory power to exclude “any machine or any other thing” from the definition. See: *Report on Computer Misuse* (1986) Recommendation 2(iii).

198 Final Report, December 1995.

199 *Ibid*, 73.

Code

| |
|--|
| |
|--|

problem of overcriminalisation 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 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.

The Discussion Paper remarked that the “breadth and uncertainty of application of prohibitions directed to ‘computer data’ remain...as a cause for concern.” That cause for concern remains. One submission made the point, reinforced by expert advice to the Committee, that recent technical developments and miniaturisation of components have dramatically extended our understanding of what is and what is not a computer. Credit cards and the like can be categorised as mere data storage devices. But a “smart card” is a micro-processor and there is no apparent reason to deny it the description of a computer. Screens and keyboards which enable logical operations to be performed are no more than a means - one among a number of possible means - of access to the computer.²⁰⁰ They are not the thing itself.

The Committee invited submissions on the question whether the terms “computer”, “data” and “program” should be defined in ways which would locate the area of criminal conduct more precisely. Submissions on the question were divided. Most were opposed to definition, substantially for the reasons advanced in this Report.²⁰¹ Only one submission argued in favour of definitions. The Commonwealth Director of Public Prosecutions suggested that a minimalist definition, drawn from current dictionaries, might serve a useful purpose and would be unlikely to have unwanted consequences.²⁰² Reconsideration of current dictionary definitions left the committee unpersuaded that legislative

200 Australian Institute of Criminology, 3 April 2000, per Dr Russell Smith.

201 Model Criminal Code Review Committee, Western Australia, 20 March 2000, per Hon Justice Scott; Sir Harry Gibbs, 29 March 2000; Australian Institute of Criminology, 3 April 2000, per Dr Russell Smith; Victoria Police 5 April 2000, per Neil O’Loughlin Deputy Commissioner Policy and Standards; Australian Federal Police, 28 April 2000, per John Guerts, Director Technical Operations.

202 Commonwealth Director of Public Prosecutions; 22 March 2000, per Geoff Gray, Assistant Director.

Code

| |
|--|
| |
|--|

adoption would serve any useful purpose. The definitions are unnecessary when the answer is obvious. They seem unlikely to be of assistance in marginal cases and they seem unlikely to provide a barrier against debate involving the competing views of expert witnesses in those marginal cases. They are, indeed, more likely to inspire unnecessary debate.²⁰³

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.

Computer networks and systems

The draft provisions make no reference to computer “systems” and one reference only to computer “networks”, in the s4.2.1 definition of “data held in a computer”. No attempt is made to define the meaning of a computer “network”. Use of the term, in this particular context, is meant to ensure that liability for offences of unauthorised impairment of data is not limited by the spatial location of the tangible components of an data processing system.

Current Australian and UK legislation make no reference to computer networks. The Victorian and Tasmanian Acts do refer, however, to computer “systems”.²⁰⁴ Only in Tasmania, however, is it clear that the reference to a computer system was intended to cover a network of computers. The Tasmanian Law Reform Commission originally envisaged a more explicit provision. In its report of 1986, the Commission proposed the following definition:

“Computer network” includes the interconnection of two or more computers, whether geographically separated or in close proximity, which may be used to transmit data from one computer to another computer.

The definition was intended to fix the meaning of the term in proposed offences of unauthorised access to a computer network, unauthorised alteration of data in a network and unauthorised omission to record data in a network. In the event, the Tasmanian legislature did not adopt the recommendations of the Law Reform Commission, though references in the Tasmanian Code offences

²⁰³ *The Macquarie Dictionary* (1981) defines a computer as “an apparatus for performing mathematical computations electronically according to a series of stored instruction called a program”. “Data” is defined as “information” and the verb “to program” is defined: “to organise and arrange (data, etc) relevant to a problem so that it can be solved by a computer”.

²⁰⁴ *Summary Offences Act 1966* (Vic) s9A; *Criminal Code* (Tas) ss257B, 257C, 257D, 257E.

Code

| |
|--|
| |
|--|

to a “computer or system of computers” appear to reflect the spirit of the original recommendations.²⁰⁵

The offences proposed in this Part include, in s4.2.6, unauthorised impairment of electronic communications between computers. No reference is made, in the formulation of this offence, to networks or systems of computers. In the absence of any criterion for determining whether physically separate components of a linked system are distinct computers or components of a single computer, references to networks or systems of computers are best avoided in this particular context.

²⁰⁵ See also *Computer Misuse*, New Zealand Law Commission No54 para 15.

4.2.2 Meaning of access to data, modification of data and impairment of electronic communication

- (1) In this Part, *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.
- (2) In this Part, *modification* of data held in a computer or data storage device means:
 - (a) the alteration or removal of the data, or
 - (b) an addition to the data.
- (3) In this Part, *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.
- (4) A reference in this Part to any such access, modification or impairment is limited to access, modification or impairment caused (whether directly or indirectly) by the execution of a function of a computer.

4.2.2 Meaning of access to data, modification of data and impairment of electronic communications

Introduction

Access to data, modification of data and interference with electronic communications are defining physical elements in the proposed offences. Access, modification and interference, as defined in Chapter 4, all require proof that the access, modification or interference resulted from conduct which caused a computer to execute a programmed function. One does not, for example, obtain access to computer data by merely inspecting a computer screen. Nor can one obtain unauthorised access to data held in a computer with a screwdriver, modify data with a handaxe or use a pair of scissors to impair electronic communications. Acts of gross physical interference with the computer or its parts fall within the scope of the criminal damage provisions.²⁰⁶

The conduct elements of the offences effected by execution of a computer function are, variously:

- cause unauthorised access to data;
- cause unauthorised modification of data;
- cause unauthorised impairment of electronic communications to or from a computer.

Causing a computer to execute a function

The Code offences follow the UK *Computer Misuse Act* (1990) in their description of the conduct of the offender as causing a computer “to execute a function”.²⁰⁷ This requirement, which is common to all the proposed offences, bears an unwelcome appearance of technical complexity. It would have been preferable, had it been possible, to stick to the plain English of prohibitions against “use of a computer” with intent to commit a serious offence, impair data, or impair electronic communications.

On reflection, it became apparent that a degree of technicality was unavoidable. 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 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.

²⁰⁶ Sections 4.2.5(3) and 4.2.6(3) make provision for reciprocal alternative verdicts.

²⁰⁷ Section 1(1)(a) *Computer Misuse Act* 1990: “causes a computer to perform any function”.

Code

| |
|--|
| |
|--|

Though it is necessary to extend the scope of the offences in this way, the extension amplifies uncertainty over the meaning of the word “computer”. 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 potential scope of the offences in this Part will depend on the development of a case law jurisprudence which determines the limits of what can and cannot amount to a “computer”. Though the Code is no different from existing law in that respect, the breadth of the interpretive task assigned to courts is a cause for concern.

Accessing Data

The concept of “access” makes only one appearance among the proposed Code offences. Section 4.2.4 prohibits unauthorised access with intent to commit a serious offence. By contrast with existing law in a number of jurisdictions, mere unauthorised access will not amount to a Code offence. The Committee does propose, however, a summary offence of unauthorised access to restricted data.

The summary offence is discussed separately.

Like current UK and Australian legislation, which is aimed at individuals who “obtain”²⁰⁸, “gain”²⁰⁹ or “secure”²¹⁰ unauthorised access to a computer or computer data, the draft provisions avoid the use of “access” as a verb.

Access is defined exhaustively to cover conduct which causes data output, execution of a computer program, modification of data held in a computer and copying or moving data. With the exception of a provision in the *Tasmanian Criminal Code* which states that “gaining access” includes “communication with a computer”,²¹¹ Australian legislation contains neither definition nor explanation of the term.

Though the draft provisions are more explicit than existing Australian legislation, they avoid the technicalities of the UK *Computer Misuse Act 1990*, which provides extended explanations of computer “output” and “use” of a computer program. The Committee is of the view that these definitions are unnecessarily complex. For details see Appendix 3.

208 *Crimes Act 1914* (Cth) s76D; *Crimes Act 1900* (NSW) s309; *Crimes Act 1900* (ACT) s135J.

209 *Summary Offences Act 1966* (Vic) s9A: “gain access to or enter a computer system”.

210 *Computer Misuse Act 1990*, s17(2).

211 *Criminal Code* (Tas) s257A.

4.2.2 Meaning of access to data, modification of data and impairment of electronic communication

- (1) In this Part, 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.
- (2) In this Part, *modification* of data held in a computer or data storage device means:
 - (a) the alteration or removal of the data, or
 - (b) an addition to the data.
- (3) In this Part, *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.
- (4) A reference in this Part to any such access, modification or impairment is limited to access, modification or impairment caused (whether directly or indirectly) by the execution of a function of a computer.

Modification of Data

The definition follows, in its essentials, the corresponding provision of the UK *Computer Misuse Act 1990*.²¹²

Impairment of data and impairment of electronic communications

The Code proposes an offence of impairing communications to or from a computer. The offence is aimed at such tactics as flooding email with input beyond its capacity, resulting in system breakdown(s.4.2.6). The offence of unauthorised modification of data in s4.2.5 is also defined in terms requiring proof of an impairment of access to data or the reliability, security or operation of data. Unlike “access” and “modification” the concept of “impairment” is not defined. It extends to any harm affecting electronic communications. In this respect “impairment”, which includes intangible as well as tangible harms, is akin to the undefined concept of causing “damage” to property.

The Code will not deal with interception, which raises quite different issues and is the subject of specialised legislation.

²¹² *Computer Misuse Act 1990*, s17(7), see Appendix 3.

4.2.3 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.

4.2.3 Meaning of unauthorised access, modification or impairment

Hackers and other outsiders who impair electronic communications, modify or obtain access to data, in the absence of any entitlement to do so, clearly act without authorisation. So also when an individual obtains permission to do any of these things by means of fraud or subterfuge. In these cases the offender breaches a barrier intended to keep out intruders.

Cases involving insiders who misuse their authority are more difficult. A person who is entitled to impair electronic communications, modify or obtain access to data, pursuant to permission, may do so for an ulterior purpose. Victorian case law, drawing an analogy with the law of burglary, holds that the insider who misuses authority in this way, is guilty of the summary offence of computer trespass.

Computer Trespass in Victoria: The Meaning of Unauthorised Entry

Section 9A of the Victorian *Summary Offences Act* 1966 states that a person must not “gain access to or enter a computer system or part of a computer system without authority”. A bank employee with access to a computer terminal took an automatic teller “off host,” so enabling himself to overdraw his account. He was authorised to perform this operation in certain circumstances, but not in order to enable himself to operate his own account. Charged with computer trespass, he escaped conviction at first instance. The magistrate was of the view that the offence was limited to unauthorised entry by outsiders or hackers. In *Director of Public Prosecutions v Murdoch* [1993] 1 VR 406, Hayne J upheld an appeal against the magistrate’s decision. Since entry was “not within the scope of...permission”, the employee was guilty of entering the system without lawful authority.

The decision in *DPP v Murdoch* was based explicitly on the Victorian law of burglary, which requires proof that the burglar entered the building as a trespasser: [*Crimes Act* 1958 (Vic) s76]. In *Barker* (1983) 153 CLR 338, the High Court held that a person who had permission to enter a building may be a trespasser if entry is made for purpose which was expressly or impliedly excluded by the terms of the permission. The High Court divided, however, on the question whether entry is trespassory when the permission is general in scope, but the purposes are dishonest and plainly contrary to the tacit expectations of the invitor. In *DPP v Murdoch*, Hayne J suggested that entry to a computer system would not be trespassory if the person had a general permission to use the system, even though entry was for the purpose of committing a fraud.

The persuasiveness of the analogy with burglary depends vary largely on the fact that the Victorian offence is expressed in terms of a spatial

Code

| |
|--|
| |
|--|

metaphors of trespass. The “computer system” to which the provision refers is conceived as a space divided into parts which the offender enters, as a trespasser. Elsewhere, existing prohibitions avoid reliance on the spatial metaphor. The corresponding offence in s309(1) of the New South Wales *Crimes Act* 1900 simply makes it an offence to “obtain access to...data stored in a computer” without authorisation.

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.²¹³ 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 Offences*, Final Report, December 1995, s16.3(2) and commentary, pp83-89]. The recommendation of the Committee on this issue was the subject of divergent responses. Law enforcement agencies divided on the question whether the concept of unauthorised access should be confined in the way suggested by the Committee.²¹⁴ Consideration of those submissions which argued in favour of a more expansive definition of unauthorised access has not persuaded the Committee to alter its views on the issue.

It should be noted, at the outset, that the issue is unlikely to arise in the offences which prohibit unauthorised modification of data [s4.2.5] and unauthorised impairment of electronic communications [s4.2.6]. 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,

213 *Barker* (1983) 153 CLR 338. There is no doubt, of course, that the shoplifter steals if property is taken and liability for attempted theft is incurred if a would be shoplifter tries to steal. The question is whether a person entering a shop, or an invited guest who enters the house with intent to steal, should be guilty of the far more serious offence of burglary.

214 Victoria Police 5 April 2000, per Neil O'Loughlin Deputy Commissioner Policy and Standards; New South Wales Police Service, 31 March 2000, per Michael N Holmes, General Manager. The recommendation was supported by Australian Federal Police, 28 April 2000, per John Guerts, Director Technical Operations. A helpful and detailed submission from the Police Commissioners' Conference Electronic Crime Steering Committee, 2 May 2000, per MJ Palmer, Chair, PCCECSC, noted the absence of unanimity among law enforcement agencies on the acceptability of the Committee recommendation. The recommendation was opposed by the Model Criminal Code Review Committee, Western Australia, 20 March 2000, per Hon Justice Scott.

Code

| |
|--|
| |
|--|

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 [s4.2.4]. It is also likely to arise, of course, when the summary offence of unauthorised access to restricted data is charged [discussed below at p187]

The Emerging Caselaw on Unauthorised Access

The Chapter 4 draft provisions follow the *Computer Misuse Act 1990* (UK) in making a distinction between unauthorised access and misuse of authorised access. In *R v Bow Street Metropolitan Stipendiary Magistrate*²¹⁵ the House of Lords held that misuse of authorised access for an ulterior purpose would not fall within the scope of prohibitions against unauthorised access. A woman called Joan Ojomo, who was a Florida based employee of a United States credit card company, was able to obtain general access to client's accounts. Though this was something which Ojomo was able to do, she was only authorised to access particular client's accounts if they had been assigned to her by her employer. She accessed other accounts, without authorisation, and obtained information which enabled her and her fellow conspirators to withdraw money from those accounts. One of the conspirators, a man called Allison, was arrested in England. The United States Government sought to extradite him for trial in the United States, a procedure which required proof that the conduct amounted to an "extradition offence" in English law. The question at issue, eventually resolved against him by the House of Lords, was whether Joan Ojomo's conduct amounted to the offence of securing unauthorised access to data, within the meaning of ss1, 17(5) of the *Computer Misuse Act 1990*. Their Lordships held that the Act imposes liability when the offender is not authorised to secure access to data "of the kind in question". Since Joan Ojomo was not authorised to access the particular accounts which were the target of the conspirators' fraudulent activities, her conduct would have been an offence in England and so provided grounds for extradition of her fellow conspirators. It is implicit in their Lordship's decision that s1 of the English Act would have no application to Joan Ojomo's conduct, if she had taken information for fraudulent purposes from the accounts to which her

²¹⁵ *R v Bow Street Metropolitan Stipendiary Magistrate and another, ex parte Government of the United States of America* 1999; noted JC Smith, "Case & Comment" [1999] Crim LR 970. See also *Bigall* [1998] 1 Cr App R 8, approved by the House of Lords and comment on that decision by Professor JC Smith, "Case & Comment" [1998] Crim LR 53. Compare *Stockdale*, Victorian Court of Appeal No126/1995, in which the offender was convicted, on a plea of guilty, to charges of obtaining and divulging protected Commonwealth information relating to clients of the Department of Social Security.

Code

| |
|--|
| |
|--|

authorisation extended. In the circumstances, however, neither mere *capacity* to obtain access to data nor the fact that she had authority to obtain access to similar data, relating to other client's accounts, could provide an answer to the charge of unauthorised access.

The few recent Australian authorities on unauthorised access are consistent with the House of Lords decision. In *Gilmour*,²¹⁶ a decision of the New South Wales Court of Criminal Appeal, the offender was an employee who had access, via password and user ID to a Commonwealth Tax Office computer. He made certain entries granting taxpayers relief from obligations without the required authorisation from his superior to do so. The Court upheld his conviction for unlawful alteration of data, contrary to s76C of the *Crimes Act 1914* (Cth). The fact that he was authorised to use the computer and had the capacity to make the entries provided no answer to the charge, for he had no authorisation to alter the particular data in question.²¹⁷

The effect of the Committee's recommendation should not be exaggerated. There was a tendency, on the part of those who advocate a more extended definition of unauthorised access, to conceive of the offence in broad terms, as one of unauthorised access to a "computer" or "computer system." The Chapter 4 offences are far more discriminating in their effect however. The authorisation must relate to the particular data in question. The prohibitions avoid making general references to computers and computer systems and prohibit instead, unauthorised access to data, unauthorised modification of data or unauthorised impairment of communications between computers. The fact that an offender has authority to use the computer system has no bearing on the questions whether there is authority to obtain access to particular data, modify that data or impair communications. Nor does the mere fact that the offender is able to obtain access to data on an employer's computer amount to authority to do so. In this respect, the draft conforms to existing law.²¹⁸

Though the Committee remains of the view that misuse of authorised access for an ulterior purpose should not fall within the scope of the Chapter 4 offences,

216 *Regan Gerard Gilmour v DPP NSW CCA No60488/95*

217 Compare *United States v Morris* (1991) 928 F2d 504 (2d Cir. 1991) cert. denied, 502 US 817 (1991) which draws a similar distinction. Morris, who was authorised to use computers at Cornell University, where he was a graduate student, devised a computer virus which he released on the Internet. The virus was designed to penetrate programmes on other computers linked to the network and replicate itself in those programmes. Morris' use of the Email facility to *send* his messages would not amount to access without authorisation, though his purpose was sabotage. He was guilty of an offence of unauthorised access because his programmed virus enabled him to obtain access other computers to which he had no account and no authority for entry.

218 *Regan Gerard Gilmour v DPP NSW CCA No60488/95*.

Code

| |
|--|
| |
|--|

there is an undoubted need for one or more specialised offences which would deal with misuse of authorised access to particular categories of data. So, for example, one of the submissions made particular reference to the misuse of authority by police officers who obtain access to computer records and sell or pass on confidential information from those records.²¹⁹ The Committee touched on those issues in the introduction to this part of the Report. Legislation which imposes criminal penalties for obtaining confidential information, sale or publication of that information cannot be restricted to instances where the offender happened to acquire the information by operating a computer.

Absence of authorisation is an element of each of the offences in this Part. There will be occasions, however, when mistakes are made concerning the scope of authorisation. Liability can only be imposed if the accused was both unauthorised and aware of the fact that the activity was unauthorised.

²¹⁹ The issue was raised specifically in the submission from Police Commissioners' Conference Electronic Crime Steering Committee, 2 May 2000, per MJ Palmer, Chair, PCCECSC. For instances in reported cases, see *Regan Gerard Gilmour*; *ibid*; *Bignall* [1998] 1 Cr App R 8.

4.2.4 Unauthorised access, modification or impairment with intention to commit serious offence

- (1) A person who causes any unauthorised computer function:
- (a) knowing it is unauthorised, and
 - (b) with the intention of committing a serious offence, or facilitating the commission of a serious 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 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 communications to or from any computer.
- (3) For the purposes of this section, a *serious offence* is:
- (a) an offence in this jurisdiction punishable by imprisonment for a period of 5 years or more, or
 - (b) an offence in any other jurisdiction, being an offence so punishable if committed in this jurisdiction.
- (4) A person may be found guilty of an offence against this section:
- (a) even if committing the serious offence concerned is impossible, or
 - (b) whether the serious 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.

Unauthorised access, modification or impairment to commit a serious offence

Elements of the offence

Physical:

- unauthorised access to data held in any computer; or
- unauthorised modification of data held in any computer; or
- unauthorised impairment of electronic communications to or from any computer.

Fault:

- knowledge of absence of authorisation;
- intent to commit or facilitate commission of an offence punishable by imprisonment for five or more years by the person or by another person.

Penalty:

- imprisonment for a term equal to the penalty for the offence which the offender intended to commit or facilitate.

Nature and rationale of the offence

The provision combines elements of existing Australian offences which penalise frauds involving computers, with the more general offence in the UK *Computer Misuse Act*, of unauthorised operation of a computer with intent to commit a serious offence.²²⁰ The scope of the proposed offence extends well beyond existing Australian legislation and, in some respects, exceeds the scope of the English provision as well. A “serious offence” is an offence punishable by 5 years imprisonment.

Section 4.2.4 is a preparatory offence, akin to an attempt to commit the principal offence, and it is accordingly punishable, like attempt, with the same penalty as the principal offence.

Considered as a preparatory offence, akin to attempt, s4.2.4 contains a crystallised proximity rule. The offence is committed if and when the offender causes an unauthorised computer function with the appropriate intention. As in attempt law, liability is imposed even if the intended or principal offence is impossible of achievement. Liability extends beyond the scope of the offence of attempt, however, to include conduct which was intended to facilitate the commission of an offence by another person.²²¹ In view of its character as a preparatory offence, liability for attempting this offence is specifically excluded.

²²⁰ *Computer Misuse Act* 1990 s2.

²²¹ Compare Model Criminal Code: Chapter 2, s11.1(7).

Code

| |
|--|
| |
|--|

Using computers for crime: the inadequacy of existing legislation

Legislatures in many jurisdictions have extended the law of theft and fraud to cover obtaining services, goods or money by fooling a computerised dispenser. So, for example, legislation in New South Wales and Victoria extends the offence of obtaining property or a financial advantage by deception so as to include conduct which “deceives” a machine or computer.²²² As the reference to “machines” indicates, the conduct caught by these prohibitions is not limited to computers. Chapter 3 of the Model Criminal Code: *Theft, Fraud, Bribery and Related Offences*, like the New South Wales and Victorian provisions, equates “deception” of a person with unauthorised conduct which evokes a response from a computer or machine.²²³ These provisions, which ensure that the general offences of dishonesty extend to instances of fraud involving computers, may require supplementation by specialised and more precisely targeted offences for specific forms of fraud. So, for example, the potentiality for security market manipulation by use of the almost unlimited communicative capacities of the internet in spam campaigns will almost certainly require the creation of one or more specialised offences.²²⁴

New South Wales, Northern Territory, ACT and Tasmania have enacted specialised offences of using a computer with intent to defraud.²²⁵ Most of these provisions appear capable of application in cases where access is authorised or the computer, data and programs in question belong to the offender.²²⁶ Section 135L of the ACT Crimes Act reduces the diversity of these provisions to the essential elements of liability:

222 *Crimes Act* 1900 (NSW), s178BA; *Crimes Act* 1958 (Vic) s81(4). See also s83A(9)(a) which equates persons and machines for the purpose of imposing liability for inducing a person to accept a false document as genuine and act on it, to that person's prejudice. For the interpretation of this difficult provision, see *DPP v Murdoch* [1993] 1 VR 406. See I Leader-Elliott & M Goode, “Criminal Law” in *Annual Survey of Australian Law* (1993) 181 at pp221-226.

223 Chapter 3, Model Criminal Code s17.3. See also s19(1) and (2), unauthorised acts inducing machines to respond to discs, tapes & 19.6, devices for making false documents.

224 Problems associated with unsolicited commercial electronic communications, known colloquially as “spam” range from nuisance essentially akin to any other form of junk mail to major communications interdiction or major fraud. The development of codes of regulation for unsolicited electronic mail is discussed in the introduction to this segment. Particularly informative submissions on the potential for fraud involved in mass spam campaigns were received from Australian Securities and Investment Commission 27 April 2000, per Joseph P Longo, National Director, Enforcement.

225 *Crimes Act* 1900 (NSW) s309(2); *Criminal Code Act* 1983 (NT) s276; *Crimes Act* 1900 (ACT) s135L; *Criminal Code Act* 1924 (Tas) s257B.

226 In New South Wales, s309(2) *Crimes Act* 1900 requires proof that the offender “obtained access” to data with intent to defraud &c. Nothing in the provision requires proof that the access was unauthorised. Compare the Commonwealth *Crimes Act* provision in s76D, which restricts liability to cases involving unauthorised access to data or programs with intent to defraud. Section 257B *Criminal Code Act* 1924 (Tas) looks as though it might have been intended to apply only when the offender causes a computer owned by another to perform some function. There is no explicit limitation to this effect, however, and the offence extends to the use of any computer with intent to defraud. The provision appears to derive from the recommendation of the Law Reform Commission of Tasmania, *Computer Abuse* Report No 47, Recommendation 3(I). The Northern Territory provision, s276 *Criminal Code* 1983, prohibits unlawful alteration, erasure &c, with intent to defraud.

Code

| |
|--|
| |
|--|

A person who, by any means, dishonestly uses or causes to be used, a computer... or part of a computer...with intent to obtain by that use a gain for himself or herself or another person, or to cause by that use a loss to another person, is guilty of an offence...²²⁷

This offence, like its counterparts, is preparatory in form, imposing liability even before the offender has reached the point of attempting to commit a crime of dishonesty. It makes no difference whether the offender uses a computer with or without authorisation. Moreover the prohibition extends to use of the offender's own computer for a fraudulent purpose. In this respect the offence is a near relation to the traditional offence of "going equipped for theft", which appears in s16.7, Model Criminal Code Chapter 3: *Theft, Fraud, Bribery and Related Offences*.²²⁸

Offences of this nature, which were originally designed to plug holes in theft legislation, cannot play a major role in the control of crime involving computers. The risks of serious crime involving unauthorised use of computer data and networks extend well beyond fraud and related property offences. The marked variations between jurisdictions in the penalties imposed for these preparatory offences reflect a general legislative failure to realise and define the potential risks associated with unauthorised use of computer data for criminal purposes. With the exception of the ACT and Northern Territory provisions, the penalties are minor, appropriate to summary offences.²²⁹ Minor penalties are appropriate, in view of the fact that they extend to conduct by an authorised user of a computer or use of the offender's own computer. Moreover the potential involvement of unauthorised operations involving computers and computer networks in the commission of serious offences extends well beyond fraud and other offences of dishonesty.

A generalised preparatory offence of unauthorised computer conduct

An offence of unauthorised modification, access or impairment of electronic communications with intent to commit another offence should not be restricted to offences involving dishonesty. An outlaw computer hacker may be activated by an intention to cause injury to people or damage to tangible property. In *Crime and the Computer* (1991), Martin Wasik points to the increasingly apparent risks of physical harm to person or property associated with hacking and other forms of computer misuse:

227 *Crimes Act* 1900 (ACT) s135L extends liability to dishonest use of a computer or "machine", defined as a "machine designed to be operated by means of a coin, banknote, token, disk, tape or any identifying card or article."

228 The proposed Model Criminal Code offence is punishable by two years imprisonment. This is consistent with the New South Wales and the Commonwealth offences of using a computer with intent to defraud, both of which are punishable by two years imprisonment. Compare s135L of the ACT *Crimes Act*, which imposes a 10 year penalty.

229 *Crimes Act* 1914 (Cth) s762B(2) [2 years imprisonment]; *Crimes Act* 1900 (NSW) s309(2) [2 years]; *Crimes Act* 1900 (ACT) s135L, 10 years; s276 *Criminal Code* 1983 (NT) imposes a 3 year penalty for alteration &c of data with intent to defraud and 7 years if the offender intends another to rely on altered data.

Code

| |
|--|
| |
|--|

[S]ince computers now perform so many safety-critical tasks, in the near future we can expect to see computer malfunctions as increasingly significant causes of death and injury. In ... 1985 there were terrorist attacks on the computer and communications systems of Tokyo Airport and the Japanese railways.²³⁰

If injury is caused or damage is done, offenders can be convicted of the appropriate offences against person or property. If injury or damage is averted, however, unauthorised access with intent is a sufficiently discrete and identifiable form of wrongdoing to deserve specific prohibition and punishment.²³¹

Liability for the offence extends to cases in which the offender, acting without authorisation, modifies or obtains access to data held in a computer disk or other removable data storage device. When the disk or device is placed in any computer, including a computer owned by the offender, data stored in the disk or device becomes “data held in a computer” within the meaning of s4.2.1.²³²

Penalty

The penalty for this offence is not fixed at any particular term of years. In this respect it is unlike the offences of impairment of data [s4.2.5] and impairment of communication [s4.2.6], both of which are punishable with a maximum of ten years imprisonment. The degree of wrongdoing here is geared to the offence which the offender intended to commit, by unauthorised access to data, unauthorised modification or impairment of data. The degree of wrongdoing can be less than that involved in the ss4.2.5 and 4.2.6 offences. This offence does not require proof of impairment of data or of electronic communication. Mere unauthorised access is sufficient, if accompanied by an intent to commit an offence punishable by five years imprisonment. On the other hand, the degree of wrongdoing involved in a s4.2.4 offence may far exceed the wrong involved in offences of impairing data or communications. Consistent with its character as a preparatory offence, akin to attempt, the penalty matches that of the principal offence, which the offender intended to commit.

230 M Wasik, *op cit*, 150.

231 One submission suggested that the s4.2.4 offence should be extended by allowing liability to be imposed for an attempt to obtain access to data, modify data or impair communications with intent to commit an offence: Legal Aid Western Australia 31 March 2000, per George Turnbull, Director. The committee remains of the view that liability for attempt is inappropriate when the offence in question is itself a preparatory offence, punishable with the same degree of severity as the projected offence. An offender who attempts to modify data, impair communications or obtain access without authorisation would be liable for an attempt to commit one of those offences.

232 So also the *Computer Misuse Act* 1990 (UK): see s17(6).

4.2.5 Unauthorised modification of data 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 4.1.6 (Damaging property), or
- (b) an offence against section 4.2.6 (Unauthorised impairment of electronic communications).

Unauthorised Modification Of Data To Cause Impairment

Elements of the offence

Physical:

- conduct causing
- unauthorised modification of data held in any computer or data storage device

Fault:

- knowledge of absence of authorisation for modification
- intent to impair access to, or impair reliability, security or operation of data held in any computer or data storage device or recklessness as those consequences

Penalty:

- 10 years imprisonment

Nature and Rationale of the Offence

Physical damage to the cabinet, keyboard or other physical components of a computer will be an offence against the criminal damage provisions of Chapter 4. Is it necessary to provide a supplementary form of liability when unauthorised interference with a computer causes impairment of data rather than physical damage? British case law on criminal damage suggests that the concept of damage is sufficiently flexible to cover impairment of data: any unauthorised erasure or alteration of data or programs could be said to result in damage to a computer disk or other storage medium, for the erasure or alteration will inevitably involve a rearrangement of magnetic particles on the disk:

What the Act requires to be proved is that tangible property has been damaged, not necessarily that the damage itself be tangible. There can be no doubt that the magnetic particles upon the metal discs were part of the discs and if the appellant was to have intentionally and without lawful excuse altered the particles in such a way as to cause an impairment of the value or usefulness of the disk to the owner, there would be damage within the meaning of [the Criminal Damage Act 1971].²³³

There seems no particular reason to restrict the application of the Court's argument to "magnetic particles". From this Olympian vantage, any

²³³ *Whitely* (1991) 93 Cr App R 25, at 28 per Lord Lane CJ. The decision in *Whitely* appears to have resolved the uncertainties apparent in the reasoning in *Cox v Riley* (1986) 83 Cr App R 54, discussed M Wasik, *op cit*, 140ff. See also, Brown, "Computer Related Crime Under Commonwealth Law, and the Draft Federal Criminal Code" (1986) 10 Criminal Law Journal 377 at 386.

Code

unauthorised rearrangement of atoms or molecules, resulting in an impairment of the use or value of a disk or computer, will amount to property damage.

The equation of damage with unauthorised molecular rearrangement seems more ingenious than practical and would require courts to subscribe to a faintly embarrassing fiction in the construction of offences of criminal damage. Though it is possible that any conduct worth catching in a specially drafted offence already falls within the scope of criminal damage legislation it is preferable, in principle, if distinctive kinds of wrongdoing, like impairment of computer data or programs, are made the subject of specific legislative provision.

Several Australian jurisdictions have enacted legislation forbidding what is commonly described as “damaging computer data”. Section 4.2.5 draws on these provisions and the corresponding offence in s3 of the UK *Computer Misuse Act* 1990. The Code offence is more narrowly drawn than existing Australian provisions which extend to conduct which merely involves unauthorised use of a computer. The Code offence is conceived as an extension of criminal damage offences to cover analogous harms to intangible property.

Though legislation against criminal damage extends to harms of a very minor character, the offence is nevertheless limited by a requirement that the offender do something which can be described, with reasonable accuracy, as damage to property. Mere unauthorised use of another’s property or conduct which impedes another’s use of property is not criminal damage. It has long been accepted that the distinction between damage and misuse in criminal damage legislation expresses a principled division between matters which are appropriate for criminal punishment rather than a civil lawsuit or disciplinary action in the workplace. No justification is apparent for abandoning these principled limits when liability for offences involving computers, computer programs or data is in issue. Chapter 4 accordingly avoids imposing criminal liability for misuse of data or computers. The offence requires proof of modification with intent to impair data or recklessness as to such impairment. The Code offences are supplemented, however, by a summary offence of unauthorised access to restricted data [see p 186].

Computer misuse and data damage: the Australian compromise

Section 310 of the *Crimes Act* 1900 (NSW)) is titled “Damaging data in a computer”. The provision, which was derived from s76C of the Commonwealth *Crimes Act* 1914, is representative of the approach taken in a number of Australian jurisdictions: compare ss135K *Crimes Act* 1900 (ACT); s257C *Criminal Code Act* 1924 (Tas); *Criminal Code Act* 1899 (Qld) s408D. The offence carries the same 10 year penalty as criminal damage. Despite its misleading title, it extends well beyond conduct involving damage or impairment of property or its intangible equivalents.

Code

| |
|--|
| |
|--|

s310 Damaging data in computer

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 for penal servitude for 10 years, or to a fine of 1,000 penalty units, or both.

The provision contains two distinct kinds of prohibition. The first, which forbids unauthorised destruction, erasure, alteration or insertion of data into a computer, is limited to conduct which activates a computer function. The description of the offence is misleading: liability does not require proof of anything which could be described as damage to data or programs. Since data includes information, unauthorised use of a computer will almost certainly involve the “insertion of data.” Whatever may be said of erasure or alteration, insertion of data need not involve harm or damage to the computer, its functions, data or programs.

The second leg of the offence, forbidding conduct which interrupts, obstructs or interferes with lawful use of a computer, extends to conduct which may involve no function of the computer or its programs. On a literal reading, an unauthorised act of locking the door of the computer room, in order to prevent access, would fall within the scope of the offence.

The breadth of application of the New South Wales offence might have been appropriate had it been restricted, like the Commonwealth provision from which it was copied, to misuse of *government* computers.²³⁴ In its present form, however, it includes much trivial misconduct which should not fall within the scope of a criminal prohibition punishable by a substantial prison term.²³⁵ The penalty of 10 years imprisonment for unauthorised interference with a computer is twice the penalty for destroying it entirely, under the criminal damage provisions, unless the destruction is accomplished by fire or explosives.²³⁶ Much conduct which

²³⁴ Compare, however, the far more tightly drawn provisions of the *Computer Fraud and Abuse Act* 1986 (US) 18 USC 1030.

²³⁵ The New South Wales Police Service, 31 March 2000, per Michael Holmes, mounted a defence of the provision on the grounds of its “utility and broad application”. It was argued that the provision should be retained “to deal with unforeseen circumstances which may arise in the future”. The Committee remains of the view that more precisely targeted legislation is required to deal with computer damage.

²³⁶ *Crimes Act* 1900 (NSW) s195.

Code

| |
|--|
| |
|--|

will fall within the scope of the New South Wales offence falls well short of the minimal levels of wrongdoing required for conviction of criminal damage.

The proposed Code offence covers two quite different kinds of harm. It will be an offence to modify programs so as to impair their reliability, security or operation. The offence will also extend to any modification resulting in alteration, deletion or concealment of electronic data so as to deny information to authorised users. The latter effect of the prohibition is a computer specific variation on existing criminal damage offences of defacing a document, altering it or rendering it illegible.

There are three broad areas of operation of the offence:

- A person with limited authorisation impairs data or programs by engaging in an unauthorised operation on data or programs;
- A hacker obtains unauthorised access to data or program and then modifies, causing damage or impairment;
- Offender causes damage or impairment by circulating a disk containing a worm or virus &c which infects the target computer data or program via the actions of an innocent agent.²³⁷

The British Comparison²³⁸

The British prohibition against unauthorised modification of computer data was enacted against a background of concern about the acceptable limits of criminal liability. Section 3 of the *Computer Misuse Act 1990* was meant to complement s1 of the *Criminal Damage Act 1971*. It forbids impairment of the use of a computer, impairment of data or hindering access to data in a computer. The offence extends to impairment or hindered access resulting from the circulation of an infected disk or other storage device. So far as data stored in a computer are concerned, the British offence and Model Criminal Code draft cover the same ground. Unlike the Model Criminal Code draft, however, the British offence does not extend to impairment of data held in a data storage device.

²³⁷ Model Criminal Code, Chapter 2: *General Principles of Criminal Responsibility* (1992) s11.3 (Innocent Agency).

²³⁸ Canadian Law, as expressed in s387 of the Canadian *Criminal Code*, comes close to the form of the New South Wales provisions: see the discussion in M Wasik, *op cit*, 146-147. It should be noted, however, that the Canadian provision dealing with computer crime rides piggyback on criminal damage provisions which are significantly more general in their effect than NSW offences of criminal damage. Wasik, *ibid*, criticises Canadian law for its excessive breadth.

Code

| |
|--|
| |
|--|

Like other serious offences in the *Computer Misuse Act 1990*, unauthorised modification of the contents of a computer is punishable by a maximum penalty of five years imprisonment. That is substantially less than the ten year penalty for the offence of criminal damage in the UK *Criminal Damage Act 1971*. The reduced penalty may have been intended to reflect a perceived difference between the wrongs involved in damage to tangible property and intangible impairment of data. The decision to differentiate between the penalties for criminal damage and the data impairment offence required the erection of a barrier between the offences. The Act declares that modification of the contents of a computer will not amount to criminal damage unless the modification “impairs...the physical condition” of the computer or data storage device.²³⁹ With the passage of time, it is apparent that there is no reason to avoid an overlap between the offences. They deal with essentially similar kinds of wrongdoing. There is no reason why smashing a computer cabinet should carry twice the penalty which can be visited on an offender who impairs computer data - an offence which may result in catastrophic economic loss or disruption.

Fault: recklessness, conditional intentions and conditional harms

Liability is imposed for intentional and reckless impairment alike. In this respect, the provisions require the same fault elements as the criminal damage offences. The net is cast more widely here than it is in s3 of the UK *Computer Misuse Act 1990*, which requires proof of an intention to impair data.²⁴⁰

Though the majority of cases may be expected to involve modifications which result in an immediate impairment of data, the offence does not require proof of impairment. It is sufficient if the modification was done with an intention to impair or recklessness as to a substantial risk of impairment. The prospective form of the offence differentiates it from counterpart offences of criminal damage.

Impairment of data may be contingent on a future event. The activities of a saboteur may result in the placement of a logic bomb in a computer program, timed to detonate on the occurrence of a future event. The event may be one which is certain to occur, such as the next conjunction of the 13th day of the month with a Friday, or the event may be a more or less remote contingency. If the bomb detonates, resulting in an impairment of data or programs, the offence is of course committed. The plant may be discovered, however, before that moment. Early discovery may occur, for example, where the saboteur reveals the existence of the threatened harm, coupling a demand for money or some

239 *Computer Misuse Act 1990*, s3(3). ATH Smith, op cit, para 11.23 suggests that the drafter’s intent has miscarried and that the offence of unauthorised modification will always involve an “impairment [of the] physical condition” of a computer or data storage device in consequence of *Whitely* (1991) 93 Cr App R 25.

240 It is accordingly unnecessary to include a provision like s3(3) of the *Computer Misuse Act 1990*, which declares that the intention to cause impairment need not be aimed at any particular data.

Code

| |
|--|
| |
|--|

other advantage with a promise to deactivate the bomb. Quite apart from liability for blackmail, under s18.1, Model Criminal Code: Chapter 3, *Theft, Fraud, Bribery and Related Offences*, such an offender would commit offences against ss4.2.4 and 4.2.5. Data in a computer has been modified and it has been modified with the intention of causing impairment or with recklessness as to that eventuality. A conditional intention is nonetheless an intention,²⁴¹ as when a burglar takes a gun to shoot the nightwatchman in case he should turn up at the scene of the crime.

Computer Disks, Tapes or Other Storage Media

Like the other computer offences, liability for impairment of data contrary to s4.2.5 extends to impairment of data on computer disks and other data storage devices. If the disk or other storage device is held in a computer or if it is otherwise accessible by a computer, impairment of data on the device will amount to an offence: see 4.2.1. In this respect, the Committee's proposals have a more extensive operation than existing Australian legislation or the UK *Computer Misuse Act* 1990, which are restricted to impairment of data "stored in a computer".²⁴² Since the essence of the offence is the impairment of data, the level of protection should not change according to whether data or programs on disks or other storage devices are external to the computer or incorporated within its cabinet. The harm involved in unauthorised modification of data is the same. Since it is almost certainly beyond the limits of interpretive latitude for any court to hold that a floppy disk is a computer, the draft extends the ambit of prohibition to include data held on a disk or other storage medium.

241 Different types of intention, perhaps, but intentions nonetheless: see K Campbell, "Conditional Intention" (1982) 2 L.S. 77; JW Meiland, *The Nature of Intention* (1970) Chapter 2. Section 2.02(6) of the American Law Institute's Model Penal Code (1962) provides a crisp articulation of principle: "When a particular purpose is an element of an offence, the element is established although such purpose is conditional, unless the condition negatives the harm or evil sought to be prevented by the law defining the offence."

Note the definition of intention at section 5.2 of Chapter 2:

"Intention

5.2(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."

242 See: *Crimes Act* 1914 (Cth) s76C: refers to data "stored in...a computer". Though s76A defines "computer" to include "a part of a computer system", this will not include most storage devices. The same limitation is found in State and Territorial legislation: see s310, *Crimes Act* 1900 (NSW); *Crimes Act* 1900 (ACT) s135K. The *Criminal Code Act Compilation Act* 1913 (WA) refers to "information stored in a ... system" (s440A). "System" is defined in the same section to mean "a computer system or a part or application of a computer system". In the UK, s3 of the *Computer Misuse Act* 1990 is similarly limited to unauthorised modification of the "contents of any computer". Compare *Computer Fraud and Abuse Act* 1986 (US) 18 USC 1030(e)(1) which defines "computer" to include "any data storage facility...operating in conjunction with" a computer.

Code

Omissions

Section 4.2.5 requires proof of an act resulting in impairment of data. The New South Wales Act, like its Commonwealth and ACT counterparts, does not impose liability on a person who *omits* to record or store data in a computer. Though the Tasmanian Law Reform Commission once recommended a more inclusive prohibition, extending to those who omitted performance of a contractual or other duty to introduce, record or store data, the recommendation was not adopted. Chapter 2 of the Model Criminal Code requires specific provision or positive implication before liability can be imposed for an omission.²⁴³ The Committee could see no justification for an extension of liability to include cases where impairment resulted from breach of a contractual or other duty.

Penalty

In Australian jurisdictions which recognise the offence, damage to data or programs generally carries a ten year prison sentence.²⁴⁴ It is apparent from the British provisions that attempts to distinguish between this offence and criminal damage are both complex and unnecessary. Since the offences overlap and serious cases of damage to data or networks are at least equivalent, in terms of wrongdoing, to serious cases of damage to tangible property, the penalties for criminal damage and criminal data impairment should also be equivalent.

Alternative Verdicts

Section 4.2.5 overlaps the criminal damage offence in s4.1.5. The extent of the overlap depends on the extent to which courts are willing to classify the molecular rearrangements involved in processing data as “damage”, when those molecular rearrangements result in harm to human interests. It is important to ensure that the formulation of offences of impairing data and criminal damage avoid any encouragement to litigation disputing the metaphysical location of the borderline between the offences. The draft assumes that the offences can overlap and makes provision for alternative verdicts. In cases where the harm done by the alleged offender involves nothing which could be readily described as physical damage, the safer course is to charge the offence of unauthorised impairment of data.

²⁴³ Model Criminal Code Chapter 2: *General Principles of Criminal Responsibility*, s4.3 restricted liability to “acts” unless liability for omissions is specified or necessarily implied.

²⁴⁴ Tasmanian *Criminal Code Act* (1924) s257C carries a nominal penalty of 21 years imprisonment, in common with all Code offences for which penalties are not specifically provided.

4.2.6 Unauthorised impairment of electronic communication

- (1) A person who:
- (a) causes any unauthorised impairment of electronic communications 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 4.1.6 (Damaging property), or
 - (b) an offence against section 4.2.5 (Unauthorised modification of data to cause impairment).

Unauthorised Impairment of Electronic Communication

Elements of the offence

Physical:

- conduct causing;
- unauthorised impairment of electronic communication to or from a computer.

Fault:

- knowledge of absence of authorisation for impairment;
- intent to impair electronic communication to or from the computer or recklessness as those consequences.

Penalty:

- imprisonment 10 years.

Nature and Rationale of the Offence

Communications links between computers are vulnerable to attack directed against the target computer; against carriage service providers, including Internet providers and attacks against the communications system itself. Prohibitions against criminal damage will catch offenders who engage in the cruder forms of physical interdiction of communications. The s4.2.5 offence of modification with intent to impair data will extend to some more sophisticated forms of attack. Not every impairment with communications results in an impairment of data however. Attacks may take a variety of forms. Communications links to the target computer may be blocked by flooding the system with unwanted messages. The target computer may be induced to generate sufficient volume of messages to prevent communication. Addresses may be altered and messages rerouted. Impairment of communications by the use of these and similar means are collectively described as “denial of service attacks”. Though some involve impairment of data, others do not.

Offences involving telecommunications facilities aside, the proposed offence has no counterpart in existing legislation.

Like other offences in this chapter, s4.2.6 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. In this respect, s4.2.6 is consistent with offences of criminal “damage” in Part 4.1 and, in this Part, with the s.4.2.5 offence of impairment of data which will also catch conduct which is transient and trifling in its harmful effects. Once it is accepted that

Code

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.

Fault: recklessness, conditional intentions and conditional harms

Like the s4.2.5 offence of data impairment, s4.2.6 imposes liability for reckless as well as intentional impairment of communication. Unlike s4.2.5, which extends to prospective impairment of data, this provision requires proof that communication was impaired. Threats to impair communication, coupled with an unwarranted demand, may amount to blackmail, contrary to s18.1 of Model Criminal Code - Chapter 3: *Theft Fraud, Bribery and Related Offences* (1995) and Chapter 2: *General Principles of Criminal Responsibility* (1992) will impose liability for an attempt to impair communications.

Omissions

Section 4.2.6, like the other provisions in Part 4.2 requires proof of an act resulting in impairment of communication between computers.

Federal, State and Territorial Offences

This offence, like others proposed in the Discussion Paper, overlaps offences in Commonwealth law. Provision is currently made, in s76F, of the *Crimes Act* 1914 (Cth) to preserve the operation of existing state and territorial computer offences against challenge based on s109 of the Constitution. Similar provision will be necessary to preserve the operation of this offence. The issue is discussed in more detail in the introduction to the computer offences.

Penalty

The offences of criminal damage, impairment of data and impairment of communication between computers overlap substantially in application. Though each is capable of application to trivial or transient misconduct, commission of any of these offences may involve substantial and serious public harms. The offence of impairing communications between computers, like criminal damage and impairment of data, is accordingly punishable by 10 years imprisonment.

Alternative Verdicts

In marginal cases, Part 4.2 offences overlap with each other and they overlap as well with the offence of criminal damage. Determining the extent of these overlaps will involve nice questions of interpretation involving issues which may be of considerable technical complexity. Provision is made to avoid unmerited acquittals by permitting courts to convict of the alternative when the wrong offence is charged.

4.2.7 Possession of data with intent to commit computer offence

- (1) A person who is in possession or control of data:
- (a) with the intention of committing a computer offence, or
 - (b) with the intention of facilitating the commission of a 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 computer offence concerned is impossible.
- (4) It is not an offence to attempt to commit an offence against this section.

4.2.7 Possession of data with intent to commit computer offence

Elements of the offence

Physical

- possession of a computer, data storage device or document in which data is held or recorded; or
- control of data held in a computer that is in the possession of another person.

Fault

- intention to commit an offence of:
 1. unauthorised access with intent to commit a serious offence [s4.2.4] or
 2. unauthorised modification of data to cause impairment [s4.2.5]; or
 3. unauthorised impairment of electronic communications [s4.2.6]; or
- intention to facilitate an offence of:
 4. unauthorised access with intent to commit a serious offence [s4.2.4] or
 5. unauthorised modification of data to cause impairment [s4.2.5]; or
 6. unauthorised impairment of electronic communications [s4.2.6].

Nature and rationale of the offence

Several submissions suggested that there was need for a range of preparatory offences which will penalise individuals caught in possession of data or programmes which are intended for use in the commission of a computer offence.²⁴⁵ Possession with intent covers a part of this field. A separate offence, of obtain, produce or supply data with intent to commit a computer offence” is also proposed [s4.2.8]. Both offences are derived from the Council of Europe Draft Cybercrime Convention.²⁴⁶ A brief discussion of the draft convention can be found in the introductory discussion of the computer offences in this Report.

²⁴⁵ New South Wales Police Service, 31 March 2000, per Michael Holmes, General Manager; Australian Federal Police, 28 April 2000 per John Geurts, Director Technical Operations.

²⁴⁶ Draft No 22, October 2000. See <<http://conventions.coe.int/treaty/en/projets/cybercrime.htm>>

Code

**COUNCIL OF EUROPE: DRAFT CONVENTION ON
CYBERCRIME**

Preparatory Offences: Article 6 - Illegal Devices

Each party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law when committed intentionally and without right:

- (a) The production, sale, procurement for use, import, distribution or otherwise making available of:
 - 1. a device, including a computer program, designed or adapted [specifically] [primarily] [particularly] for the purpose of committing any of the [proposed offences of illegal access, interception or interference with data];
 - 2. a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed with intent that it be used for the purpose of committing the [proposed offences of illegal access, interception or unauthorised interference with data].
- (b) The possession of an item referred to in paragraphs (a)(1) and (2) above, with intent that it be used for the purpose of committing the [proposed offences of illegal access, interception or unauthorised interference with data]. A party may require that a number of such items be possessed before criminal liability attaches.

These preparatory offences supplement the law of attempt, incitement and conspiracy in their application to offences of unlawful data modification [s4.2.5] and interference with electronic communications [s4.2.6].

Prohibitions directed against supply or possession of the means of committing criminal offences are endemic in criminal legislation. The proposed offence of possession with intent is analogous to the offences of “going equipped for stealing” in Chapter 3 of the Code,²⁴⁷ and “possession of a thing with intent to damage property” in this Chapter: see s4.1.10. The offence is committed by anyone who is in possession of data with intent to commit the offences of unauthorised modification of data to cause impairment [s4.2.5]; unauthorised impairment of electronic communications [s4.2.6] and unauthorised access &c with intent to commit a serious offence [s4.2.4].

247 Section 16.7, Model Criminal Code, Chapter 3: *Theft, Fraud, Bribery and Related Offences*, Final Report 1995, pp 102-103.

Code

| |
|--|
| |
|--|

The essential element in offences of this nature is the requirement of proof of intention to commit a further offence. The nature of the object or entity possessed will usually lend evidential support to the allegation of that ulterior intent, but that is not a necessary element of the offence. The draft makes no attempt to restrict liability to cases involving possession of data or programs which are specially adapted to the commission of an offence. In this respect, the offence resembles the offences of going equipped for stealing and possession of a thing with intent to damage property, neither of which restrict the range of things which can provide the possessory foundation for liability. Like those offences, it is not supplemented by the possibility of liability for attempt under Chapter 2 of the Code.

It is possible to envisage an individual who is caught in the process of devising a computer program which is intended for use in commission of an offence against this part. Though liability will not be incurred for the offence of possession with intent, the next succeeding offence of obtain, produce or supply data with intent will extend to this activity [s4.2.8].²⁴⁸

Application of the possession offence may be as simple and obvious as it is in corresponding cases where a would-be burglar is found in possession of a jemmy or an instruction manual for safeblowers. But an offence which includes “possession” of electronic data poses peculiar problems of definition. The offender may be caught in possession of a computer, a disk, a printout or some other tangible item of property plainly intended for use in a projected computer offence. In many instances, however, application of the offence will not involve physical possession of tangible devices, tokens or records. It would be contrary to principle to introduce an offence which permitted criminal conviction simply on the ground that a person *knows* a procedure, routine or password and intends to use that knowledge to commit an offence of data modification or interference with electronic communications. Criminal liability requires some tangible manifestation of the crime charged and offences of possession have never extended to the possession of secret information unless it is recorded in some tangible form. Safecrackers who memorise the combination of the target safe do not “go equipped for stealing”. The offence of possession of data with intent does retain the requirement of some tangible manifestation of the crime charged. It is undeniable, however, that the requirement is attenuated by comparison with more familiar possessory offences.

Liability for the offence is intended to extend well beyond those cases in which the offender is found in physical possession of some tangible thing intended for use in a computer offence. The data may have been parked in computer which is in the possession of an innocent, who may be completely unaware of its existence. The reference to data in the possessor *or control* of the offender is intended to extend the application of the offence to individuals who have access

248 Liability pursuant to s4.2.8 is extended by application of Part 2.4 of Model Criminal Code - Chapter 2 *General Principles of Criminal Responsibility*, which impose liability for attempt, incitement and conspiracy.

Code

| |
|--|
| |
|--|

to data without physical possession of the computer or other device in which it is stored. The requirement of control, rather than mere access to data, is intended to limit the offence to circumstances in which there is some exclusivity of access.²⁴⁹

Fault Elements

Unlike the substantive offences of *unauthorised modification of data to cause impairment* [s4.2.5] and *unauthorised impairment of electronic communications* [s4.2.6], liability is restricted to those who possess data with the intention of committing one of those offences. There is no liability for mere recklessness. It should be noted, however, that “intention” bears an extended meaning in the Code so that some offenders will be caught though one would not describe their connection with the projected offence as purposive. Circumstances and results which comprise the elements of an offence are taken to have been intended if the offender believes that they are practically certain to exist or occur: [ss5.2(2) and (3)]. A person who was in possession of data, knowing that this would facilitate the commission of a computer offence by another person, will be taken to have intended to facilitate commission of the projected offence.

Jurisdiction

Since this offence extends to data held in a computer which is the possession of another, it is quite possible for a person in Victoria to plan an act of electronic vandalism by utilising data held in a computer in, say, New Zealand, to damage communications in, say, Canada. Potentially difficult jurisdictional issues are involved when an offence is defined by reference to conduct which is accompanied by an intention to commit an offence. That might seem to entail a requirement of proof that the projected offence which is to occur in another jurisdiction, would be an offence against this Part. Jurisdictional issues are sufficiently complicated without inviting this further level of complexity. Ordinary jurisdictional principles of State, territorial or Commonwealth law will apply to the conduct element of the possession offence. So far as the projected offence is concerned, however, it is sufficient to show that it would amount to an offence against this Part *or* that it would amount to a corresponding offence against the laws of the place where the impairment of data or communications is intended to occur.

Penalty

The penalty of three years imprisonment is the same as the penalties imposed for other Code offences of possession with intent.

²⁴⁹ Any person with an internet connection has access to data which will enable the transmission of pornographic images; provide instructions for the manufacture of bombs and a host of other dangerous or illegal enterprises. It cannot be said, however, that one has *control* over such data so long as it is in the public domain. Control denotes some degree of exclusivity of access. If, however, a person downloads any of this information into a computer or disk which is in their possession or control, they are in possession or control of that data.

4.2.8 Producing, supplying or obtaining data with intent to commit computer offence

- (1) A person who produces, supplies or obtains data:
- (a) with the intention of committing a computer offence, or
 - (b) with the intention of facilitating the commission of a 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, *produce, 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 computer offence concerned is impossible.

4.2.8 Obtain, produce or supply data with intent to commit computer offence

Elements of the offence

Physical

- obtain data; or
- produce; or
- supply data

Fault

- intention to commit an offence of:
 1. unauthorised access with intent to commit a serious offence [s4.2.4] or
 2. unauthorised modification of data to cause impairment [s4.2.5]; or
 3. unauthorised impairment of electronic communications [s4.2.6]; or
- intention to facilitate an offence of:
 4. unauthorised access with intent to commit a serious offence [s4.2.4] or
 5. unauthorised modification of data to cause impairment [s4.2.5]; or
 6. unauthorised impairment of electronic communications [s4.2.6].

Nature and rationale of the offence

Like the preceding offence of possession of data with intent, the offence of obtain, produce or supply with intent was proposed in submissions to the Committee²⁵⁰ and adapted from the Council of Europe Draft Cyber-crime Convention.²⁵¹

The primary object of the provision is to catch those who devise, propagate or publish computer programs which are intended for use in the commission of a computer offence. The scope of prohibition is broad, extending from conduct which is barely distinguishable from simple possession to conduct which might

250 New South Wales Police Service, 31 March 2000, per Michael Holmes, General Manager; Australian Federal Police, 28 April 2000 per John Geurt, Director Technical Operations.

251 Draft No 22, October 2000 at <<http://conventions.coe.int/treaty/en/projets/cybercrime.htm>>

Code

| |
|--|
| |
|--|

be described as trafficking in programs intended to damage data, communications or violate access restrictions. As a consequence of this potential breadth of application the law of attempt applies so as to impose liability on would-be procurers, inventors and suppliers.

Obtain, produce or supply data

The expression is intended to include the activities of “production, sale, import, procurement for use, distribution or otherwise making [data] available” in Article 6 of the Draft Cybercrime Convention.

Though the provision refers to data in held in a computer, data storage device or data recorded in a document, the definition is not exhaustive and it imposes no restriction on the form which the data might take. Data includes “information in any form” and extends to any computer program or part of a computer program [s4.2.1].

Jurisdiction

Like the offence of possession with intent, this is an offence which is defined in part by reference to the offender’s intention to commit a further offence. The same potential for jurisdictional puzzles arise, since the offender’s intention to commit an “offence against this Part” invites the question whether the projected offence would fall within the jurisdictional provisions of the Code. So far as the projected offence is concerned, it is sufficient to show that it would either amount to an offence against this Part or that it would amount to a corresponding offence against the laws of the place where the projected offence is intended to occur.

Penalty

The offence overlaps the s4.2.7 offence of possession with intent and, in view of their common origin in Article 6 of the Draft Cyber-crime Convention, carries the same penalty of 3 years imprisonment.

Summary Offence

Unauthorised access to or modification of restricted data

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

Maximum penalty: Imprisonment for 2 years.

- (2) 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.

Comparison

See also section 44 of *Summary Offences Act 1953 (SA)*

- (1) A person who, without proper authorisation, operates a restricted access computer system is guilty of an offence. ...
- (3) A computer system is a restricted access computer system if -
 - (a) the use of a particular code of electronic impulses is necessary in order to obtain access to information stored in the system or operates the system in some other way; and
 - (b) the person who is entitled to control the use of the computer system has withheld knowledge of the code or the means of producing it, from all other persons, or has taken steps to restrict knowledge of the code, or the means of producing it, to a particular authorised person or class of authorised persons.

Criminal Code (WA), s440(1)(b) is framed in similar terms to the South Australian provision.

Unauthorised Access To Restricted Data

Elements of the offence

Physical:

- cause access to;
- restricted data held in computer;
- without authorisation.

Fault:

- intention to cause access;
- knowledge that access is unauthorised.

Nature and rationale of the offence

Prohibitions against unauthorised access have, as their primary target, the activities of the “hacker”, an outsider with no semblance of authority for access to computer data or programs. In practice, however, hackers are far outnumbered by individuals who exceed a limited authorisation for the use of a computer in the course of employment or similar relationships.²⁵² The proposed summary offence, like its existing counterparts in Australian and British law, extends alike to hackers and insiders who exceed their authority.

Like the Code offences in Part 4.2, the summary offence is restricted to conduct which provides access to data by means of a programmed function of the computer. Merely to inspect data on a computer screen without permission is no offence, though a person who displays restricted data to another would fall within the prohibition. The offence is restricted to data which is protected by an access control system, such as an entry code or password. Unauthorised access to data is an offence whether or not the computer in which the data is stored is part of a network or linked system of computers.²⁵³

The formulation of the offence follows the UK *Computer Misuse Act 1990* in placing primary emphasis on the need to ensure the integrity of computer systems and networks against unauthorised access. Though the draft prohibition will provide a measure of protection for privacy, that benefit is incidental to its main purpose. In the absence of general laws imposing criminal penalties for invasions of privacy, the Committee was not persuaded that liability should be imposed simply because private information happens to be stored in the form of computer data. The need to ensure the security and integrity of systems, rather than claims to privacy, justifies the existence of the offence. The UK Law Commission is persuasive on this issue:²⁵⁴

252 See *Computer Misuse Law Com No186 1989*, para 3.35. See also Review of Commonwealth Criminal Law: *Interim Report Computer Crime* (1988) para 4.43.

253 Compare *Attorney General's Reference* (No 1 of 1991) [1993] QB 94.

254 *Computer Misuse Law Com No186 1989*, para 1.29.

Code

In our view the most compelling arguments for the criminalisation of hacking are those stemming from, first the actual losses and costs incurred by computer system owners whose security systems are (or might have been) breached; secondly, that unauthorised entry may be the preliminary to general criminal offences and thirdly, that general willingness to invest in computer systems might be reduced, and effective use of such systems substantially impeded, by repeated attacks and the resulting feeling of insecurity on the part of computer operators....The importance of the integrity and proper functioning of operational computer systems is...obvious and the need for total confidence in that integrity leads to great expense and inconvenience if such systems are penetrated, even if later investigations show that no actual impairment of the system had been achieved.²⁵⁵

Existing Australian offences of unauthorised access tend to display a certain confusion about the objectives sought to be achieved. Liability is sometimes imposed for conduct resulting in unauthorised access to the computer itself, rather than data held in the computer.²⁵⁶ A decade or so after their enactment, these prohibitions appear incongruous. Criminal liability for making temporary use of another's chattels without permission is rarely imposed in our law. Whatever may have been the case when computers were exotic, costly and scarce, it can no longer be argued that they require a protection of the criminal law against unauthorised use when other appliances used in the home or office are not protected in this way.

Similar arguments tell against the assumption that private information should acquire special status, protected by criminal prohibitions and penalties, simply because it is stored in a computer. In New South Wales, the prohibition against unauthorised access was copied from Commonwealth law, which derived in turn from the *Review of Commonwealth Criminal Law*, prepared by the Gibbs Committee. The pattern of prohibition in these jurisdictions was set by provisions originally designed to protect Commonwealth government data and Commonwealth computers. But protection of confidential government information involves issues which are far more limited and particular than those which engage a law reform committee charged with drafting model legislation of general application.

²⁵⁵ *Ibid*, paras 2.14, 2.15.

²⁵⁶ See *Crimes Act 1900* (NSW) s310(b), which makes it an offence to interrupt, obstruct or interfere with the "lawful use of a computer"; *Summary Offences Act 1966* (Vic) s9A, "access...a computer system"; Tasmanian *Criminal Code*, s257D: "access to a computer [or] system of computers". Compare the conclusion of the English Law Commission that: "an authorised user should not commit a hacking offence merely because he uses the computer for an unauthorised purpose....our view remains that there is nothing to distinguish the misuse of an employer's computer from the misuse of the office photocopier or typewriter, and that it is therefore inappropriate to invoke the criminal law to punish conduct more appropriately dealt with by disciplinary measures": *Computer Misuse Law Com No 186 1989*, para 3.38. (But compare Law Commission, *Computer Misuse*, Working Paper No110 1988, 89).

Code

| |
|--|
| |
|--|

In one respect, the summary offence proposed by the Committee is narrower in application than its British counterpart in s1 of the *Computer Misuse Act 1990*. The protective scope of the draft offence is limited to data which is protected by an access control system such as a password. The Committee adopted this restriction on the scope of the offences from existing legislation in South Australia and Western Australia.²⁵⁷ These provisions are unusual in the Anglo-Australian context, though there are parallels in West German and Norwegian law, which also restrict the unauthorised access offence to computer material which is the subject of some form of special protection.²⁵⁸ The Scottish Law Commission, which reported in 1987, rejected the limitation on the ground that discrimination against computer systems which were not protected by a password or other security device would not be justified: “[J]ust as the law of theft does not distinguish between householders who lock all their doors and those who do not, so too...it would be inappropriate to distinguish between owners with and without security devices or systems”.²⁵⁹ With the passage of time, the inconsistency which the Scottish Law Commission perceived in the proposal is less apparent than the need to set some limit to potential criminal liability. Computer ownership has proliferated and computers are familiar elements in employment, education, recreation and entertainment. Access restriction, whether by password or more sophisticated means, is now general when administrative, commercial or personal considerations require data to be protected. If access is not restricted in this way, it is reasonable to suppose that there is nothing at stake worth the imposition of criminal penalties.²⁶⁰ General prohibitions which threaten criminal penalties for mere breaches of trust or of good manners are incongruous and unnecessary.

Fault Elements

The offence requires proof that a person accused of the offence knew that access was unauthorised. Neither negligence nor recklessness is sufficient for liability when absence of authorisation is in issue. The fault requirements for guilt are more demanding in this respect than they are in existing Australian law. New South Wales legislation, in common with Commonwealth, Tasmanian and ACT

257 *Summary Offences Act 1953 (SA)* s44; *Criminal Code Act Compilation Act 1913 (WA)* s440(1)(b).

258 M Wasik, *op cit*, 80.

259 Scottish Law Commission (1987) para 4.15, quoted M Wasik, *op cit*, 80-81. See too Hughes, “Recent Developments in Australian Computer Crime Regulation” (1991) 7 *Computer Law and Practice* 94, at 96, criticising the South Australian provisions on the ground that they provide insufficient protection for confidential data.

260 A submission from the New South Wales Police Service, 31 March 2000, per Michael Holmes, took issue with the Committee’s conclusion on this point, drawing an analogy with the offence of burglary, an offence which can be committed even though the door to the burgled premises is not locked. The analogy tells in favour of the Committee’s conclusion, rather than against it. The offence of burglary is committed by one who enters premises with intent to commit a crime. The offence of unauthorised access is committed simply by entry, regardless of the offender’s purpose. General prohibitions which threaten criminal penalties for mere breaches of trust or of good manners are incongruous and unnecessary.

Code

| |
|--|
| |
|--|

variants, requires proof that the offender obtained access “intentionally”²⁶¹ though the provisions are not explicit on the point, it appears that they require no more than recklessness with respect to the fact that access was unauthorised.

When the activities of a hacker or other intruder are in question there is rarely room for doubt that the offender knew that the activity was unauthorised. Proof that an insider, such as an employee, knew that access was unauthorised may be more difficult. Section 1 of the UK *Computer Misuse Act 1990*, like the proposed draft, restricts criminal liability to an offender who “knows at the time he causes the computer to perform the function” that access is unauthorised. The Law Commission, which proposed the restriction, justified it on two grounds. The first - which relates to British uncertainties over the meaning of “recklessness”²⁶² - has no application in Australian law. The second is of more direct relevance:

[I]f the hacking offence is to be aimed at protecting the integrity of the computer (and our view is that it should), then there is no justification for exempting employees who threaten that integrity. We have emphasised...the importance that we attach to a definition of *mens rea* in terms that make it clear that intentional and not merely reckless access is required. Any conduct on the part of an employee that fell within the definition would...be a deliberate act of disobedience, and indeed of defiance of the law and not merely carelessness, stupidity or inattention. The latter might legitimately attract disciplinary sanctions, but should not in our view be a ground for criminal liability.²⁶³

The Law Commission defended the requirement of knowledge on the ground that it would require management “to identify, and to be clear about the status of, the person alleged to have authority to control the access which is in issue.”²⁶⁴ The Review of Commonwealth Criminal Law appears to have been of the same view: “Access without authority would include the case of a person who has limited authority, but *knowingly* exceeds that authority...”²⁶⁵

261 *Crimes Act 1914* (Cth) s76B; *Crimes Act 1900* (NSW) s309; *Crimes Act 1900* (ACT) s135J; *Criminal Code Act 1924* (Tas) 257D. In Victoria, the offence of computer trespass in s9A of the *Summary Offences Act 1966* makes no reference to fault elements. The unauthorised access offences in South Australia and Western Australia are similarly reticent on the point: *Summary Offences Act 1953* (SA) s.44; *Criminal Code* (WA) s440(1)(b).

262 Law Com No186, para 3.62 fn72, raises the issue in the context of the offence of unauthorised modification of data or programs.

263 Law Com No186, para 3.36.

264 *Ibid*, para 3.37; M Wasik, *op cit*, 78. See, in a similar vein, S Krishcock, *op cit*, 106-107. If liability is to be imposed on individuals who exceed authorisation to obtain access to data or programs, the person who gives the authorisation should bear the onus of making the limits clear.

265 Commonwealth Attorney General's Department: Review of Commonwealth Criminal Law - *Interim Report on Computer Crime* (November 1988) para 4.52.

Code

| |
|--|
| |
|--|

The Committee is persuaded that the imposition of liability on insiders who exceed their authority would not be justified unless it can be proved that the offender knew that access was unauthorised.

Unauthorised access by employees and other insiders

In practice, hackers are far outnumbered by individuals who exceed a limited authorisation for the use of a computer in the course of employment or similar relationships.²⁶⁶ An insider, such as an employee, commits the offence if a restricted computer program is executed or if restricted data is displayed, copied, moved or modified with the knowledge that the operation is unauthorised.

Insiders who obtain unauthorised access to programs or data protected by a password or other restriction will commit the offence.²⁶⁷ So, for example, the provision catches an employee who defies an employer's ban and bypasses a restriction to obtain access to the internet via the employer's computer. No liability is incurred, however, if access to the internet is authorised but the employee misuses the opportunity in order to view pornography or place a bet on a horse race. Conduct of this nature is no more than unauthorised use of a computer. In his discussion of British proposals for a new offence of unauthorised use of a computer, Martin Wasik remarks that most instances of unauthorised use are too trivial for criminal penalties:

It is the kind of matter which is better dealt with by way of warning or other disciplinary action taken by an employer. The question is how to distinguish these cases from the few serious cases where the defendant may be running his own profitable business in his employer's time, using his employer's computing facilities.²⁶⁸

Wasik concludes that an employee accountant, who exceeded authorisation in this way, would *not* be guilty of obtaining unauthorised access to the employer's data or program under the *Computer Misuse Act 1990*.²⁶⁹ Australian law on the point is more equivocal. In Victoria, where the offence is formally defined as "computer trespass", unauthorised access has been held to include the case where an employee misuses authorised access to a computer system for an unauthorised purpose.²⁷⁰ New South Wales law, which makes it an offence to obtain access to a program or data stored in a computer "without authority" is at best equivocal on the issue.

266 See *Computer Misuse Law Com No186 1989*, para 3.35. See also Review of Commonwealth Criminal Law: *Interim Report Computer Crime* (1988) para 4.43.

267 Compare Review of Commonwealth Criminal Law, *ibid*, para 4.52: "[a]ccess without authority would include the case of a person who has limited authority, but knowingly exceeds that authority in making the access in question."

268 M Wasik, *op cit*, 100.

269 *Ibid*, 101-102. Accord: *R v Bow Street Metropolitan Stipendiary Magistrate and another, ex parte Government of the United States of America* 1999, noted J C Smith; "Case and Comment" (1999) *Crim LR* 1970.

270 *Director of Public Prosecutions v Murdoch* [1993] VR 406, discussed Leader-Elliott & Goode, "Criminal Law" in *Annual Survey of Australian Law* 1993, 181 at 221-226.

Code

| |
|--|
| |
|--|

There are persuasive arguments in favour of the British position on this issue. The criminal law does not recognise a general head of criminal liability for unauthorised use of property belonging to another. It is arguable, perhaps, that the law should be changed on this score. Perhaps it should be an offence to make unauthorised use of property belonging to another with a view to gain. If such an offence were to be introduced, however, there would be no reason to distinguish between liability for misuse of an employer's computer data and misuse of a delivery truck, haybaler or other plant and equipment.

Access for unlawful purposes

If the person who obtains unauthorised access is motivated by a dishonest purpose, the law of theft, fraud and related offences provides the appropriate rubric for liability. So, for example, a bank employee who makes a dishonest gain of financial advantage or money by using the bank's computer, will be liable to conviction of offences against Model Criminal Code: Chapter 3 - *Theft, Fraud, Bribery and Related Offences*.²⁷¹ Special provision may be necessary to ensure that criminal liability is imposed in cases where the computer is "deceived" by a person who exceeds their authorisation. The need for legislation of this kind is in no way specific to computers. It is equally necessary to guard against obtaining dishonest gain by manipulating other machines which dispense property or services. A person who uses a weighing machine, without paying the fee, commits the same offence, whether the machine is computerised or of traditional construction, operated by springs, weights and levers.

Penalty

Unauthorised access is a summary offence in New South Wales, punishable with a maximum of 6 months imprisonment. In this respect, it resembles its Commonwealth counterpart²⁷² and the corresponding offence in the UK *Computer Misuse Act 1990*.²⁷³ Elsewhere in Australia the offence carries similarly modest penalties.²⁷⁴

271 Final Report 1995, s17(1). In the obtaining offences, "deception" includes "conduct by a person that causes a computer system or any machine to make a response that the person is not authorised to cause it to do". In cases where property is obtained, as a consequence of use of a computer without authorisation, the offender will normally be guilty of theft on the ground that this is a simple appropriation without consent, contrary to s15.1, *ibid*.

272 *Crimes Act 1914* s76B(2).

273 *Computer Misuse Act 1990* (UK) s1.

274 *Summary Offences Act 1966* (Vic) s9A [Computer Trespass, 6 months imprisonment]; *Summary Offences Act 1953* (SA) s44, [Unlawful Operation of a Computer System, fine only unless the act was done with the intention of obtaining a benefit from or causing a detriment to another person]; *Criminal Code Act Compilation Act 1913* (WA) s440A, [1 year imprisonment]. *Criminal Code Act 1899* (Qld) s408D(1) [Unauthorised use of a restricted computer, 2 years imprisonment]; *Criminal Code Act 1983* (NT) s222 [3 years imprisonment]; *Crimes Act 1900* (ACT) s135J [2 years imprisonment]. The penalty regime in Tasmania is radically different from that of other Australian jurisdictions. The *Criminal Code Act 1924* imposes a standard penalty of 21 years imprisonment for most Code offences, including the s257—257E computer offences. These are duplicated in the *Police Offences Act 1935* - s43A-43D - where they are punishable with 2 years imprisonment.

Summary Offence

Unauthorised impairment of data held in computer disk, credit card, etc.

- (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 impairment is unauthorised, and
 - (c) who intends to cause that impairment,
- is guilty of an offence.

Maximum penalty imprisonment for 2 years

- (2) For the purposes of this section, impairment of the reliability, security or operation of any data is *unauthorised* if the person is not entitled to cause that impairment.

Unauthorised impairment of data

Elements of the offence

Physical:

- Conduct causing impairment of reliability, security or operation;
- Of data held in a computer disk, credit card, token, ticket or other device used to store electronic data;
- Absence of authorisation to cause impairment.

Fault:

- intention to cause impairment of reliability, security or operation;
- knowledge of absence of authorisation.

Nature and rationale of the offence

The distinction between this offence and the more serious offence of unauthorised modification of data to cause impairment [s4.2.5] depends on the undefined term “computer”. The more serious offence is limited in its application to “data held in a computer”. The summary offence extends to data held on a “computer disk, credit card, token or ticket or other device used to store data by electronic means.” In practice, the distinction is likely to involve frequent exercise of prosecutorial discretion rather than nice analysis of what can and what cannot be described as a computer. “Smartcards”, which might be described as a “device[s] to store data by electronic means” are, in reality, miniaturised computers. Both the indictable and summary offences are capable of applying to conduct which modifies data held on the smartcard.²⁷⁵

²⁷⁵ The summary offence will extend to some forms of damage to the smartcard which are not caught by s4.2.6, which is limited in its applications to modification of data resulting from an “execution of a function of a computer [s4.2.2(4)].

PART 4.3 - SABOTAGE

INTRODUCTION

It will be apparent that the sabotage offences in Part 4.3 are aggravated forms of the basic property damage and computer offences. Like arson [s4.1.7] and bushfire [4.1.8] they are directed against individuals who might cause catastrophic harm, for which especially severe penalties may be justified.

The proposed offences are derived from the United Nations General *Assembly Convention for the Suppression of Terrorist Bombing*.²⁷⁶ Relevant sections of the Convention are printed in Appendix 4 of this discussion Paper. The directly applicable requirements of the Convention, which has not yet been adopted by Australia, would only have a marginal effect on domestic law. It is limited in its application to terrorism which crosses national borders or involves foreign nationals²⁷⁷ and limited to acts of terrorism which involve the use of an “explosive or other lethal device”.²⁷⁸ If one disregards those limitations, however, the substance of the Convention suggests the existence of a significant gap in Australian domestic statute law. In most jurisdictions, property damage offences are directed at relatively minor forms of criminality; they are ill adapted for use against terrorists. Though existing state and federal legislation would impose some form of criminal liability for any instance of terrorist attack on public facilities, many of these offences are not punishable with penalties of appropriate severity.²⁷⁹

The Committee proposes offences of sabotage and threatened sabotage to fill the gap in existing law. Proposals for offences of this nature go well beyond existing legislation in most jurisdictions.²⁸⁰ It is anticipated, however, that Australia will adopt the Convention and, in consequence, the enactment of some form of anti-terrorist legislation will be obligatory.

The offences follow the formulation proposed in the Convention in their application to conduct which damages or involves a threat to damage public facilities or infrastructure. It is anticipated that prosecution for the offence would be reserved for instances of very serious criminal threats to public facilities. Sabotage requires proof of conduct which was intended to cause major economic loss, major disruption of government functions or a major disruption to the use of services by the public; threatened sabotage extends to conduct which is

276 Adopted General Assembly Resolution, 72 Plenary Meeting, 15 December 1997.

277 Convention, Article 3.

278 *Ibid*, Article 2(1).

279 *Ibid*, Article 4(b) requires parties to the Convention to make terrorist offences “punishable by appropriate penalties which take into account the grave nature of those offences”.

280 The exception is New South Wales, which adopted a modified version of the Discussion Paper proposal for sabotage offences in *Crimes Act 1900 (NSWE)* ss203A, 203B, 203C.

intended to induce fear of those consequences. The requirement, common to both offences, of intention to cause major disruption or major economic loss draws on formulations and definitions in the Convention.

The sabotage offences proposed in the Code are more broadly focussed than those in the Convention, which is restricted to terrorism involving bombs and lethal devices. Liability for sabotage is imposed when damage or disruption to public facilities results from a property damage offence or a conduct causing an unauthorised computer function (s4.3.1), which was intended to cause major disruption or major economic loss. There is no restriction to any particular means of causing damage or disruption, so long as those means involve commission of an offence of property damage or a computer offence.

The offence of sabotage resembles other, more familiar, offences of ulterior intention in the fact that individuals who intend very serious harm are still caught by the prohibition though the actual level of harm falls well short of their intentions.²⁸¹ Though proof of some damage or disruption is required, it is not necessary for the prosecution to establish that the actual level of damage or disruption caused by the offender's conduct involved major disruption or major economic loss. Though the offence may be regarded as inchoate, it is extended by the possibility of liability for attempt, incitement or conspiracy under Model Criminal Code - Chapter 2: *General Principles of Criminal Responsibility*, Part 2.4

In the Chapter 4 Discussion Paper, s4.3.1 applied to conduct which caused "damage to a public facility". The offence was limited by the requirement of "damage" and limited, in addition, by the definition of "public facility", which was oriented towards buildings, places, conveyances and other hardware. Submissions were invited on the question whether the offence should be drawn more widely, so as to encompass major disruption to services whether or not physical damage was caused to a facility. The object was to ensure that sabotage would extend to include electronic sabotage. Many of the submissions addressed the issue. Agreement on the need for an offence which would include sabotage by means involving computer crime was virtually unanimous. In its revised form, protected public facilities include communication services and public information systems. Damage or disruption to these systems, whether resulting from crude physical attack or attack by electronic means, falls within the scope of the offences.

281 Compare, for example, the familiar offence of wounding with intent to cause grievous bodily harm. In law, any breaking of the skin counts as a wound. In this offence it is the intention to cause a far more serious level of harm than a mere wound which justifies the heavy penalties imposed for the offence.

Part 4.3 - Sabotage

4.3.1 General definitions

In this Part:

property offence means:

- (a) an offence against Part 4.1, or
- (b) conduct in another jurisdiction that is an offence in that jurisdiction and that would constitute an offence against Part 4.1 if the conduct occurred in this jurisdiction.

public facility means any of the following (whether publicly or privately owned):

- (a) government facilities, including premises used by government employees in connection with official duties,
- (b) public infrastructure facilities, including facilities providing water, sewerage, energy, fuel, communication or other services to the public,
- (c) public information systems, including systems used to generate, send, receive, store or otherwise process electronic communications,
- (d) public transport facilities, including conveyances used to transport people or goods,
- (e) public places, including any premises, land or water open to the public.

unauthorised computer function means any of the following (within the meaning of Part 4.2):

- (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.

4.3.1 Definitions

“Property”

The definition of “property offence” includes all Part 4.1 offences. In terms of practical effect, however, the primary “property offence” to which reference is made is that of Damage to property [s4.1.6]. Other, more specialised offences in Division 2, like *Arson* [s4.1.7] and *Bushfire* [s4.1.8], which impose aggravated penalties for particular kinds of damage, are mere allotropes of the basic offence of property damage. It is quite unnecessary for the prosecution incur the additional burdens of establishing commission of one of the aggravated offences in order to gain a conviction for sabotage.

“Public facility”

The list of “public facilities” includes those specified in the *Convention for the Suppression of Terrorist Bombings*²⁸² and extends that list by the specific inclusion of “public information systems”. As in the Convention, the potential targets for sabotage include private property and private facilities which are available for public resort.

“Unauthorised Computer Function”

The unauthorised computer functions listed in the definition are identical in content to the prohibited result in the offences of unauthorised modification of data to cause impairment [s4.2.5]; unauthorised impairment of electronic communication [s4.2.6] and the proposed summary offence of unauthorised access to restricted data held in a computer [see p. 186].

²⁸² Convention, Article 1: see Appendix 4.

4.3.2 Meaning of damage to public facility

- (1) In this Part, *damage* a public facility means:
 - (a) cause damage to the facility or any part of the facility, or
 - (b) cause disruption to the use or operation of the facility.
- (2) For the purposes of an offence under this Part, a person causes any such damage or disruption if the person's conduct substantially contributes to the damage or disruption.

4.3.2 Meaning of damage to public facility

The offence of sabotage extends beyond destruction of public facilities to include conduct which causes a major disruption to their use by government or by the public. In short, damage includes disruption in the sabotage offences. An attack on a public information system may cause catastrophic breakdown of services though little or no physical damage results. For this reason the concept of “Damage” is defined more widely here than it is in Part 4.1, which deals with the property damage offences.

The definition of causation follows the form adopted in the property damage offences [s4.1.5].

4.3.3 Sabotage

A person:

- (a) who damages a public facility by committing a property offence or by causing an unauthorised computer function, and
- (b) who intends to cause:
 - (i) major disruption to government functions, or
 - (ii) major disruption to the use of services by the public, or
 - (iii) major economic loss,

is guilty of an offence.

Maximum penalty: Imprisonment for 25 years.

4.3.3 Sabotage

Elements

Physical elements

- conduct causing
 1. a property damage offence; or
 2. an unauthorised computer function.
- cause damage or disruption to a public facility by that conduct

Fault elements

- intention to cause
 1. major disruption to government functions; or
 2. major disruption to the use of services by the public; or
 3. major economic loss.

Definition

“Public facility” includes:

- government premises and facilities;
- public infrastructure, including water, sewerage, energy, fuel, communications;
- public information systems;
- public transport;
- public places.

Penalty

- 25 years imprisonment.

Nature and rationale of the offence

Sabotage is an aggravated form of criminal property damage or an aggravated form of one of the computer offences. The offence is based on proposals originally designed to deal with terrorism in United Nations General *Assembly Convention for the Suppression of Terrorist Bombing*.²⁸³ Conviction of the offence authorises imposition of particularly heavy penalties in circumstances where the offender caused, or meant to cause, major economic loss or major disruption to government functions or public services: See: Introduction to Part 4.3.

²⁸³ Adopted General Assembly Resolution, 72 Plenary Meeting, 15 December 1997.

Code

| |
|--|
| |
|--|

Sabotage by means of an unauthorised computer function will usually involve conduct which impairs data or electronic communications. It is apparent, however, that major disruption to public facilities could result from conduct which involved no more than unauthorised access to a electronic communication system. Though the Committee has not recommended a separate Code offence of unauthorised access, it is an element of the offence of sabotage and the offence of unauthorised access &c with intent to commit a serious offence [s4.2.4]. Reports from the United States suggest that hacker attacks may be motivated by a desire to demonstrate that the hacker's skills can subvert systems designed to ensure the secrecy of government information.²⁸⁴ Once it is known that the integrity of the system is breached, major disruption is possible if the system has to be shut down while new security precautions are taken. The Code offence of sabotage would extend to conduct of this nature, if the hacker acted with the intention of causing major disruption.

Fault requirements

Formulation of the offence follows the UN Convention in restricting liability to individuals who intend to cause major disruption or major economic loss. It is the element of deliberate attack on public or governmental facilities, which will frequently involve outright terrorism, which justifies the severity of the penalty proposed for sabotage. In the absence of proof of intention to cause harm of this magnitude, the penalties for criminal damage or the computer offences provide adequate sentencing ranges for the merely reckless offender.

In the Code, a person who acts with the realisation that a harmful consequence is certain to follow their action is taken to have intended that consequence.²⁸⁵

Supersession of existing offences of damage to infrastructure

Criminal liability for sabotage supplements the general offence of criminal damage. Taken together, the offences of sabotage and criminal damage eliminate the need for a host of particular provisions in existing law, dealing with damage to railways, waterways and other infrastructure.²⁸⁶

Penalty

Sabotage is by far the most serious of the Chapter 4 offences, punishable with the same severity as manslaughter or dangerous driving causing death. The draconic penalty for sabotage is a reflection of the origin of the offence as an anti terrorist measure.

²⁸⁴ See *United States v Morris* (1991) 928 F2d 504 for a well known example.

²⁸⁵ It is of interest to note that the definition of intention in Chapter 2: *General Principles of Criminal Responsibility* s5.2 resolves the much discussed jurisprudential problem of the "Strategic Bomber". For recent discussion, see AP Simester, "Why Distinguish Intention from Foresight" in AP Simester and ATH Smith, *Harm and Culpability* (1996) 71-103.

²⁸⁶ See, for example, *Crimes Act 1958* (Vic) ss225 - 246B; *Criminal Law Consolidation Act 1935* (SA) ss259, 260

4.3.4 Threaten sabotage

- (1) A person who:
 - (a) makes to another person a threat to damage a public facility by committing a property offence or by causing an unauthorised computer function, and
 - (b) intends that person to fear that the threat will be carried out and will cause:
 - (i) major disruption to government functions, or
 - (ii) major disruption to the use of services by the public, or
 - (iii) major economic loss,is guilty of an offence.
Maximum penalty: Imprisonment for 15 years.
- (2) In the prosecution of an offence against this section it is not necessary to prove that the person threatened actually feared that the threat would be carried out.
- (3) For the purposes of this section:
 - (a) a threat may be made by any conduct, and may be explicit or implicit and conditional or unconditional, and
 - (b) a threat to a person includes a threat to a group of persons, and
 - (c) fear that a threat will be carried out includes apprehension that it will be carried out.

4.3.4 Threaten sabotage

Elements

Physical elements

- conduct expressing or implying a threat to an individual or group;
- to damage a public facility;
- by conduct causing:
 1. a property damage offence; or
 2. an unauthorised computer function.

Fault elements

- intention to cause the person to whom the threat is made fear or apprehension:
 1. that the threat will be carried out; and
 2. fear that the threat will cause:
 - (a) major disruption to government functions; or
 - (b) major disruption to the use of services by the public; or
 - (c) major economic loss.

Definition

“Public facility” includes:

- government premises and facilities;
- public infrastructure, including water, sewerage, energy, fuel, communications;
- public information systems;
- public transport;
- public places.

Penalty

- 15 years imprisonment.

Nature and Rationale of the Offence

Chapter 4 proposes a general offence of threatening to cause property damage. The penalty for that offence will be comparatively small: most instances of threatened property damage involve trivial or implausible threats of property damage. Terrorism is in a different league and any prohibition of terrorist damage should be coupled with a prohibition of threats of terrorist damage.²⁸⁷

²⁸⁷ It is surprising that the Article 2 of the *Convention For The Suppression Of Terrorist Bombings*, which lists the proposed offences, makes no reference to threats of terrorist destruction.

Code

| |
|--|
| |
|--|

In terms of their claim to a place in the Code, the justification for the sabotage offences is similar to the justification for the public order offences of contamination and threatened contamination in Model Criminal Code - Chapter 8: *Public Order Offences: Contamination of Goods*. They are offences aimed at the public at large, rather than individuals. Unlike the contamination offences, however, sabotage and threatened sabotage do not require proof of intent to cause public alarm.

Fault elements

Threatened sabotage, like its parent offence, requires proof of *intention* rather than recklessness.²⁸⁸ The offence is aimed at terrorism and related conduct. There is, once again, a parallel with the Chapter 8 offence of threatened contamination, which requires proof of an intention to cause alarm.²⁸⁹ Lesser offences of causing or threatening property damage do not require proof of intention as to the consequences.

Penalty

Threatening sabotage is punishable by 15 years imprisonment. There is a substantial difference in culpability between this offence and attempted or completed sabotage, which is punishable by 25 years imprisonment. By contrast, no distinction is drawn between penalties for offences of contaminating goods and threatened contamination of goods in Chapter 8. In each of those offences, however, the offender is responsible for the same central harm - the intentional creation of public alarm or anxiety.

288 Compare Model Criminal Code - Chapter 8: *Public Order Offences: Contamination of Goods*, s8.1.4, false statements intended to cause public alarm.

289 *Ibid.*

PART 2.7 - GEOGRAPHICAL JURISDICTION (AMENDMENTS TO CHAPTER 2)

Introduction

By the early part of the nineteenth century, the common law had adopted the “territorial theory” of criminal jurisdiction, which is firmly based on the view that criminal jurisdiction is limited territorially. The practical legal effects of a strict view of the “territorial theory” are that (a) a criminal court has jurisdiction only over crimes committed within the territory over which it has domain; (b) once a criminal court has such jurisdiction, it always applies its own criminal law; and (c) no offender can be prosecuted in a place where he or she is not alleged to have committed a criminal act.²⁹⁰

It did not take the courts long to discover that this law of criminal jurisdiction, if strictly applied, would lead to poor results. In general terms, what began to happen can be summarised as follows:

“... strict invocation of the territoriality principle could potentially render certain transborder crimes unpunishable anywhere. In an effort to avoid such a result, the common law courts developed a number of interpretive techniques for characterizing the location of any given crime. The cumulative result of these varying interpretive mechanisms, however, has fallen far short of analytic clarity. ...the courts have taken different stances at different times and the general result...is one of doctrinal confusion. ...courts...[have] devised so many techniques for locating frauds, conspiracies, and other offences inside or outside a given jurisdiction that no one principle can possibly be said to reconcile the various pronouncements.”²⁹¹

The territorial theory was once thought to imply that only one locality can have jurisdiction over any one given crime. With the development of more flexible or, according to point of view, result oriented jurisdictional claims, that is not the case. One crime may be justiciable in a number of localities - and it is productive of confusion to approach the area with the idea that criminal jurisdiction is exclusive in this sense.

290 See, for example, Levitt, “Jurisdiction Over Crimes (Pt 1)” (1925-6) 16 J CL, Criminol & PS 316 at 324, and The English Law Commission, Working Paper No 29, *Codification of the Criminal Law: Territorial and Extraterritorial Extent of the Criminal Law*, (1970). Other useful articles are Sarkar, “The Proper Law of Crime In International Law” in Mueller and Wise, (ed), *International Criminal Law* (1965); Berge “Criminal Jurisdiction and the Territorial Principle” (1930) 31 Mich LR 238; and Leflar, “Extrastate Enforcement of Penal and Government Claims” (1932) 46 HLR 193.

291 Morgan, “*Criminal Process, International Law, and Extraterritorial Crime*” (1988) 38 UTLJ 245 at 270-271 paraphrasing and quoting the judgment of LaForest J in *Libman* (1985) 21 CCC (3d) 206.

The Territorial Principle

There are a number of decisions which illustrate the *strict* operation of the territorial principle in a more or less straightforward way.

In *Harden*²⁹³, the accused sold refrigerators. The operation was financed by a company in Jersey. Harden was based in England. He posted hire purchase agreements from England to Jersey. The documents included an “offer for sale” which included the sentence: “This offer may be accepted by you at any time within one month of the date hereof by sending your cheque for the net amount”. When an offer was accepted, the Jersey company would then post a cheque in satisfaction to the accused.

Some of the hire purchase forms were alleged to be fictitious. The accused was charged with obtaining the cheques by false pretences. An English court held that it lacked jurisdiction to try the case. On an examination of the documents, the court concluded that the accused and the victims had agreed that receipt of the documents by the post office in Jersey amounted to receipt by the accused. On that basis, any obtaining which took place as a result of the false pretences took place in Jersey - and out of the territorial jurisdiction of the English courts. The effect of the decision is that an agreement between the parties to a fraudulent transaction may determine the location of the crime and the jurisdiction of the courts. The decision has survived, despite considerable judicial criticism²⁹⁴. However, it is often distinguished, or characterised as a “high water mark” in territorialism.²⁹⁵

In *Hildebrandt*²⁹⁶, the accused was charged with, in substance, “putting” or “depositing” a bomb on an aircraft which was travelling between Sydney and Brisbane. The bomb was brought onto the aircraft in pieces and assembled by the accused on the flight. There was no evidence whether the accused “put” or “deposited” the completed bomb on the aircraft while it was over New South

293 [1963] 1 QB 8.

294 Notable, for example, by Lords Reid and Diplock in *Treacy* [1971] AC 537 at 551 and 563 and Lord Diplock in *Stonehouse* [1978] AC 55 at 63. However, it has gained new vitality by its application in *Manning* [1999] 2 WLR 430.

295 A good example of distinguishing *Harden* is *Tirado* (1974) 59 Cr App R 80. In that case, the accused was also charged with obtaining property by deception. The appellant ran an employment agency in England. He wrote to Moroccans in Morocco offering jobs for a fee. The Moroccans deposited money in a bank in Morocco at the suggestion of the accused. The bank then sent a draft to the accused who then deposited it in his bank. The court held that it had jurisdiction on the basis that the accused eventually obtained the proceeds in England. The court distinguished *Harden* on the tenuous basis that the suggestion made by the accused as to the method of payment by the victims did not amount to an agreement, express or implied, that deposit in the Moroccan bank concluded the transaction with the accused. *Selkirk* [1965] 2 CCC 353 is very similar to *Harden* and has come under similar criticism in, for example, *Horbas and Myhaluk* (1968) 67 WWR 95 and *Re Chapman* [1970] 5 CCC 46. In *Ancuta* (1990) 49 A Crim R 307, it was conceded that there was no jurisdiction where both (it seems) the initial obtaining and the false pretences took place outside the forum.

296 [1964] Qd R 43.

Wales or Queensland. The court held that in such circumstances, a Queensland court had no jurisdiction to try the accused for those offences. It further held that “putting” and “depositing” were single acts, so that, even if the bomb was assembled and put and deposited in New South Wales, the Crown could not successfully argue that the “putting” and/or “depositing” were continuous acts which, having been done in New South Wales, continued in effect when the aircraft entered Queensland airspace.²⁹⁷

Where an offence contains more than one element and one or more of those elements occur in different localities the territorial theory is difficult to apply. One way of overcoming the difficulty, is to interpret the offence in such a way that the location of one element becomes more important than that of the other(s). That more important element becomes “the gist of the offence” and its location crucial.

A standard example of the gist of the offence approach is *Treacy*²⁹⁸ in which the accused was charged with blackmail; demanding money with menaces. The accused posted a letter in England to the victim in West Germany. The letter contained the menaces. By a majority, the House of Lords held that the English courts had jurisdiction to try the offence. Lord Hodson, with whom Lord Guest agreed, held that the English *Theft Act* applied on its own terms to the facts of this case. That was so because it criminalised the making of the demand and the demand was made when and where the letter was posted. This was so because the superseded *Larceny Act* would have covered the case and it was presumed that Parliament, in enacting the *Theft Act*, should be presumed to have intended the law unchanged in this respect.

Lord Diplock gave two reasons for agreeing with the result.²⁹⁹ The first ground will be examined in more detail below. The second was based on his interpretation of the *Theft Act*. He took the view that that Act was designed to replace the technical and complex structure and content of the common law and ancient statutory offences with common-sense offences phrased in ordinary language. He then asked rhetorically: “would the ordinary person have said ‘I have made my demand’ when he posted the letter or when it was received?” In his view, the ordinary person would say “I have made by demand” when the letter was posted, and hence that was where the offence was committed.

Lords Reid and Morris dissented, their disagreement lying in their analysis of the “gist of the offence”. Lord Morris, for example, stated:

“...the notion of making an unwarranted demand with menaces involves that the demand is made to or of someone who could

297 The matter of “continuing” offences or elements of offences is dealt with below. Hildebrandt was convicted of equivalent offences in New South Wales: *Hildebrandt* (1963) 81 WN (NSW) Pt 1 143.

298 [1971] AC 537.

299 The first reason involves his theory of criminal jurisdiction, and will be examined below.

comply with it and who could be influenced by the menaces which accompany the demand. The act of making the demand is not, in my view, committed until it is communicated to the person who is being unjustifiably menaced. There must be contact between the demander and the victim. ...A demand is not made until it is communicated. If the demand is contained in a letter it is not made until the letter is received.”³⁰⁰

On the dissenting view, then, the “gist of the offence” was the communication of the demand and that did not take place within the forum.

In some cases, it is possible to assert jurisdiction under the territorial theory even though the main (gist) or only element of the offence *looks like* it took place outside the territory of the forum. That can be done if the crucial element of the offence can be regarded as “continuing” until it takes place in the forum as well. Put another way, this approach asserts that a conventional territorial analysis of a multi-element offence which seems to show that two or more elements of that offence are located within different territorial jurisdictions is insufficiently precise, and a little ingenuity can locate all elements of the offence within one territorial location.

An early example of this technique is *Ellis*.³⁰¹ In that case the accused made false representations in Scotland. As a result, he obtained goods on credit in England. He was charged in England with the offence of obtaining goods by false pretences. The majority in that case adopted a “gist of the offence” analysis. On that basis, the English court had jurisdiction. Although Wright J agreed that such an approach would solve the problem, he was also prepared to use an alternative route to the same end:

“The evidence is that the goods were delivered to, and therefore obtained by, the defendant in [England] under a representation in [Scotland], and I think that his possession of the goods may be treated as a possession in [England] under a representation made in [Scotland] and continuing in [England].”³⁰²

The key word is, of course, “continuing”. The false representation accompanied its maker back to England. Consequently, he was still “making” it to agents of the victim after his return to England. On this analysis, therefore, *both* the false pretence *and* the obtaining were located in England.

Continuing Crimes

If elements of offences may be analysed as continuing, so may whole crimes. The classic example is the crime of conspiracy. In *Doori*³⁰³ the accused were

300 At 555-556.

301 [1899] 1 QB 230. Compare *Bevan* (1986) 84 Cr App R 143.

302 At 241.

303 [1973] AC 807.

charged with conspiring in a number of European and African countries to import drugs into England with a view to their trans-shipment to the ultimate destination in the United States. The House of Lords held unanimously that the English courts had jurisdiction to try that crime. However, they were not unanimous about why that was so. Two of the Law Lords used the device of a continuing crime. Lord Pearson and Viscount Dilhorne thought that there was jurisdiction because, in their view, an agreement, once made, continues in effect wherever the conspirators are present. If the conspirators come to the forum, then the agreement comes with them, and is located there³⁰⁴. This is so, even if only one conspirator ventures to the forum, despite the fact that the law of conspiracy requires two to conspire as logic requires at least two pigeons to make a flock. The agreement makes the rest “present” by a fiction like the fiction of constructive presence.³⁰⁵ Although conspiracy does not require proof of an overt act under the agreement, the commission of an overt act is often vital to the proof of the agreement itself.³⁰⁶ So, in relation to jurisdiction, the proof of an overt act by the conspirator(s) in the forum is vital to proving the continuance of the agreement there.³⁰⁷

This reasoning may apply to substantive crimes as well as inchoate crimes. In *Clements*, for example, the accused were charged with being concerned in the supply of cannabis resin. The evidence was that X travelled from Scotland to England and, while in England, obtained from the accused about 7 kg of cannabis resin which he took back to Scotland. There was no evidence that the accused was in Scotland at any time, but the court was prepared to draw the inference that the accused knew that the drugs would be taken back to Scotland. The Scottish court took jurisdiction on a number of grounds. One of them was that the supply offence continued from England to the ultimate destination in Scotland³⁰⁸.

304 This was not a new notion by any manner of means. The same result and reasoning are to be found in *Brisac* (1803) 4 East 164, 102 ER 792, citing the unreported case of *Bowes* (1787) and *Burdett*, *ibid*. *Brisac* was widely regarded as correct; see, for example, *Connolly and McGreevy* (1894) 1 CCC 468; *Kellow* [1912] VLR 162; and *Hyde* (1912) 225 US 347. For later cases following *Doot*, see, for example, *Borro and Abdullah* [1973] Crim LR 513; *Tarling* (1978) 70 Cr App R 77 discussed in Smith, “Theft, Conspiracy and Jurisdiction: Tarling’s Case” [1979] Crim LR 220; *Sanders* [1984] 1 NZLR 636; *Johnston* [1986] NZLJ 335, [1986] NZRL 394. See also the English Law Commission, *ibid*, at para 95. The holding raises certain detailed difficulties about the limits of the doctrine which are analysed in Goode, *Criminal Conspiracy in Canada* (1975) at 164-167.

305 See also *Simmonds* [1969] 1 QB 685.

306 There is a consistent series of Canadian cases holding that proof of an overt act within the forum is sufficient to found jurisdiction no matter where the agreement was formed and no matter where its eventual objective was to be completed. Examples are *Isbell* (1928) 60 OLR 489; *Lebrique* (1941) 75 CCC 117; *Container Materials Ltd* (1939) 72 CCC 383; (1940) 74 CCC 113; (1941) 75 CCC 117; *Container Materials Ltd* (1939) 72 CCC 383; (1940) 74 CCC 113; (1941) 76 CCC 18; *Howard Smith Paper Mills* (1954) 109 CCC 65; *Cassidy* (1974) 18 CCC (2d) 1. On continuation of the conspiracy generally, see Aronoff, “Acts of Concealment and the Continuation of a Conspiracy” (1983) 17 Ga LR 539.

307 But there now may be no need to show any overt act at all - see *Liangsiripraesert v US Government* [1990] 2 All ER 866 discussed below.

308 [1991] JC 62 at 72-73 (Lord Coulsfield) and 76 (Lord Wylie).

The Protective Theory

Under the protective theory of criminal jurisdiction, the forum has jurisdiction in relation to any conduct engaged in by any person anywhere which conduct is contrary to forum criminal law and threatens the peace, security or good government of the forum. The protective principle comes from the period of radical nationalism which produced the French and American revolutions. It was originally limited to what would today be called “national security crimes”³⁰⁹ but has progressed far beyond that point and is now a major influence on the common law.³¹⁰ The following are some examples of it being applied.

In *Hansford*³¹¹ the accused was charged with fraudulent conversion in South Australia in relation to a maze of dealings involving companies and bank accounts in South Australia and Victoria which seemed somehow to be an attempt to use the money of others to gamble on the price of volatile shares. The court on appeal was hard pressed to disentangle the facts and law in order to determine whether the accused had committed fraudulent conversion - but there was also the question of jurisdiction. The majority fastened on the idea that the South Australian court had jurisdiction because the last act necessary to complete the transaction was the crediting of the bank account of the accused in Adelaide, but that finding is, to say the least, problematic, particularly given the nature of the crime and the facts involved. Wells J cut through the technical analysis, however, by saying:

“The true basis, in my opinion, for the conclusion that acts performed or taking place partly in South Australia and partly outside may be governed by South Australian laws is that it is proper for them to be so governed when they constitute behaviour that affects, and is clearly linked with, the peace, welfare and good government of the State. Where behaviour of that kind is placed before the court the only question that then remains is one of interpretation.

The acts attributed to the defendant in the case at bar plainly, in my opinion, fall within the category of behaviour that poses a threat to the South Australian community.”³¹²

309 See, for example, Garcia Mora, “Criminal Jurisdiction Over Foreigners For Treason And Offences Against The Safety Of The State Committed Upon Foreign Territory” (1958-9) 19 U Pitt LR 567.

310 Examples of its legislative influence may be found in ss 3A and 85E(2) of the Commonwealth *Crimes Act*. The common law influence of the principle is traced in the discussion below.

311 (1974) 8 SASR 164.

312 At 195. See also *McNeilly* (1981) 4 A Crim R 46 where it was held that a NSW court had jurisdiction over a charge of attempted murder where the accused posted a letter bomb in Queensland to an address in NSW. The court found jurisdiction either on the basis that the crime terminated in NSW when the bomb was delivered there as the accused intended or, more straightforwardly, the impact of the crime was to be felt in NSW.

In *Robert Millar (Contractors) Ltd*³¹³ a company and one of its directors were charged with counselling and procuring the causing of six deaths by dangerous driving. The director had required an employee to drive a truck from Scotland to England knowing that the truck had a defective tyre. The tyre exploded and six people were killed in the resulting crash in England. The Court of Appeal held that the forum had jurisdiction despite the fact that the counselling or procuring took place in Scotland in part because the accused had set in train a chain of events which had disastrous effects in England.³¹⁴

*Liangsiripraesert*³¹⁵ was an extradition case which came to the Privy Council on appeal from Hong Kong. For the purposes of this discussion, the question was whether the Hong Kong courts would have had jurisdiction over a charge of conspiracy to traffic in dangerous drugs in Hong Kong against a Thai national where the agreement and all of the performance of the agreement took place in Thailand. In short, this was a *Doot* case except that the accused had not committed any overt act in the territory of the forum at all.

Lord Griffiths for the court held that Hong Kong would have had jurisdiction in such a case. He noted that, apart from isolated dicta, no authority supported the assertion of jurisdiction in such a case - although no authority, it was said (without any justification whatever) militated against asserting jurisdiction in such a case. Lord Griffiths held:

“Unfortunately in this century crime has ceased to be largely local in origin and effect. Crime is now established on an international scale and the common law must face this new reality. Their Lordships can find nothing in precedent, comity or good sense that should inhibit the common law from regarding as justiciable in England inchoate crimes committed abroad which are intended to result in the commission of criminal offences in England.”³¹⁶

The assertion of jurisdiction is avowedly protective in nature, and does not depend on any territorial connection at all.

“If the inchoate crime is aimed at England with the consequent injury to English society, why should the English courts not accept jurisdiction to try it if the authorities can lay hands on the offenders, either because they come within the jurisdiction or through extradition procedures? ...why should an overt act be

313 [1970] 1 All ER 577.

314 Followed in, for example, *Rajalingam Sivaprahasam* [1972] WAR 137; *Smith* [1973] 2 All ER 1167 and *Wall* [1974] 2 All ER 245. These cases concern persons who while overseas are concerned in the importation of drugs into the forum. The reasoning is avowedly protective in nature. The court in *Millar* was also prepared to hold that it had jurisdiction on the alternative ground that the counselling or procuring, having begun in Scotland, continued in England.

315 [1990] 2 All ER 866.

316 At 878.

necessary to found jurisdiction? In the case of a conspiracy in England the crime is complete once the agreement is made and no further overt act need to be [sic] proved as an ingredient of the crime. The only purpose of looking for an overt act in England in the case of a conspiracy entered into abroad can be to establish the link between the conspiracy and England or possibly to show the conspiracy is continuing. But if this can be established by other evidence, for example the taping of conversations between the conspirators showing a firm agreement to commit the crime at some future date, it defeats the preventative purpose of the crime of conspiracy to have to wait until some overt act is performed in pursuance of [sic] the conspiracy.”³¹⁷

This piece of judicial advocacy has been applied enthusiastically to drug³¹⁸ and terrorism³¹⁹ offences.

Modern General Theories Of Jurisdiction

In light of the failure of the territorial principle and law to deal with the problems of criminal jurisdiction, there have been various attempts to fashion a new set of general rules.

‘Result-Crimes’ and ‘Conduct Crimes’

On a number of occasions, Lord Diplock reached jurisdictional conclusions on the basis of the territorial principle (or something which closely resembles it) by classifying offences as ‘result-crimes’ or ‘conduct-crimes’ and applying consequential locational reasoning.³²⁰ The *exact* distinction between the two types of offence is not precisely clear, but the general idea is simple. Some crimes concentrate on the results achieved by the conduct of the accused, and in that case the location of the result, actual or intended, is crucial³²¹. ‘Conduct crimes’ take place where the conduct happens; ‘result crimes’ take place where the result happens. These labels and the analysis have been employed in a significant number of subsequent cases.³²²

Despite the fact that these labels have proved attractive to some judicial minds, this sort of analysis hinders more than it helps. It should be avoided. It is an embroidery on the “gist of the offence analysis” - the gist is either the conduct

317 At 877-878.

318 Notably in *Fan* [1991] 24 NSWLR 60; *Clements* [1991] JC 62; *Sansom, Williams, Smith and Wilkins* [1991] 2 WLR 366 and *Winfield and Lipohar* (2000) 168 ALR 8.

319 Notably in *Ellis v O’Dea* [1991] IR 251.

320 See, for example, *Stonehouse*, [1978] AC 55; *Treacy*, [1971] AC 537; *Wiggins* [1980] 2 All ER 593 and *Markus* [1975] 1 All ER 958.

321 As noted immediately above, for example, Lord Diplock was of the view that obtaining by false pretences is a ‘result-crime’ and hence the location of the result - obtaining - is crucial.

322 Aside from subsequent English decisions, recent examples are *Clements* [1991] JC 62 at 73; *Brownlie v SPCC* (1992) 27 NSWLR 78 at 83; *Toubya* [1993] 1 VR 226 at 234.

or the result of the conduct - but it replaces with a simplistic label what should be an explicit interpretation of the purpose of the offence which proper “gist” analysis requires. Put another way, the label attached to an offence (“conduct” or “result”) serves only to hide an analysis of the legislative intention in creating the offence. It may well be that, for example, obtaining by false pretences is a result-crime - but that label avoids the central question, which is why the courts take the view that the element of obtaining is more important in terms of legislative intent than the element of telling a lie.³²³ The legislature may have attached equal abhorrence to both the conduct and its result. Even if it did not, it may be impossible to tell which element was uppermost in the legislative mind. Is the offence of carrying an animal in such a way as to cause it injury or unnecessary suffering a ‘result crime’ or a ‘conduct crime’? Lord Diplock thought the latter.³²⁴ But an equally persuasive case can be made for the former.

Further, the reasoning is inverted from that which is correct. Primary attention in recent times has been on a movement to the protection of the interests of the forum and the attraction of the imposition of the criminal sanction by the taking of jurisdiction where those interests are threatened. It may well be that the public interests of the forum are threatened by the fact that the result of the crime - or its intended result - will occur in the forum and *therefore* the location of the result is crucial - but simply because the crime is formulated by the legislature as punishing a result does not necessarily mean that such a conclusion is inevitable.

The unreasoned labelling of offences as ‘conduct crimes’ or ‘result crimes’ has no rational foundation in jurisdictional analysis and should be abandoned.

‘Terminatory’ and ‘Initiatory’ Theory

In 1965, Glanville Williams wrote an influential analysis of the way in which the common law had reacted to jurisdiction and venue problems.³²⁵ He distinguished between the “terminatory theory” and the “initiatory” theory of criminal jurisdiction. According to the terminatory theory, the crime is committed where the crime is completed, that is, where the last act necessary to constitute the offence occurs. According to the initiatory theory, the crime is committed where the offender acts to set the crime in train.

323 The English Law Commission takes the more moderate line that, while the distinction is “difficult and controversial”, it is useful for some crimes, such as obtaining by false pretences, “which fit easily into the pattern of conduct on the part of the accused followed by a defined result of that conduct.” Law Commission, “Criminal Law: Jurisdiction Over Offences of Fraud and Dishonesty With A Foreign Element, Report No 180 (1989) at para 2.2n4. The Commission has not thought that concession through.

324 *Air India v Wiggins* [1980] 1 WLR 815.

325 “The Venue and Ambit Of The Criminal Law” (1965) 81 LQR 518.

The terminatory theory is based on the idea that the purpose of the criminal law is to protect the public and the individual. The initiatory theory is based on the idea that the purpose of the criminal law is to regulate or deter behaviour. Glanville Williams argued that the general trend of the common law had been to adopt the terminatory theory, but that the initiatory theory was the better of the two.

In fact, however, the common law has not followed any one theory consistently but has adopted the most convenient analysis of the facts and the law in each individual case.³²⁶ Although there is still an emphasis on the terminatory view of the crime, this is being transformed into an examination, not of the place where the crime is complete, but of the location in which the criminal behaviour impacts.³²⁷ Those two locations may be the same - but need not be. Glanville Williams' analysis is, therefore, of limited value.

Lord Diplock and Comity

In concurring with the majority in *Treacy*.³²⁸ Lord Diplock suggested a theory of criminal jurisdiction which, when applied to the facts in that case, supported the conclusion that the English forum had jurisdiction over the blackmail. It will be recalled that the case involved a demand with menaces posted in England to an intended victim in Germany. His theory may be summarised as follows:

- (a) a sovereign Parliament, subject to the rules of its own constitution, has the theoretical power to make it an offence for anyone to do anything anywhere. It does not do so. Instead, it limits the application of its legislation, not only because it would be futile to make it an offence for French people to drink French wine in France, for example, but also because of principles based on international comity that are designed to prevent one sovereign from unreasonably interfering with the sovereignty of another;
- (b) there is nothing in these principles of international comity to prevent Parliament from making or intending to make it an offence to do something in its territorial jurisdiction having harmful effects elsewhere because people within the territory owe allegiance to local law and must conduct themselves in conformity with it. Equally, there is nothing in the principles of international comity to prevent Parliament from making or intending to make it an offence for persons located outside its territorial jurisdiction from doing something which has harmful effects within the jurisdiction;

326 See also Law "The Extra-Territorial Criminal Jurisdiction of English Courts" (1978) 27 ICLQ 168.

327 See generally Katzenbach, "Conflicts On An Unruly Horse: Reciprocal Claims And Tolerances In Interstate And International Law" (1956) 65 Yale LJ 1087 at 1141-1142 and Hanbury, "Territorial Limits of Criminal Jurisdiction" (1952) 37 Grotius Soc 171 at 172-173.

328 [1971] AC 537.

(c) consequently:

“...the rules of international comity...do not call for more than that each sovereign state should refrain from punishing persons for their conduct within the territory of another sovereign state where that conduct has no harmful consequences within the territory of the state which imposes the punishment. ...where the definition of any such offence contains a requirement that the described conduct of the accused should be followed by described consequences, the implied exclusion is limited to cases where neither the conduct nor its harmful consequences took place within the jurisdiction.”³²⁹

This analysis has much to commend it in terms of the reality of legislative power and intentions and the results that the courts want to reach. It has, however, not been explicitly employed as a principal method for achieving a result in any particular case since it was formulated.³³⁰

La Forest J and Real and Substantial Link

In *Libman*³³¹ the accused was charged in Canada with fraud and with conspiracy to defraud in relation to a telephone solicitation scheme. The accused directed the telephoning from Canada of residents of the United States to invite them to invest in South American companies. The money was sent to various South American countries. The accused went to those places, collected the money, and returned with it to Canada.³³²

La Forest J delivered the judgment of a unanimous Supreme Court of Canada. Having surveyed the English and Canadian authorities at length, he held that the Canadian courts had jurisdiction. In doing so, he discarded the approaches based on the territorial principle. Instead, borrowing from Lord Diplock, he created a new approach to the question of criminal jurisdiction. His judgment may be summarised as follows:

- (a) the English and Canadian courts began with the strict territorial theory based on locating the crime in the place in which the crime was completed, but soon found it necessary to devise a series of reasons or devices, not entirely consistent with each other, to avoid the perceived undesirable consequence of freeing an accused on an unmeritorious technicality;

³²⁹ At 564.

³³⁰ Lanham, *Cross-Border Criminal Law* (1997) at 39-44 contains a more detailed discussion of what the comity limitation may entail. Although the English Court of Appeal appears to have been greatly influenced by the theory of comity in *Smith* [1996] 2 Cr App R 1, it precipitously and explicitly refused to follow either *Smith* or the theory in *Manning* [1999] 2 WLR 430. It may be that *Libman* (below) can be regarded as another variation on the comity theory.

³³¹ (1985) 21 CCC (3d) 206.

³³² It should be noted that the Canadian *Criminal Code* contains legislative provisions designed to widen the jurisdiction of Canadian courts over Canadian based conspiracies.

- (b) the law on the subject has acquired an air of unreality and is characterised by such anomalies as the decision in *Harden*³³³ which shows that it is possible for a clever international criminal can so arrange his or her affairs as to manipulate criminal jurisdiction if a strict territorialist view is taken;
- (c) the instant case was also a good example of a possible anomaly. To say that the gist of the offence of fraud is the obtaining smacks of unreality because not only the obtaining, but also the fraud must be proved. The scheme involved the enjoyment of the fruits of the crime in Canada. The law would certainly be an ass if it could be avoided by the simple expedient of persuading the victims to send their money to another country where it could be “obtained” by the accused;
- (d) a Canadian court has jurisdiction over a crime if “a significant portion of the activities constituting the offence took place in Canada” or there is “a real and substantial link between the offence and the country”.³³⁴ The only significant limitation on this is the doctrine of comity,³³⁵ and that is certainly not infringed if Canadian courts convict those of their citizens who prey on neighbouring residents. In short:

“In a shrinking world, we are all our brothers’ keepers. In the criminal arena this is underlined by the international schemes that have been developed among national law enforcement authorities”.³³⁶

There is much to be said for this robust common-sense way of approaching the question of criminal jurisdiction. As La Forest J pointed out: “[This] is in fact the test that best reconciles all the cases. The only ones that do not fall within it are *Harden* and *R v Brixton Prison Governor, ex parte Rush* which, in my view, should no longer be followed”.³³⁷

333 [1963] 1 QB 8.

334 At 232, followed in *Douglas* (1989) 51 CCC(3d) 129, a conspiracy charge which ordinarily may have run foul of the rule in *Owen* if charged at common law. See also the similar attitude in *Laird v HM Advocate* [1985] JC 37.

335 pace Lord Diplock in *Treacy*.

336 At 233.

337 At 232. *Harden* is discussed above. *Ex parte Rush* [1969] 1 All ER 316 was an extradition case in which the accused sent letters and circulars from Canada to the United States inviting the recipients to purchase shares. The purchase money was sent to Panama and Nassau but eventually reached Canada by one route or another. The question for the English court is whether a Canadian forum would have jurisdiction. It held that it would not. The court held that the gist of the offence was the obtaining and that the money was obtained either when and where it was posted in the United States or when and where it was received in Nassau or Panama. Rush was later convicted in Canada of receiving stolen money: *Rush* [1970] 2 CCC 29.

The approach advocated by *Libman* has not found favour elsewhere. Indeed, Australian courts have recently gone to considerable lengths to avoid its application.³³⁸

Professor Lanham's Policy Considerations

In a recent book, Professor Lanham has suggested that the law in this area should be guided by nine "policy considerations". They are:

- There should be no legal vacuum;
- Defendants should not be held liable in one place for obedience to the law in another;
- Penalties should not exceed those under the most appropriate law;
- Defences under the most appropriate law should be available wherever the defendant is tried;
- Appropriate evidence must be accessible;
- International sensitivities should be respected;
- Prosecutorial resources should be appropriately deployed;
- Criminal trials should not be unduly complicated;
- Defendants should not be punished twice for the same offence.³³⁹

The core of these principles is Professor Lanham's notion of "the most (or the substantially) appropriate court/law". Professor Lanham suggests that: "the place where the harm occurs or is intended has a better right to try than the place where the act causing the harm is performed."³⁴⁰ Of the principles listed above, principles 1, 2, 5, 6, 7, and 8 are very much the same as some of the factors that courts consider when determining the convenient forum for the purposes of civil litigation. These concepts require further exploration. That detail is beyond the scope of this Discussion Paper.³⁴¹

Of the others, principles 3 and 4 represent types of choice of law rule. Considered generally, it appears that there is little to differentiate Professor Lanham's proposals from the more precise formulation suggested in *Libman*. Both appeal to a general factor based test based on "significant relationship" (*Libman*) or "appropriate law" (Lanham).

338 See, for example, the convoluted reasoning in *Isaac* (1996) 87 A Crim R 513.

339 Lanham, *Cross-Border Criminal Law* (1997) at 16.

340 Lanham, *Cross-Border Criminal Law* (1997) at 17.

341 For further exploration of the concept see M Goode, "The Tortured Tale of Criminal Jurisdiction" (1997) 21 Melb ULR 411.

But a word of caution is appropriate. In the area of tort law, significant emphasis has been placed upon application of the law of the place of the tort³⁴², and there is a significant pressure to make this the primary choice of law rule in Australia. Systems of law placing significance on the law of the place of the tort are characterised by manipulation and evasive legal techniques to avoid the result of the application of the law of the place where the tort was committed (whatever that may mean) because it gives rise to anomalous and/or unjust results.³⁴³ It has been demonstrated above that a similar rule has produced the same or similar results in the area of criminal jurisdiction (effectively criminal choice of law). In the area of torts, this led to the generation of a vast amount of legal scholarship and a great deal of judicial anguish about replacing the territorial rule with a more flexible rule or approach based on “significant relationship” or some other general approach.³⁴⁴ This movement has been stoutly resisted in Australia largely because it will lead to “uncertainty”.³⁴⁵ Without passing comment on the obvious incongruity of such a claim, there can be little doubt that any proposal to adopt overtly more flexible approach to criminal jurisdiction/choice of law will meet with the same response, no doubt with similar effect. This may explain the reluctance of courts to abandon the cloak of territorialism, despite evasive reasoning which, to say the least, brings territorialism into disrepute, and it may also explain the Australian reluctance to embrace the kind of reasoning employed in *Libman*.

342 In the United States, the rule was exclusively based on the *lex loci delicti* until the 1950s. The literature on what happened then is vast and it would be foolish to attempt even a representative sampling in this note. In Australia, the rule in *Phillips v Eyre* (1870) LR 6 QB 1 prevailed without question until *Breavington v Godleman* (1989) 169 CLR 41 in which the High Court failed to achieve a coherent majority on any question, including the survival of *Phillips v Eyre* vs a return to the law of the place of the tort or some variation on it, but *Phillips v Eyre* prevailed in some form by later decision: *McKain v RW Miller(SA) Pty Ltd* (1992) 174 CLR 1; *Stevens v Head* (1993) 67 ALJR 343. The rule in *Phillips v Eyre*, and its variations, gives a flexible role to both the law of the forum and the law of the place of the tort. That role depends entirely on interpretation. See, for example, Goode, “Dancing on the Grave of *Phillips v Eyre*” (1984) 9 Adelaide LR 345.

343 For a summary of the United States experience, see, for example, O’Toole, “The Place of the Wrong Rule: ‘An Unrepealed Remnant of a Bygone Age, A Drag on the Coattails of Civilization?’” (1978) 13 New England LR 613.

344 The “most significant relationship” was introduced by the Second Restatement, Proposed Official Draft, 1968 r 145. See Reese, “Conflict of Laws and the Restatement Second” (1963) 28 Law & Contemp Prob 679. There is a very large number of alternative approaches and/or rules in the academic literature and a number have been adopted by American courts. A “flexible exception” (based on a version of the Second Restatement) to the law of the place of the tort factor in the rule in *Phillips v Eyre* was given authoritative status in *Chaplin v Boys* [1971] AC 356 but has had a chequered career in the case law since that time, and has failed to command majority support in the High Court.

345 See, generally, Australian Law Reform Commission, Report No 58, *Choice of Law* (1992).

Statutory Intervention On A National Basis

South Australia, New South Wales, the Australian Capital Territory and Tasmania have enacted a criminal jurisdiction statute recommended by the Standing Committee of Solicitors-General and adopted by the Standing Committee of Attorneys-General after and as a result of the High Court decision in *Thompson*³⁴⁶. As an example, section 5C of the South Australian *Criminal Law Consolidation Act* says, in material part:

- “(1) An offence against the law of the State is committed if -
 - (a) all elements necessary to constitute the offence (disregarding territorial considerations) exist; and
 - (b) a territorial nexus exists between the State and at least one element of the offence.
- (2) A territorial nexus exists between the State and an element of an offence if -
 - (a) the element is or includes an event occurring in the State; or
 - (b) the element is or includes an event that occurs outside the State but while the person alleged to have committed the offence is in the State.”.

Subsection (3) contains a presumption that the territorial nexus is satisfied unless rebutted under ss (4). Subsection 4 requires that the trial proceed in any event and that the question of territorial nexus be decided at the end of the trial.

It was and is plain that the real offence in *Catanzariti* (conspiracy in South Australia against South Australian law to cultivate cannabis in the Northern Territory) was caught by s5C. Nevertheless, Matheson J ruled to the contrary:

“In my opinion, s5C is not an offence creating section. It is only concerned with the determination of whether a South Australian offence has been committed. It does not extend the jurisdiction of this court to include offences against the law of another country, or even, and more relevantly of another State or Territory of the Commonwealth of Australia. The word “offence” must mean a South Australian offence. Section 5C does not purport to recognise the laws of the Northern Territory or of anywhere else.”³⁴⁷

346 (1989) 169 CLR 1, (1989) 63 ALJR 447. The statutes are: SA *Criminal Law Consolidation Act* s 5C; NSW *Crimes (Application of Criminal Law) Amendment Act*, 1992; ACT *Crimes (Amendment) Act*, 1995; Tas *Criminal Law (Territorial Application) Act*, 1995.

347 (1996) 65 SASR 201 at 215.

It should be noted that while it is argued that this ruling is incorrect, the result was correct. The prosecution charged a conspiracy to breach the law of the *Northern Territory*. It is clear (with some very limited exceptions of no relevance here) that courts apply the substantive law of their own jurisdiction and cannot apply the substantive law of another. However, had the correct offence been charged, the result should have been a finding of jurisdiction. Conspiracy to produce or cultivate cannabis is a South Australian offence. The facts of this case are plainly and obviously caught by the operative subsections. Section 5C was intended to catch such cases as this - and does so.³⁴⁸

It is, in addition, quite unclear what is meant by the phrase “offence creating section”. Matheson J probably meant that s5C is not to be interpreted to create a criminal offence where there was none before. But that can have two meanings. Certainly, in a first meaning, s5C was not intended to enact a new criminal offence in the sense that, for example, the recent Parliamentary enactment of “stalking” offences creates new offences. But in its second meaning, s5C was intended to create criminal liability where there was none before because it was intended to remove “jurisdictional” obstacles to the prosecution and, if appropriate, conviction of offences which may not have been possible in the past. Conspiracy to cultivate cannabis has been an offence for quite some time and s5C (and its equivalents) do not create it. They may create a new *liability* - not a new offence. These two meanings are quite different and it is, with respect, at best unhelpful to confuse them.

Hunt CJ in *Isaac* held that the New South Wales equivalent did not catch those accused either:

“In the present case, the agreement to commit the robbery in the Australian Capital Territory existed, and all of the events necessary to establish that agreement occurred within this State. There was no event which occurred outside this State to which s3A could apply. Even the intention to carry out the robbery (which, as a state of mind, is excluded from the definition of an event) existed in this State. Insofar as the appellants still held that intention when they travelled to Canberra, again that intention does not amount to an event as defined) which occurred outside the State. If the agreement formed inside this State to commit a crime in the Australian Capital Territory did not constitute an offence known to the law of this State (as *Board of Trade v Owen* says that it does not), then s3A did not constitute it an offence against the law of this State simply because the object of the agreement or

³⁴⁸ Section 5C was also referred to by Lander J in *Winfield, Chandler and Lipohar* (1995) 83 A Crim R 301 but that was a standard case of a conspiracy outside the forum to commit a fraud inside the forum and could be resolved, with ease, without reference to statute. Lander J left open the proper construction of s 5C but was inclined to agree with *Catanzariti*. For the decision on appeal, see (2000) 168 ALR 8.

conspiracy involved the commission of a crime in another State or Territory of the Commonwealth. Section 3A is irrelevant to the present case.”³⁴⁹

This reasoning defies rational analysis. The crime in question is so tied to New South Wales, it is said, that a statute, manifestly intended to extend the “jurisdiction” of the New South Wales courts, cannot apply to it. For common law purposes, it is said, the offence charged is a crime in the Australian Capital Territory. For statute purposes it is a crime in New South Wales! Neither suffices for conviction.

The reasoning involved is fallacious. The statute applies to the case on its plain words. There is *nothing* in s3A which requires that an “event” take place *outside* the State.

The result and reasoning in these decisions are untenable. The accused in *Catanzariti* will, presumably, be taken via the *Service and Execution of Process Act* to the Northern Territory, and tried there. What of the accused in *Isaac*? Again, one might presume that the law involved in such decisions in *Doot*³⁵⁰ make the New South Wales conspiracy “justiciable” in the Australian Capital Territory. One could be excused for thinking that in a nation such as Australia, prohibiting the prosecution of two such commonplace offences in one component of the federation and therefore requiring prosecution in another serves no rational purpose of the criminal justice system or, in general terms, the public interest.

*Winfield and Lipohar*³⁵¹ concerned the reverse conspiracy allegation. The accused were charged in South Australia with conspiring in Queensland or Victoria to defraud a business carried on in Victoria with a registered office in South Australia. The only “overt act” pursuant to the conspiracy which involved South Australia was a fax sent from Victoria to South Australia in which the appellants sent a forged letter promising a promissory note in security on behalf of a fictitious client. However, the essence of the charge was that the accused conspired to obtain the \$6.5m involved from a South Australian company (ultimately, the South Australian government).

This was a standard *Doot/Liangsiriprasert* fact pattern. And indeed, after a very thorough examination of the authorities, the Court of Criminal Appeal so found. In essence, all three members of the Court held that South Australia had jurisdiction either (a) because the conspiracy was aimed at defrauding a South Australian victim and causing a loss in South Australia and was therefore

349 (1996) 87 A Crim R 513 at 525. *Isaac* was followed by the NSW District Court in *Fernando*, 1/11/98, a case of conspiracy in NSW to commit robbery in Queensland. The court expressed a degree of frustration at having to decline to proceed against the alleged offender.

350 [1973] AC 807.

351 (1997) 97 A Crim R 482 and (2000) 168 ALR 8.

a threat to the Queen's peace in South Australia; and/or (b) the transmission of the fax from Victoria to South Australia was an overt act within South Australia sufficient to found jurisdiction over the interstate agreement. To so hold is, it is submitted, unremarkable on the authorities.

On further appeal to the High Court, there was a lack of unanimity about a number of issues. It can be said with confidence that Gleeson CJ, Gaudron, Gummow, Hayne and Callinan JJ agreed that the appeal should be dismissed. Kirby J was the sole dissident. Gleeson CJ delivered a single judgment as did Callinan J. So too Kirby J. Gaudron, Gummow and Hayne JJ delivered a joint judgment. The grounds in all judgments are different. There is therefore no coherent majority opinion on the substantial issues of the case.

The judgments can be summarised as follows.

1. Gleeson CJ held that the conspiracy to defraud was of such a nature that its implementation involved deceiving people in South Australia and inducing them to act to their detriment. It was, for that reason, punishable according to the law of that State.
2. Gaudron, Gummow and Hayne JJ held that the relevant question was whether the connection between the subject matter of the charge and South Australia was sufficient. That is a search for the sufficiency of connecting factors in the context of the question whether a particular Australian court has jurisdiction to try an offence against the common law of Australia. The requirement of nexus should be liberally applied and a real connection with the jurisdiction should suffice. In this case, the persons to be deceived were in South Australia and it would be artificial to ignore the commercial realities and the real and practical consequences for the ultimate victims, including the South Australian body politic. A connection of that character will suffice.
3. Callinan J held that an offence should be regarded as having been committed against the law of a State or Territory if a conspiracy has been entered into anywhere which has a real link with the jurisdiction. A number of sufficient "real links" existed in this case.
4. Kirby J (dissenting) agreed with Gaudron, Gummow and Hayne JJ about the nature of the common law in Australia, but, centrally, held that he would not be prepared to hold that a crime completed in one Australian jurisdiction should be deemed by fiction to be completed also in another jurisdiction and that therefore the requirement of territoriality should prevail particularly since the finding of jurisdiction in South Australia should properly be seen as the creation of a new offence against South Australian law.

The three judges who delivered the joint judgment (Gaudron, Gummow and Hayne JJ) thought that this case (and the general issue) was about the underlying unity of the common law in Australia. This construction of the problems in the area does not appear to have occurred to anyone else before. Kirby J decided to address that issue and in general agreed with what the three said, albeit not with the result that they derived. So there is a majority on that point. This is discussed further below. Callinan J dissented about this point and Gleeson CJ dealt with it very shortly.

On the other hand, the judgments of Gleeson CJ and Callinan J are really about criminal jurisdiction as it has been conceived traditionally and outlined above. Kirby J also deals with these issues but dissents as to the result. The joint judgment considers these issues but cannot be said to be firm about it.

Considered as a matter of straightforward criminal jurisdiction, as these cases have been decided in the past, the individual judgments of Gleeson CJ, Callinan J and Kirby J can be considered as a group. The joint judgment, on the other hand, arrives at a general principle but by a greatly divergent reasoning process.

Gleeson CJ began with the traditional statements of the territorial theory, and rationalised the scores of twists and turns which avoid it as “considerations of pragmatism ... [being] more influential than a desire for theoretical symmetry”. Having decided for pragmatism, he applies the following rule:

“When the appellants and their co-conspirators set out to defraud the company.... Geographical considerations ... were probably largely unimportant to them. Even so, as a matter of objective fact, there was a real connection between the conspiracy and South Australia. The intended victim of the fraud was a South Australian company, whose business was controlled from that State and in the way in which the affairs of that company were managed, the effectuation of the fraud involved the making of a false representation to people in South Australia, and their acting on that representation. ... The conspiracy to defraud was of such a nature that its implementation involved deceiving people in South Australia and inducing them to act to their detriment. It was, for that reason, punishable according to the law of that State.”³⁵².

The test ultimately applied, albeit to an undefined class of exceptions to the general common law single situs rule, is a test of “real connection”. The test is an objective one. It is not about what the accused knew, intended or believed about the place of real connection - it is what “as a matter of objective fact” the real connection is.

352 (2000) 168 ALR 8 at 17.

Callinan J also concluded that South Australia could try the accused. His Honour was principally concerned to debate the question whether there is a single Australian common law (His Honour thought not, and is in a minority on this issue). In relation to the question of jurisdiction, His Honour cited *Doot*³⁵³ and *Libman*³⁵⁴ for the proposition that there are really no generally accepted rules or principles in this area of law. He then quoted extensively from *Hyde v US*³⁵⁵, and held:

“In my opinion, having regard to the exceptional nature of a conspiracy and the authorities to which I have referred, it is proper to take the view that an offence should be regarded as having been committed against the law of South Australia if a conspiracy has been entered into anywhere which has a real link with the jurisdiction. ... In this case, a relevant state of affairs existed, to provide real links in these respects: the transmission of the facsimile to South Australia as an act done in partial implementation of the conspiracy; the consideration given by the board and solicitors of Collins St in South Australia to the transaction generally and the fraudulent representations made in furtherance of the conspiracy; and the fact that the victim, the party directly affected, Collins, St, was a South Australian corporation with its registered office in South Australia. Any one of these circumstances was sufficient in this case to provide a real link... and to ground jurisdiction...”³⁵⁶.

This is more or less the general test proposed in *Libman* (“real and substantial link”) but confined to the “exceptional” case of conspiracy. There appears to be no connection with *Hyde* at all, except in the broadest policy sense.

But the argument about jurisdiction (or power to hear the case) commended itself to Kirby J. His Honour is not noted for the espousal of dry technicalities at the expense of the justice of the case. Why did he decide against “jurisdiction”?

His Honour considered, and rejected, strict territorial theory, treating conspiracy as an exception, basing jurisdiction on the presence or residence of the victim, the use of “the common law of Australia” and the test of “real and substantial connection”. He rejected them all, giving detailed reasons which will not be traversed here. But the centre of his decision can be presented as follows:

“An accused who stands at risk of trial - and hence of conviction and punishment - is entitled to demand of the law that the conduct

353 [1973] AC 807.

354 [1985] 2 SCR 178.

355 (1912) 225 US 347.

356 (2000) 168 ALR 8 at 84.

which will which will expose him or her to such a risk will be specified in advance. It should not depend on subsequent decisions, whether of a judge or of a jury. ... it is necessary for the forum which asserts such jurisdiction to establish that such an offence against its laws *does* exist. This, as it seems to me, is the fatal flaw in the Crown's case against the appellants. The Crown cannot establish that the appellant's alleged conspiracy was an offence against the law of South Australia by invoking s 5C of the Criminal Law Consolidation Act. It does not contend that the Constitution comes to its aid. It is therefore driven to an appeal to novel common law concepts never previously established as part of Australian law. The Crown's argument necessitates the effective creation by the courts of a new offence against the law of South Australia. The proved conduct of the appellants certainly appears to have established an offence against the laws of another Australian jurisdiction. But not South Australia. ... What is the law of South Australia creating the offence in that State which the appellants have breached? No one claims it is the Constitution. Certainly, it was not statute law. To hold that it is the common law is to indulge in judicial invention. None of the three or four suggested connectors to South Australia, trivial or irrelevant as they are, would warrant such a leap of creative faith."³⁵⁷

The point being made is that the conflicts choice of law rule applying the substantive offence is a law *creating* the offence and hence the liability to it. The Committee has a different view.

Substantive laws which govern the behaviour of individuals and corporations are found in the common law and in statute law. They are, to labour the point, substantive in nature, especially those derived from common law³⁵⁸. They say that one must do this or one must not do that and, if one breaks the rule, one suffers in a variety of ways. This is true of criminal law and civil law (whatever the exact line of demarcation, which may be disputed, but there are, inevitably, overlaps). These laws are *created* by either judicial decision or Parliamentary decree. The point is that in no way are laws *created* by the territorial reach of the source of the rule. The territorial source of the rule merely deals with their sphere of *application*. Choice of law rules deal with the sphere of application of the rule in question. Choice of law rules do not *create* substantive rules of

357 (2000) 168 ALR 8 at 65 (emphasis in the original).

358 Some statutes contain provisions which are purely jurisdictional and which, therefore, attempt to set out the range of operation of their substantive provisions - which may include offences. Given that forum law almost always applies to criminal charges, these therefore operate as choice of law rules where criminal offences are involved. See, for example, s 14 of the *Fair Trading Act* (SA), which is a quite complex rule about the sphere of operation of the Act and hence also the offences contained within it.

behaviour or criminal offences. They merely define the spatial limits within which the substantive rules operate.

In the case of the criminal law, the choice of law rule is simple. It is to apply the law of the forum³⁵⁹. The question that then must be asked of Kirby J is this. What is the injustice in principle and, in particular, in his articulated principles, in applying the law of South Australia to these appellants? Kirby, J would say that on the state of the present law that it was unjust because the accused did not know in advance which law applied. However, conspiracy to defraud was and remains an offence in all jurisdictions.³⁶⁰ He also asserted that none of the “connectors” to South Australia sufficed to warrant judicial invention of a common law *rule of application*.

Gaudron, Gummow and Hayne JJ delivered a joint judgment in which they concluded that the South Australian court had jurisdiction. Their starting point was a finding that the offence of conspiracy to defraud was (and remains) an offence at common law in South Australia, and that therefore, to say that the offence was an offence against the law of South Australia provides “a false starting point for analysis”³⁶¹. The point, generally speaking, is that their Honours hold that there is but a single Australian common law³⁶² and therefore, what was alleged in this case was an offence against the common law of Australia³⁶³. It is not intended to enter into that difficult and complex constitutional debate here, beyond remarking its central influence on the reasoning in this judgment. The point for present purposes is that, for their Honours, the question then became a *constitutional* one: where a court is faced with a charge that the accused offended against the common law of Australia, must there be demonstrated any kind of link between the alleged offences and the forum state and, if so, what kind of link? This is a question, not of “jurisdiction”, but of venue³⁶⁴. (For that purpose, their Honours assumed that the crime was a domestic Australian one and not an international one³⁶⁵.)

359 There are very few and possible exceptions to this rule: see Goode, “The Tortured Tale of Criminal Jurisdiction” (1997) 21 MULR 411.

360 See further at (2000) 168 ALR 65-66.

361 (2000) 168 ALR 8 at 18.

362 Callinan J disagreed with this proposition. Gleeson CJ simply failed to refer to it. Kirby J discussed it but held that insofar as the proposition could be defended, it did not go so far as the joint judgment proposed. The court is therefore split evenly on the precise point, although it might be inferred that McHugh J will agree with the joint judgment. See the next footnote.

363 Citing, at least in the first instance, the decision of McHugh J in *Kable* (1996) 189 CLR 51.

364 As their Honours point out with great clarity at (2000) ALR 8 at 28, “jurisdiction” is a term used for a variety of purposes, not often identified with precision. But it does usually signify the limits of power. “Venue” concedes power, but is about whether it should be exercised or not. “. . . venue is concerned with the place of trial while “jurisdiction” is aptly used here to identify the existence of authority to adjudicate a particular dispute.”. (2000) 168 ALR 8 at 29. Venue and jurisdiction in this area of law were confused in the early decision in *Brisac* (1803) 102 ER 792. They are also confused in the joint judgment. Their Honours lapse into the language of jurisdiction later: (2000) 168 ALR 8 at 40 [para 114].

365 (2000) 168 ALR 8 at 39.

Nevertheless, no matter the method or reasoning used to get to the conclusion, the joint judgment reaches the same point as the rest of the majority. The following extracts illustrate the point:

“The constraint upon State legislative power identified in *Union Steamship* by reference to limitations expressed or implied in the Constitution applies where the criminal offence is created by statute of the State in which the trial takes place. It does so immediately by operating upon the territorial reach of the offence specified by the statute. Where, as in the present case, the offence is not created by statute, the constraint applies but by reference to the statute which specifies the jurisdiction of the State court in question. Here this is found in... the Supreme Court Act... In the present case, the question becomes whether the connection between the subject matter of the charge and South Australia was sufficient. That is a search for the sufficiency of connecting factors. ... The requirements of nexus should be liberally applied. A real connection with the jurisdiction will suffice.”³⁶⁶

Their Honours went on to hold that the act of sending the fax to South Australia, considered together with the fact that the intended victim was a South Australian corporation and thence the South Australian body politic sufficed.

It is interesting to note that, despite the fact that Gleeson CJ, Callinan J and Gaudron, Gummow and Hayne JJ employed radically different reasoning, the result of their reasoning is the same. It is that (a) the test is whether or not there is a “real connection” between the offence and the State or Territory in which it is sought to try the accused; and (b) that there was a connection in this case; because (c) the accused had sent a false representation to South Australia and the victims were a South Australian company and, ultimately, the South Australian taxpayer.

366 (2000) 168 ALR 41-42 (emphasis added). The citation of *Union Steamship* is (1988) 166 CLR 1 at 14. It says that “a remote and general connection” between the State and the elements of the statutory offence will suffice for validity of a State law. At the risk of entering a debate disavowed in the text above, it might be noted that there is a partially unresolved tension between the notion, promoted by the joint judgment, that Australia can no longer be seen in common law terms except as a unitary common law area, and the idea that for legislative purposes, State Parliaments bear territorial constitutional restrictions that have evolved for their status as colonial legislatures, however much wider power has been given to them since the days before the *Australia Act* 1986. It seems that they cannot be regarded as individual sovereigns [see (2000) 168 ALR 8 at 40], and the notion that the restraints upon the power of a given law area in relation to an offence alleged against the Australian common law is subject to the same restraints as that imposed by the Constitution [s 77(ii)] upon the exercise of legislative power. But how can their expanded legislative powers be reconciled against this new notion of a unified common law and some form of evolving yet diminished sovereign status for jurisdictional purposes? See, generally, Mohinsky “State Extraterritorial Laws and the Australia Acts 1986” (1987) 61 ALJ 779.

This is, it is submitted, the right result, if only on the basis that it cannot be argued (and, so far as one can tell from the reports, was not argued) that there was *any* injustice or unfairness at all in trying the accused for the offences alleged in a South Australian court. The whole legal argument was and remains dry technicality. The sooner these problems are addressed the better.

It may be noted that s 5C did not have any influence in the reasons for judgment of the majority. Callinan J analysed the provision in any detail, concluding that it could not apply to the facts of the case. Kirby J, also analysed the provision in dissent, concluding it was unjust because the accused did not know in advance what law applied, calling s 5C an “imperfect provision”. This latter comment reinforces the need for the reforms advocated by the Committee in this Report.

In *Question of Law Reserved (No 4 of 1997)*³⁶⁷, the accused were charged with taking part in the sale of cannabis. The case for the prosecution was that the accused purchased and packaged cannabis in South Australia so that it could be transported to New South Wales and sold there. It was argued that the South Australian court had no jurisdiction because the sale was to take place out of the State. Doyle CJ, for the court, rejected the argument. He decided that, since previous authority had made it clear that the offence of taking part in a sale could be committed whether or not there was a sale³⁶⁸ the location of the sale was not a determinative event. A principal reason for this conclusion was, as in other drug cases, the notion that “[t]he effective enforcement of the Act would be significantly weakened”³⁶⁹ were it otherwise.

Doyle CJ found it unnecessary to make any decision about s5C. He merely made the ambiguous remark that: “It is clear that although s5C does not create new offences, it extends the application of the laws of South Australia to situations to which they would not otherwise apply: cf *Catanzariti*...”; and noted that it may well operate to extend the territorial operation of the provisions prohibiting the manufacture, production, sale supply and administration of an illicit drug.³⁷⁰ This is the one and only sign of a willingness to give the statute any substantive operation, but it is a very small straw in the wind.

International geographical jurisdiction

The Model Criminal Code is a model State and Territory law. While the States and Territories retain, under the Australian constitutional structure, principal responsibility for the general criminal law, it can be argued that the quite extensive geographical extensions to the criminal jurisdiction of a State and Territory advocated in this Report are more clearly appropriate to intra Australian

367 (1998) 101 A Crim R 561. Leave to appeal to the High Court has been refused.

368 *Question of Law Reserved on Acquittal (No 1 of 1996)* (1997) 68 SASR 117.

369 (1998) 101 A Crim R 561 at 566.

370 (1998) 101 A Crim R 561 at 568.

cases and not international cases. For example, it can be argued that the concern for a legal view of Australia inherent in the Constitution, notably, for example, in section 118 of the Constitution (the full faith and credit clause) is not applicable in the international context. Against that, it can equally be argued that the rules of criminal geographical jurisdiction should only be distinguished, to a limited extent if at all, between international and (in federations) interstate cases.

In particular, the Committee draws attention to the geographical jurisdictional component of the Commonwealth *Criminal Code Amendment (Theft, Fraud, Bribery and Related Offences) Act 2000*. The Act provides that Part 2.7 be added to Chapter 2 of the Commonwealth *Criminal Code*. Part 2.7 is of particular concern to the Commonwealth because many Commonwealth offences have an international context.

The rule in countries following the common law tradition, such as Australia, has been that criminal laws apply, in general, only to conduct in the territory of the country concerned. As noted in the commentary above, in recent years, that rule has been subject to variation for a number of reasons. Many kinds of personal or business conduct take place across national boundaries, and an intended course of conduct or a particular transaction may occur in more than one country. Sometimes extended jurisdiction needs to be asserted in the interests of effectively dealing with serious transnational crimes. Many international treaties recognise this, and in relation to particular offences call for countries to exercise jurisdiction even though the conduct in question has occurred beyond their boundaries.

The main difference with Commonwealth legislation is that it usually does not deal with the general criminal law (except where it needs to be applied for specific Commonwealth situations) but with particular interests and concerns that, being of a national character, fall within the Commonwealth sphere. The practice has been for the application of Commonwealth offence provisions to be addressed case by case, depending on the purpose of the legislation.

Sometimes a formulation has been used to the effect that a Commonwealth statute 'applies outside Australia'. From such a formulation it might be assumed, and sometimes is, that offence provisions in the Act apply to any conduct by any person anywhere in the world. When such a provision was introduced in the *Crimes Act 1914* in 1960 it was certainly intended to assert jurisdiction over some conduct beyond Australia. In the parliamentary debate, although it was suggested that some limitations applied, these were only indicated rather vaguely by some illustrations.

Another example might be found in the *Proceeds of Crime Act 1987*, which 'applies outside Australia', and thus, some might think, to the laundering of the proceeds of a foreign offence entirely outside Australia. Such lack of precision is undesirable, and can cause confusion when the question arises in the courts,

as shown by the case of *McDonald v Bojkovic* [1987] VR 387.

For all those reasons, there is a need for Part 2.7. The aim of achieving clarity and consistency of principle through a *Criminal Code* will not be met without workable provisions on geographical jurisdiction. The Part sets out a menu of five different kinds of geographical reach that might apply to Commonwealth offences. One of these is called 'standard geographical jurisdiction' and will apply by way of default unless one of the other specified kinds of jurisdiction, or perhaps yet another kind of jurisdiction, is designated by statute.

Naturally, it is intended that extended forms of jurisdiction will only be applied where there is justification for this, having regard to considerations of international law, comity and practice. Moreover, where an offence is alleged to have been committed wholly in a foreign country by a person who is not an Australian citizen, consent to a prosecution by the Attorney-General will be required.

Part 2.7 Geographical jurisdiction

2.7.1 Application and effect of Part

- (1) This Part applies to all offences.
- (2) This Part extends the application of a law of this State/Territory that creates an offence beyond the territorial limits of this State/Territory if there is the nexus required by this Part between this State/Territory and the offence.
- (3) If the law that creates an offence makes provision with respect to any geographical consideration concerning the offence, that provision prevails over any inconsistent provision of this Part.

Note: Examples of special provisions made by the law creating an offence are as follows:

Part 8.1 (offences relating to contamination of goods) - see section 8.1.5; Part 9.1 (offences relating to slavery and sexual servitude) - see section 9.1.8; Part 5.1 (offences relating to stalking) - see section 5.1.22; Part 5.1 (offences relating to genital mutilation) - see section 5.1.35; Chapter 5.2 (offence relating to persistent sexual abuse) - see section 5.2.14.

2.7.2 Interpretation

- (1) For the purposes of this Part, the necessary geographical nexus is the nexus required by section 2.7.3.
- (2) For the purposes of this Part, the place in which an offence is committed is the place in which the physical elements of the offence occur.
- (3) For the purposes of this Part, the place in which an offence has an effect includes:
 - (a) any place whose peace, welfare or good government is threatened by the offence; and
 - (b) any place in which the offence would have an effect (or would cause such a threat) if the criminal activity concerned were carried out.
- (4) A reference in this Part to this State/Territory includes a reference to the coastal waters of this State/Territory in which the criminal laws of this State/Territory apply by virtue of the [here insert relevant Act of this State/Territory].

The Proposed Model

(a) General Principles

It appears that the “jurisdictional” statute so carefully thought out by the Standing Committee of Solicitors-General is being and will be so interpreted as to achieve nothing that was not already achieved by common law. It was and remains clearly beyond argument that such was not its objective. Nor should it be. It is, in the opinion of the Committee, contrary to good public policy that, at least within the Commonwealth of Australia, common law rules devised to deal with the niceties of relationships between sovereign international States should so operate as to prevent the trial of such defendants as *Isaac* and *Catanzariti* in the place in which they were found and where they are alleged to have acted to break the law.

Some courts have been willing to take a braver stance. In *Mayer v Henderson*³⁷¹, the defendant was charged with conspiring with another in Tasmania to defraud banks in Victoria. The only overt acts took place in Tasmania. After some technical argument about the effect of ss 8 and 297(1) of the *Tasmanian Code*, the question came down to application and authority of the *Board of Trade v Owen*. Wright J distinguished *Owen* (and other authority) on the ground that in this case it was clear that the accused had committed one or more overt acts within Tasmania in order to effect their overall purpose.

This distinction is no distinction at all. There is no doubt that the decision arose from a desire to avoid the rule in *Owen* on policy grounds. In particular, His Honour quoted passages from the judgement of Deane J in *Thompson*³⁷² to the effect that the States and Territories of Australia should not be treated as if they were independent nations, referred to the idea that Tasmania should not become a “sanctuary for conspirators”³⁷³ and stated:

“It may be said that in the Commonwealth of Australia there is little reason the prophylactic effect of a prosecution for conspiracy in one State where the commission of the substantive crime or proscribed act is to occur in another part of Australia.”³⁷⁴

Another “federation” has been prepared to take this path. In *Clements*³⁷⁵ the accused were charged in Scotland with being concerned in the supplying of a controlled drug to another. The supply took place entirely in England by accused who had not left England. They did not know that the drugs were destined for Scotland. There was, in short, no conspiracy to import the drugs

371 (1993) 68 A Crim R 155.

372 (1989) 169 CLR 1.

373 (1993) 68 A Crim R 155 at 161.

374 (1993) 68 A Crim R 155 at 160. See also *Bachrack* (1913) 21 CCC 257 at 265 in which the court said: “The law would be lame if it were powerless to reach conspirators so long as they took care to agree to carry into effect their wrongs beyond the borders of the country in which they conspired to do the wrongs.”

375 [1991] JC 62.

2.7.3 Extension of offences if there is a geographical nexus

- (1) If:
 - (a) all elements necessary to constitute an offence against a law of this State/Territory exist (disregarding geographical considerations); and
 - (b) a geographical nexus exists between this State/Territory 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 this State/Territory and an offence if:
 - (a) the offence is committed wholly or partly in this State/Territory (whether or not the offence has any effect in this State/Territory); or
 - (b) the offence is committed wholly outside this State/Territory, but the offence has an effect in this State/Territory.

2.7.4 Provisions relating to double criminality

- (1) This Part applies to an offence that is committed partly in this State/Territory and partly in another place outside this State/Territory, irrespective of whether it is also an offence in that other place.
- (2) This Part applies to an offence that is committed wholly in a place outside this State/Territory only if:
 - (a) it is also an offence in that place; or
 - (b) it is not also an offence in that place, but the trier of fact is satisfied that the offence constitutes such a threat to the peace, welfare or good government of this State/Territory that the offence warrants criminal punishment in this State/Territory.

into Scotland such as would attract such decisions as *Fan*³⁷⁶, *Liangsiripraeser*³⁷⁷ and *Sansom et al.*³⁷⁸ This was, of course, a case in which, while the conduct took place wholly outside the territory of the forum but which had effect within the forum - and in these cases, particularly when they involve drugs, courts are inclined to dispense with the niceties of the territorial principle. Lords Coulsfield and Wylie did so. But the Lord Justice General, Lord Hope, also said:

“The problem in this case is one as to territorial limitation as between different jurisdictions within the United Kingdom. This depends on constitutional practice and not international comity... for the purposes of the present case it is, I think, sufficient to look only at the situation within the United Kingdom and to ask why the courts of one part of it should be denied jurisdiction if the activities of persons elsewhere in the United Kingdom are seen to have their harmful effects in that part. *The presumption [of territoriality]... does not apply.*”³⁷⁹

The Committee agrees and it seems evident that the agreed model statute will have to be amended to achieve that result.

(b) Principal Statutory Provisions

A version of the statute currently says:

Territorial application of the criminal law of the State

- 5C.** (1) An offence against the law of the State is committed if—
- (a) all elements necessary to constitute the offence (disregarding territorial considerations) exist; and
 - (b) a territorial nexus exists between the State and at least one element of the offence.
- (2) A territorial nexus exists between the State and an element of an offence if—
- (a) the element is or includes an event occurring in the State; or
 - (b) the element is or includes an event that occurs outside the State but while the person alleged to have committed the offence is in the State.

³⁷⁶ (1991) 56 A Crim R 189.

³⁷⁷ [1991] 1 AC 225.

³⁷⁸ [1991] 2 WLR 366.

³⁷⁹ [1991] JC 62 at 69 (emphasis added).

2.7.5 Procedural and other provisions

- (1) The existence of the necessary geographical nexus for an offence will be presumed and the presumption is conclusive unless rebutted under subsection (2).
- (2) If a person charged with an offence disputes the existence of the necessary geographical nexus, the court will proceed with the trial of the offence in the usual way. If, at the conclusion of the trial, the trier of fact is satisfied on the balance of probabilities that the necessary geographical nexus does not exist, it must (subject to subsection (3)) make or return a finding to that effect and the charge will be dismissed.
- (3) If the trier of fact would, disregarding any geographical considerations, find the person not guilty of the offence, it must make or return a finding of not guilty. The trier of fact must make or return a finding of not guilty on the grounds of mental impairment in any such case if they were the only grounds on which the trier of fact would have found the person not guilty of the offence.
- (4) This section also applies to any alternative verdict available by law to the trier of fact in respect of another offence with which the person was not charged. A finding of guilt may be made or returned in any such case, unless the trier of fact is satisfied on the balance of probabilities that the necessary geographical nexus for that other offence does not exist.
- (5) The issue of whether the necessary geographical nexus exists must, if raised before the trial, be reserved for consideration at the trial.
- (6) A power or authority exercisable on reasonable suspicion or belief that an offence has been committed may be exercised in this State/Territory if the person in whom the power or authority is vested suspects on reasonable grounds or believes that the elements necessary to constitute the offence exist (whether or not the person suspects or believes or has any ground to suspect or believe that the necessary geographical nexus with this State/Territory exists).

- (3) The existence of the territorial nexus required by subsection (1)(b) (the “necessary territorial nexus”) will be presumed and the presumption is conclusive unless rebutted under subsection (4).
- (4) If a person charged with an offence disputes the existence of the necessary territorial nexus, the court will proceed with the trial of the offence in the usual way and if at the conclusion of the trial the court or, in the case of a jury trial, the jury is satisfied, on the balance of probabilities, that the necessary territorial nexus does not exist, it must, subject to subsection (5), make or return a finding to that effect and the charge will be dismissed.
- (5) If the court or, in the case of a jury trial, the jury would, disregarding territorial considerations, find the person not guilty of the offence (but not on the ground of insanity), the court or jury must make or return a finding of not guilty.
- (6) The issue of whether the necessary territorial nexus exists must, if raised before the trial, be reserved for consideration at the trial.
- (7) A power or authority exercisable on reasonable suspicion that an offence has been committed may be exercised in the State if the person in whom the power or authority is vested suspects on reasonable grounds that the elements necessary to constitute the offence exist (whether or not that person suspects or has any ground to suspect that the necessary territorial nexus with the State exists).
- (8) This section applies to offences committed before or after its commencement but does not apply to an offence if—
 - (a) the law under which the offence is created makes the place of commission (explicitly or by necessary implication) an element of the offence; or
 - (b) the law under which the offence is created is a law of extraterritorial operation and explicitly or by necessary implication excludes the requirement for a territorial nexus between the State and an element of the offence; or
 - (c) a charge had been laid before the commencement of this section.
- (9) This section is in addition to and does not derogate from any other basis on which the courts of the State may exercise criminal jurisdiction.

Code

(10) In this section—

“event” means any act, omission, occurrence, circumstance or state of affairs (not including intention, knowledge or any other state of mind);

“State” includes—

- (a) the territorial sea adjacent to the State; and
- (b) the sea on the landward side of the territorial sea that is not within the limits of the State.

(11) Where a person charged with a particular offence could be found guilty on that charge of some other offence or offences, that person will, for the purposes of this section, be taken to be charged with each offence.

The problem with the statute appears to lie exclusively with subsections (1) and (2).³⁸⁰ The problem with subsection (1) is simply stated. Although it is quite clear that Parliament intended the section to have substantive operation or, to use the judicial jargon, for it to be “offence creating”, the courts have not been willing to interpret it to have that effect. That result must be remedied. It is hard to see how Parliament could have been more specific about the issue, but the Committee is of the opinion that the point should be made legislatively by changing the form of the section. It proposes to do so in two ways.

- First, the Committee proposes to do so by embedding the notion of jurisdiction within the structure of the Code itself. To that end, the Committee proposes that the Chapter 2 General Principles be amended in the way specified in the draft provisions. It is intended that the change will make it clear that the notion is a part of the constituents of the offence itself.
- Second, the Committee proposes to do so by altering the wording of section 5C itself so that it conforms to a general formula of offence creation. Thus, the Committee hopes that States and Territories which desire to enact the section without enacting the general principles of the Code will be able to do so.

There are two basic sets of alternatives for changing subsection (2) so that its objectives are achieved. The first is to replace it with a more general formula. For example, one might adopt the Canadian *Libman* formula and state:

“A territorial nexus exists between the State and an element of an

³⁸⁰ It is no answer to say that, for example, should a uniform, even a completely uniform criminal code be adopted throughout Australia, there should be no jurisdictional problems. The State/Territory laws in both *Isaac* and *Catanzariti* were identical. The problem has to do with notions of State legislative power and not content.

Code

offence if a significant portion of the activities constituting the offence took place in the State or there is a real and substantial link between the offence and the State.”

In the opinion of the Committee, the fundamental problem with such an approach is that it would still leave a large area for interpretation to the very courts which, it appears, are unwilling to move away from traditional territorial considerations, however illogical they may be.

The second approach is to be far more specific. Under this approach, the idea would be to identify those situations in which a rule was needed by reference to the fact pattern typically involved. This approach would require a larger number of specific rules.

The judicial decisions, some of which have been noted above, fall into three general categories (considered from the point of view of hypothetical States A and B). They are (a) cases in which the accused commits one or more physical elements³⁸¹ of an offence in State A and the rest of the physical elements of the offence in State B; (b) cases in which the accused commits all of the physical elements of the offence in State A but the crime is intended to take effect in State B; (c) cases in which the accused commits all of the physical elements of the offence in State B, but the crime is intended to take effect in State A.³⁸² In addition, there is of course the usual situation in which the elements of the crime occur *wholly* within State A. The latter is the obvious case. The Committee is of the opinion that the Code should contemplate the obvious case to continue to make the point that the section is intended to be part of the offence creation process. The other situations must be dealt with separately.

(a) Physical Elements in State A and State B

This is the majority of trans-border cases. It poses no problem. The answer should be that the offence is committed in both States and the accused can be tried in either. It appears that it is what s 5C(2)(a) [above] is aimed at.

(b) Physical Elements in State A - Effects in State B

The cases which pose the most serious problem in which this situation occurs and which require legislative intervention are *Board of Trade v Owen* and its

381 “Physical elements” is the language used by the Model Criminal Code. The jurisdictions statute uses the word “event” but that word is defined in such a way as to mean what the Model Criminal Code would call a physical element. It is not sensible to speak of the location of fault elements except by reference to the location of the person having them. The fact that a South Australian assassin travelled through Victoria to NSW intending to kill in NSW is hardly enough to give Victoria a claim to try him or her for the resulting murder.

382 Of course, most crime falls into (a) the accused commits all physical elements of the crime in State A and the crime is intended to take effect in State A or (b) the accused commits all physical elements of the crime in State B and the crime is intended to take effect in State B. These are, of course, purely domestic crimes and not considered further.

Code

| |
|--|
| |
|--|

progeny - that is, cases in which there is a conspiratorial agreement in State A to commit a crime wholly in State B. The argument that there should be jurisdiction in State A in such cases has been made above.

(c) Physical Elements in State B - Effects in State A

There is general agreement that State A should be able to take jurisdiction in such cases. This is readily apparent in the drug cases such as *Doot*, *Fan* and *Liangsiripraesert* and in the fraud cases such as *Hansford* and *Winfield and Lipobar*. The draft provisions are designed to deal with all of these situations.

(d) Physical Presence in State A - Crime in State B

Section 5C(2)(b) enacts another rule independent of the location of the offence which turns on the presence of the defendant within the jurisdiction when the offence is committed and one or more elements of it occur outside of that jurisdiction. It is not clear what this particular ground was aimed at. This is potentially a very wide jurisdictional ground indeed. The Committee is of the opinion that it is both unnecessary and undesirable in view of the general rules which it has proposed.

(e) Ancillary Statutory Provisions

Given the width of the jurisdictional rules sought to be imposed, there are two safeguards that ought to be brought into the statutory scheme. The first has to do with double jeopardy - since an offence can be committed in more than one jurisdiction, it is only fair that the accused can be dealt with in only one of them. The second has to do with discrepancies between State and Territory laws. While it may be desirable that a uniform Model Criminal Code exist in each jurisdiction, at least for the time being differences will occur and provision should be made for them.

(i) Double Jeopardy

At common law, it was clear from an early stage that the doctrine of double jeopardy attached to a foreign criminal proceeding in much the same way, generally speaking, that it did to a criminal proceeding in the forum.³⁸³ The law of double jeopardy, even without jurisdictional differences, is fiendishly complicated and difficult to follow.³⁸⁴ In addition, the double jeopardy protections may extend beyond the *autrefois* pleas to *res judicata* and abuse of process.³⁸⁵

³⁸³ Early authorities are *Roche* (1775) 1 Leach 134 168 ER 169; *Hutchinson* (1671) 3 Keble 785, 84 ER 1011 but discussed (1678) 3 Mod 194, 87 ER 125; *Aughet* (1918) 13 Cr App R 101. The early cases are the subject of an interesting discussion in Lanham, *Cross-Border Criminal Law* (1997) at 51-53. The exact coverage of common law rules of double jeopardy is not further explored here.

³⁸⁴ See, for example, *O'Loughlin ex parte Ralphs* (1971) 1 SASR 219; *Maple v Kerrison* (1978) 18 SASR 513.

³⁸⁵ The doctrine of issue estoppel was assimilated into abuse of process by the High Court in *Rogers* (1994) 68 ALJR 688.

Code

The position adopted by the Committee is simply that the existing double jeopardy rules, whatever they are, should extend to multi-jurisdictional cases as they would to any given domestic case.³⁸⁶ It should be noted that in *Lipohar*, discussed briefly above, Gaudron, Gummow and Hayne JJ held that the operation of *autrefois* across State and Territory borders have constitutional footing.

(ii) The Double Criminality Problem

What if there happens to be a significant difference between the laws of the two jurisdictions involved? There are a number of possible types of case in which this will occur. The most obvious, and least likely, is that the conduct will be an offence in State A but not be an offence in State B (or vice versa). The more likely is that there will be differences in detail between the laws - such as indeterminate detention rather than determinate detention for a crime, or the existence of a partial defence in one State but not in another.³⁸⁷ But the clearest case by which to examine the question is the one in which there is legality in one State and illegality in another.

- Suppose, for example, that State A decides to legalise cannabis but State B does not. In that event, what of conduct in State A designed to break the cannabis laws of State B? The answer must be that, although State A has jurisdiction to try the alleged offences, it can only apply the law of State A. Under the law of State A there is, on the stated hypothesis, no offence.
- The harder question is whether State B should be able to try the alleged offences. Under the proposed jurisdictional rules, State B could well have jurisdiction and it would apply the law of State B. Is there anything wrong with that?

³⁸⁶ There is some evidence of a judicial tendency to subvert the normal rules. In *Thomas*, [1984] 3 WLR 321an Englishman working in Italy fraudulently transferred money from his employer's account to an account of his own in England. The appellant then returned to England and claimed the money. An Italian court convicted him of fraud in his absence, and sentenced him to a fine and imprisonment. When it was sought to prosecute him in England for the theft of that money, the accused pleaded *autrefois* convict. There was evidence that he could not be extradited to Italy or forced in any other way to suffer the consequences of the Italian conviction. It was clear that the English forum had jurisdiction over the offence. The Crown conceded that the charges concerned the same offence and that the doctrine of double jeopardy would normally apply. Nevertheless, the court upheld the conviction in England. The basis of the decision was that the accused had not really been in jeopardy because he had not been present. While the common-sense behind this reasoning can be appreciated, the case is wrongly decided and should not be followed. If the court was of the view that the accused should not be able to escape punishment for the theft, it should have recognised that the problem lay in the combined effect of two factors - first, the determination of the Italian court to proceed to conviction and sentence in the absence of the accused and second, the lack of an extradition arrangement. The *autrefois* doctrines should not be manipulated to overcome the effect of these two deficiencies.

³⁸⁷ This was the situation in *Ward* (1980) 142 CLR 308 in which one jurisdiction had a defence of diminished responsibility and one did not.

Code

| |
|--|
| |
|--|

While the notion of comity has featured in some discussions in recent judgments³⁸⁸, the consequences in terms of reciprocity have not been examined in detail except, in passing, by the UK Law Commission in 1978. The Commission said:

“... it is important to note that it is for each state to decide as a matter of its own penal policy what constitutes ‘harmful consequences’, and those consequences which are considered harmful by one state may be very different from those considered by another. Thus, before adopting any general rule of jurisdiction based on harmful consequences, it is necessary to consider what would be its implications as regards the jurisdiction which might be claimed by other states in respect of activities which they regard as criminal. We think a provision applicable to all offences, enabling them to be tried in England and Wales on the basis of what may loosely be called the harmful effects of the prescribed conduct in this country, would invite similar claims by other countries in respect of offences against their criminal law where at least in some cases the jurisdiction so claimed would run counter to our conceptions of public policy.”³⁸⁹.

The Law Commission was not so much concerned with the excessive claims of jurisdiction that England may make, as with the excessive claims of jurisdiction that others may make in response.

But are such claims excessive? Consider *Winfield and Lipohar*³⁹⁰ discussed above. That case involved a conspiracy outside South Australia by persons who did not enter South Australia to defraud a South Australian entity in relation to property in Victoria. The only *physical* connection with South Australia was the sending of a facsimile consisting of a false bank guarantee from Victoria to the victim’s solicitors in South Australia. If South Australia cannot prosecute this conspiracy, who can? *Board of Trade v Owen*³⁹¹ recently applied in two Australian jurisdictions, may prevent Victoria from doing so. Victoria has little real interest in prosecuting and has not in fact done so. There is a real prospect that the offence will go unprosecuted anywhere simply because of its interstate nature. This should not be contemplated as a possible result, certainly within Australia. But this was not a case, of course, in which double criminality would have proven to be a bar. Both South Australia and Victoria

388 Notably the judgment of Lord Diplock in *Treacy* [1971] AC 537, *Liangsiripraesert* [1991] AC 225 and *Libman* (1985) 21 CCC (3d) 206. The notion of comity as a basis for jurisdiction was rejected in the recent English Court of Appeal decision in *Manning* [1999] 2 WLR 430.

389 Law Commission, *Report on the Territorial and Extraterritorial Extent of the Criminal Law*, (1978), Law Comm 91, para 7.

390 (1997) 97 A Crim R 482 and (2000) 168 ALR 8.

391 [1957] AC 620.

Code

| |
|--|
| |
|--|

have a crime of conspiracy to defraud and differing versions of fraud offences. Cases in which the conduct alleged against the accused is a crime in one State but not in another are rare, at least within the domestic Australian context. Nevertheless, the rules must also take account of international cases.

It is the second kind of case outlined above which has posed difficulties for the Committee. On the one hand, it can be argued that the only thing that can be wrong with allowing State B to prosecute is that the conduct was entirely legal where some or all of it occurred (in State A). The answer to that must be - so what? State B is entitled to protect itself against conduct which is aimed at breaking its laws. The notion that the legality or otherwise of conduct belongs exclusively to the place where it happens to be committed is precisely the logic which the proposed jurisdictional rules are designed to defeat - because that logic has been shown to be faulty.

But the contrary can be argued with considerable force. The history of criminal law reform in Australia, including that of the consideration and implementation of the recommendations of this Committee, shows that the goal of uniform criminal laws has been elusive, particularly when dealing with laws which provoke highly emotive public debate. Australians can expect disuniformity to continue in relation to such areas as gambling, drug law reform, euthanasia, the age of consent for sexual behaviour and the like. The offences over which these disputes have arisen can be characterised as those involving relationships or the provision of services which may be legal in one place, but permitted in another. Individuals in the less permissive States and Territories should be free to seek those services in the more permissive States without risking prosecution from the more restrictive State or Territory. So, for example, if the Northern Territory chooses to legislate less restrictive rules about euthanasia, individuals from South Australia should be able to take advantage of that less restrictive regime without risking South Australian prosecution. The result of the continual widening of the rules of criminal jurisdiction in the recent past has been to put that freedom at risk. This is particularly so of, for example, the basing of jurisdiction on mere presence (as one arm of section 5C seeks to do).

This is an argument about the notion of comity and its meaning. It leads those who choose that line of reasoning to argue that there should be some sort of requirement of "double criminality" to place a brake on the consequences of wider concepts of jurisdiction. The conflict arises because of the mutuality of the obligation. On the one hand, State A (permissive) should respect the decision of State B to be more restrictive. On the other hand State B (restrictive) should respect the right of State A to be more permissive.

The Committee was inclined to agree with the reasoning which leads to the requirement of double criminality. On the other hand, the Committee recognised that there will be some cases in which the conduct will be legal where done but will pose such a significant threat to the laws (or peace, order

Code

| |
|--|
| |
|--|

and good government) of the place in which it will or does have an impact that it would be unconscionable not to allow the jurisdiction which is under threat to prosecute. The Committee considered amending its proposed rule about the place of impact to a place where there was a “significant” or “substantial” impact, but decided not to do so. Once the principle of double criminality is accepted, the rule of jurisdiction proposed in such cases is simply another option which allows *either* State A *or* State B to prosecute a crime which is punishable in *both* States. As a matter of practice, the State with the greatest claim to try the accused would be likely to do so as is the case now where it is clear that an accused has committed crimes in more than one State. So, if defendant D places a bomb on a train which will travel through States A, B and C, and it is unclear where the bomb would have exploded, any of the given States can take jurisdiction.

However, the Committee decided that the *exception to the double criminality rule* should be qualified by a requirement of substantial effect, because this would, indeed, be an exceptional case. Hence, while the ordinary rule, applicable in almost all cases, ought to have a double criminality requirement, it should also be open for the prosecution to persuade the court that the offence alleged did or would have had such a significant effect in the State in which the accused is tried that the court should take jurisdiction. Suppose, for example, that State A allows pyramid selling and State B does not. While State A is of the firm and considered opinion that it should not interfere in this particular form of private enterprise, State B is equally of the firm and considered opinion that such schemes are general frauds on the public and ought to be punished. If two accused agree in State A to set up a pyramid scheme aimed wholly or partly against a substantial number of residents of State B (via the Internet, for example), it should be open for a prosecutor in State B to argue that the offence alleged did or would have had such a significant effect in State B that the court should take jurisdiction, even though what was done was legal in State A, where the accused acted and were present.

The substantive content of the way in which the Committee has tried to reconcile the demands of comity and freedom is apparent from both the draft provisions and the commentary which follows. At this point, however, it is appropriate to record the results of consultation on the Discussion Paper. The area of law being canvassed is, of course, both esoteric and complex, and thus elicited little excitement and few responses.

General Comments

1. The Western Australian Supreme Court Judges³⁹² thought that jurisdiction should (at least) be based on the presence of the accused within the jurisdiction at the time at which the harm occurs

392 Submission, 15 March, 2000.

Code

| |
|--|
| |
|--|

anywhere. As noted in the discussion above, this is the rule currently expressed in the equivalents of s 5C(2)(b). The Committee remains of the opinion that the rules that it proposes cover the situations which the Judges wanted addressed and do so more comprehensively. The “hacker” who operates within (say) Western Australia and causes damage outside of that State will be caught by the rule covering conduct wholly or partly committed within that State, unless there is an offence which has no conduct at all. The last alternative is not a realistic possibility.

2. The Western Australian Supreme Court Judges also thought that there should be a rule which said that a person who is guilty of an offence anywhere should be triable where he or she commits an offence and then comes into the territory of the State having committed the offence. The object of this provision would be to prevent an offender using the border as a haven. The Judges state that this once was the rule in Western Australia³⁹³ but the rule was repealed in 1990. As it turns out, the relevant provision was concerned with criminal offences which occurred in the “adjacent off-shore area” of Western Australia and *not* anywhere at all. The Murray Report recommended its repeal in 1983 as being no longer needed because of the constitutional settlement reached as a result of the Crimes at Sea legislation. No doubt that is why it disappeared. The effect of the Judges’ recommendation would be to abolish jurisdictional rules entirely. It is not a recommendation based on legal precedent. The Committee could not agree with it.
3. The Australian Customs Service submitted that there should be no exceptions to the double criminality requirement³⁹⁴. The submission states: “... it is thought that [the provision] goes too far in that it seeks to create a criminal offence in a jurisdiction in which there is no offence of that kind. While criminal liability for given conduct may be highly desirable, the creation of offences should not arise in provisions concerned with jurisdiction. Additionally, the kind of offence referred to in [the provision] becomes difficult to defend because the offending conduct has not been properly defined with that jurisdiction.” (emphasis in the original). The Committee is of the opinion that the principles advocated in this comment are correct, but involve a misapplication of the relevant provision. First, for reasons already explained, it is necessary to make jurisdictional provisions “offence creating” in the relevant sense. But, second, more specifically, the “offence

³⁹³ Citing s 14A of the *Criminal Code*, repealed by No 101 of 1990, s 5.

³⁹⁴ Submission, 22 March, 2000.

Code

| |
|--|
| |
|--|

creation” does not occur according to the recommended provision in the jurisdiction in which the conduct is *legal*. The provision in question permits the jurisdiction in which the conduct is *illegal* to apply its criminal law to the conduct of the accused even though that conduct took place where the conduct was legal (in highly specific and exceptional circumstances). There is, therefore, no creation of an offence in the place where the conduct is legal. Nor is there any greater difficulty in defending the charge where the conduct is illegal.

4. Sir Harry Gibbs was also of the opinion that the double criminality exception was too wide, although his opinion was based on narrower grounds. The root of his objection lay in the use of the phrase “peace welfare and good government” as being too unclear and vague. While it is difficult to summarise justly and concisely the submission of a person of his legal eminence, the essence of what he has to say appears to be as follows:

“It is true that it has been said that one reason for treating acts done outside the jurisdiction as within the scope of a criminal statute is that they are a threat to society within the jurisdiction, but that does not mean that general words used in giving a reason for a conclusion should be transposed into a criminal statute as the test for applicability of the statute. The aim of any criminal statute should be clarity and precision, and the use of the words “peace welfare and good government” would not assist the attainment of that aim.”

Again, the Committee agrees with the general principles advocated by Sir Harry Gibbs. It does not agree with the conclusions that he draws from them. As Sir Harry Gibbs says, there must be some mechanism for describing in law the power of the criminal courts of a forum to deal with conduct contrary to the laws of the form which is committed elsewhere but which has an impacts in the forum or which attacks the interests of the forum which are protected by that criminal law. *Lipohar and Winfield*³⁹⁵ is the classic example. The only question that is left is how best to describe the principle that does it. The formula used by the common law is a series of variations on whether or not the crime in question involved a breach of the Queen’s Peace in the impacted State³⁹⁶. There is nothing very precise about this formulation. The phrase “peace welfare and good government” is, as Sir Harry points out, the formula used by the High Court to describe and define the

395 (2000) 168 ALR 8.

396 See, for example, *Hansford* (1974) 8 SASR 164.

Code

| Code |
|------|
|------|

limits of power of sovereign State legislatures. Concededly, it is not very precise either. But it has a meaning well known to the courts, defined and described by precedent. Some things are and some things are not. It is the best descriptor that the Committee could devise within which to circumscribe the limits of State power in an exceptional situation. It does not stand alone. The section also requires a judgment that the State interest is so impaired as to warrant criminal punishment. This is also a familiar formula. While extremely imprecise and demanding an individual qualitative judgment, it is no less useful for all that. Finally, what is the alternative? Sir Harry Gibbs suggests that it be replaced by the criterion of whether or not the conduct was intended to have an impact on the offended State. That, it is submitted, contains little more in the way of precision and is, in any event, contrary to all of the judgments in *Lipohar and Winfield*³⁹⁷ (and the desirable result on the facts in that case). In the end, therefore, Sir Harry Gibbs is right to say that the test is imprecise - but it can be little else, for the reasons given in the commentary which explain why it is that the exception to double criminality requirement is recommended.

5. The Committee received some lengthy and well considered comments from Professor David Lanham of the University of Melbourne³⁹⁸, whose expertise in the area of criminal jurisdiction is well known³⁹⁹. While it is difficult to do justice to the complexity of his submission here, broadly speaking, Professor Lanham is of the opinion that the widening of the scope of criminal jurisdiction proposed by the Committee will lead to injustice because it will allow the prosecution to “forum shop” to prosecute in the State or Territory with the harshest law. This is a problem of the applicable law. He says:

“What then is needed is not a double criminality rule but a rule which identifies the appropriate law and requires that liability shall not exceed that under the appropriate law. There is no need for double criminality where the defendant is tried in the jurisdiction of the appropriate law, nor is any other jurisdiction called to enforce that law.”

Professor Lanham argues strongly that it is likely that the appropriate law will be the place where the harm is done. Without wishing to do any injustice to the depth and subtlety of Professor

³⁹⁷ See the account of the judgments of that case in the discussion above.

³⁹⁸ Submission, 22 February, 2000.

³⁹⁹ Lanham, *Cross-Border Criminal Law* (1997).

Code

| |
|--|
| |
|--|

Lanham's views, the Committee does not think that the solution to the problems which it has outlined lie in (a) the creation of a very general and vague choice of law rule which (b) points the courts back to the old law of the place where the crime had impact. This seems, to the Committee, to be little improvement upon what it sees as the unsatisfactory state of the current law.

It should be noted that New South Wales has already enacted the recommended provisions⁴⁰⁰.

International and Interstate Cases

The Discussion Paper sought comment on the question whether the proposed State/Territory jurisdictional provisions should apply to international as well as intra-national cases. There was no consensus on that issue. The responses to that question are as follows:

1. The Commonwealth DPP said that "the proposed provisions should be redrafted to make it clear, beyond all possible doubt, that they are designed to apply to international conduct as well as inter-State conduct."⁴⁰¹ That is a drafting issue. The drafting advice available to the Committee is to the effect that the unqualified enactment of the proposed provisions will achieve the desired result.
2. Dr Russell Smith, of the Australian Institute of Criminology, expressed the view that the proposed provisions should be capable of application to international crimes⁴⁰². So too did the Australian Federal Police⁴⁰³.
3. On the other hand, the Australian Customs Service⁴⁰⁴ thought that, while the problems were much the same, the claiming of international jurisdiction by States and Territories in this way could lead to the (undesirable) prosecution of people for conduct lawful in their own countries, and that the preferable way to proceed is by way of international treaties. The latter reason is a matter of opinion, but the former is no real objection. Whether or not conduct is lawful in the country of the accused's country of origin is an irrelevant consideration under either current or proposed law absent any other considerations, and so it should be. If South

400 *Crimes Legislation Amendment Act*, No 43 of 2000.

401 Submission, 22 March, 2000.

402 Submission, 3 April, 2000. Dr Smith also expressed reservations in relation to the double jeopardy issue and the vagueness of certain terms used. These reservations are addressed elsewhere in this discussion.

403 Submission, 30 April, 2000.

404 Submission, 22 March, 2000.

Code

| |
|--|
| |
|--|

Australia should possibly legalise the possession of cannabis, one begs leave to doubt that that legal fact will impress the authorities of Malaysia should a South Australian possess some there. Legality in the place in which one is committing conduct has greatly exercised the mind of the Committee in the ways described above.

4. Sir Harry Gibbs⁴⁰⁵ was also of the opinion that the proposed provisions should be limited to intra-national cases. His reasons, generally stated, were that such a broad claim of criminal jurisdiction would (a) offend notions of international comity⁴⁰⁶; and (b) invite reciprocal claims of broad reach jurisdiction by other countries against Australian offenders.

The Committee accepts that there is a clear divergence of opinion on this issue and it may be one where individuals jurisdictions will differ. However, in the end, the Committee came to the conclusion that the jurisdictional rules which it has proposed are justifiable on their merits and sees no reason why they should not be applied by States and Territories in the international context. If a State Parliament has the constitutional power to legislate for the peace, welfare and good government of the State, it has the correlative right to, in effect, enact criminal offences which protect its justifiable interests. State and Territory legal systems must, by their nature, have other laws which determine the reach of their application, and that is no less true of criminal laws than of other laws. We call those laws, in the criminal context, jurisdictional rules. If the Committee's recommendations are not followed, then other default rules will be applied. The Committee believes that it has demonstrated that those default rules are inefficient and lead to poor results. They should therefore be replaced. The Committee's believes that its model provisions offer a fair and just solution to the problem.

Other Issues

The Western Australian Supreme Court Judges⁴⁰⁷ and the Australian Customs Service⁴⁰⁸ were of the opinion that the issue should not be "reserved for trial" because it should be resolved prior to the commencement of the trial, as is the case with many pre-trial issues, thereby saving considerable delay and expense in the criminal justice system. This submission did not attract the support of the Committee. First, the provision referred to is intended to prevent the issue of jurisdiction being litigated at the preliminary hearing or committal stage. But second, and more importantly, if the issue is contested, the agreed provisions clearly provide that the matter is one of the jury, a position with which the

405 Submission, 29 March, 2000.

406 Citing *Treacy* [1971] AC 537.

407 Submission, 15 March, 2000.

408 Submission, 22 March, 2000.

Code

Committee agrees. For the reasons described in the discussion above, the Committee has taken the position that jurisdiction is “offence creating” and thus akin to an element of the offence itself. It is, therefore not analogous to questions of procedure and the admissibility of evidence which can be dealt with expeditiously in the way to which the Judges refer.

The Australian Customs Service⁴⁰⁹ and Legal Aid (WA)⁴¹⁰ both thought that there should be explicit provision for the operation of the rules preventing double jeopardy in this context. The Committee did not do this, although it agrees that the normal rules should apply, for the reasons stated earlier in this discussion.

409 Submission, 22 March, 2000.

410 Submission, 25 March, 2000.

Part 2.7 Geographical jurisdiction

2.7.1 Application and effect of Part

- (1) This Part applies to all offences.
- (2) This Part extends the application of a law of this State/Territory that creates an offence beyond the territorial limits of this State/Territory if there is the nexus required by this Part between this State/Territory and the offence.
- (3) If the law that creates an offence makes provision with respect to any geographical consideration concerning the offence, that provision prevails over any inconsistent provision of this Part.

Note: Examples of special provisions made by the law creating an offence are as follows:

Part 8.1 (offences relating to contamination of goods) - see section 8.1.5; Part 9.1 (offences relating to slavery and sexual servitude) - see section 9.1.8; Part 5.1 (offences relating to stalking) - see section 5.1.22; Part 5.1 (offences relating to genital mutilation) - see section 5.1.35; Chapter 5.2 (offence relating to persistent sexual abuse) - see section 5.2.14.

2.7.2 Interpretation

- (1) For the purposes of this Part, the necessary geographical nexus is the nexus required by section 2.7.3.
- (2) For the purposes of this Part, the place in which an offence is committed is the place in which the physical elements of the offence occur.
- (3) For the purposes of this Part, the place in which an offence has an effect includes:
 - (a) any place whose peace, welfare or good government is threatened by the offence; and
 - (b) any place in which the offence would have an effect (or would cause such a threat) if the criminal activity concerned were carried out.
- (4) A reference in this Part to this State/Territory includes a reference to the coastal waters of this State/Territory in which the criminal laws of this State/Territory apply by virtue of the [here insert relevant Act of this State/Territory].

Part 2.7 - Geographical Jurisdiction

This Part, which deals with *Geographical Jurisdiction*, began from the notion that drafting should use the existing legislation, approved by the Standing Committee of Attorneys-General, and enacted in several Australian jurisdictions, as a basis for reform. The need for reform is outlined in the text and stems from a sequence of judicial decisions limiting the effect of the SCAG model. The drafting of this Part was informed, so far as was possible in the very limited time available, by the decision of the High Court in *Lipohar* [2000] 168 ALR 8. However, the core of the reasoning in *Lipohar* is based on the fact that a common law offence was charged whereas the Model Code is, of course, based entirely in statutory offences.

It should be noted that the draft does not distinguish in any way between State and Territory offences occurring wholly within Australian borders and offences which have international connections. *Lipohar* offers no guidance as to the relevance of the distinction, if any.

2.7.1 - Application and Effect of Part

This section is designed to make it clear that the Part is “offence creating” in the sense that it *extends* the geographical or territorial reach of state offences. In accordance with the injunction of the High Court in *Lipohar*, the word “jurisdiction” has been avoided in favour of the words “geographical” and “territorial”. The current SCAG approved scheme speaks of “disregarding” geographical reach. This word was also avoided because it is clear that geographical considerations are not disregarded - they are a part of the offence, but the reach of the offence is extended beyond the territorial boundaries of the State or Territory.

2.7.2 - Interpretation

The definition of the place where the offence is committed is defined to mean the place in which the physical elements of the offence occur. This definition requires two comments. First, it is meant to refer to any place in which any of the physical elements of the offence occur. Offences may, both in current law and in the proposed law, occur in more than one place at any given time. Second, the term “physical elements” is a technical term under the Code and refers to the definition of “physical elements” in s 4.1 of Chapter 2 of the Model Criminal Code - that is, conduct, circumstances or results.

The definition of the place where an offence has an effect refers, inter alia, to any place whose “peace, welfare or good government” is threatened by the offence. The phrase “peace, welfare or good government” has been used as a demarcation of the constitutional limitation placed upon the otherwise plenary legislative power of a State. The High Court has indicated that “peace, welfare or good government” bears the same meaning as “peace, order or good government” [*Union Steamship v King* (1988) 166 CLR 1 at 9].

2.7.3 Extension of offences if there is a geographical nexus

- (1) If:
 - (a) all elements necessary to constitute an offence against a law of this State/Territory exist (disregarding geographical considerations); and
 - (b) a geographical nexus exists between this State/Territory 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 this State/Territory and an offence if:
 - (a) the offence is committed wholly or partly in this State/Territory (whether or not the offence has any effect in this State/Territory); or
 - (b) the offence is committed wholly outside this State/Territory, but the offence has an effect in this State/Territory.

2.7.4 Provisions relating to double criminality

- (1) This Part applies to an offence that is committed partly in this State/Territory and partly in another place outside this State/Territory, irrespective of whether it is also an offence in that other place.
- (2) This Part applies to an offence that is committed wholly in a place outside this State/Territory only if:
 - (a) it is also an offence in that place; or
 - (b) it is not also an offence in that place, but the trier of fact is satisfied that the offence constitutes such a threat to the peace, welfare or good government of this State/Territory that the offence warrants criminal punishment in this State/Territory.

2.7.3 - Extension of offences if there is a geographical nexus

This is the key section in which the essential changes to the current model are made. It defines the necessary geographical nexus that must exist between the offence and the State or Territory claiming the power to try the offence. The section simply claims power to try the offence if the offence is committed wholly or partly in the State or Territory (that is to say, one or more of the physical elements occur in the State or Territory) or, if no physical elements occur in the State or Territory, the offence has an effect (as defined above) in the State or Territory.

2.7.4 - Provisions relating to double criminality

As noted in the text, there is a good argument that, where no physical elements occur in the State or Territory, there should be a requirement that those who have acted entirely lawfully in the place where all of the elements of the offence occurred should not be exposed to criminal liability in another place unless that other place has such an overriding interest in the suppression of that particular conduct that the reach of the statute (via this Part) and hence the imposition of criminal liability is warranted. This matter is dealt with in s 2.7.4(2)(b). This is inevitably a question upon which no hard and fast rules can be devised, for this Part deals with a potentially enormous range of behaviours. Moreover, the inherent vagueness of such a criterion is not unprecedented - for example, the key criterion of "dishonesty" in relation to a wide variety of offences in Chapter 3 is similarly one which is notoriously incapable of precise delineation.

2.7.5 Procedural and other provisions

- (1) The existence of the necessary geographical nexus for an offence will be presumed and the presumption is conclusive unless rebutted under subsection (2).
- (2) If a person charged with an offence disputes the existence of the necessary geographical nexus, the court will proceed with the trial of the offence in the usual way. If, at the conclusion of the trial, the trier of fact is satisfied on the balance of probabilities that the necessary geographical nexus does not exist, it must (subject to subsection (3)) make or return a finding to that effect and the charge will be dismissed.
- (3) If the trier of fact would, disregarding any geographical considerations, find the person not guilty of the offence, it must make or return a finding of not guilty. The trier of fact must make or return a finding of not guilty on the grounds of mental impairment in any such case if they were the only grounds on which the trier of fact would have found the person not guilty of the offence.
- (4) This section also applies to any alternative verdict available by law to the trier of fact in respect of another offence with which the person was not charged. A finding of guilt may be made or returned in any such case, unless the trier of fact is satisfied on the balance of probabilities that the necessary geographical nexus for that other offence does not exist.
- (5) The issue of whether the necessary geographical nexus exists must, if raised before the trial, be reserved for consideration at the trial.
- (6) A power or authority exercisable on reasonable suspicion or belief that an offence has been committed may be exercised in this State/Territory if the person in whom the power or authority is vested suspects on reasonable grounds or believes that the elements necessary to constitute the offence exist (whether or not the person suspects or believes or has any ground to suspect or believe that the necessary geographical nexus with this State/Territory exists).

2.7.5 - Procedural and other provisions

These procedural provisions are a minor redraft of the existing SCAG model with no significant changes of substance. The only change worthy of note is that it includes a provision dealing with the situation in which there is a problem of proving a geographical nexus and the jury would not acquit the defendant but would rather find him or her not guilty on the ground of mental impairment. Subsection 2.7.5(3) clarifies the position by requiring a finding of not guilty on the grounds of mental impairment if they were the only grounds on which the trier of fact would have found the person not guilty of the offence. This is necessary to ensure these cases are appropriately recognised because they do not involve an acquittal.

Professor Lanham is of the opinion that the reversal of onus of proof in relation to jurisdiction is unfair⁴¹¹. He points out that the question of jurisdiction may, as in *Ward*⁴¹², determine substantive liability, or the degree of substantive liability. If, for example, as in *Ward*, the possibilities were manslaughter in NSW but murder in Victoria, then, says Professor Lanham, if the prosecution cannot prove beyond a reasonable doubt that the homicide took place in Victoria, it cannot prove murder and therefore the proper verdict is manslaughter. This objection is sustainable only if there is a choice of law rule in criminal cases. On Professor Lanham's position⁴¹³, if there is real doubt whether the homicide took place in NSW or Victoria, then, absent a shift in the burden of proof, on current common law the accused is bound to be acquitted *entirely* in *both* Victoria and NSW. That problem can only be alleviated, on Professor Lanham's position, if one has a choice of law rule which somehow applies the lowest common denominator of the possibly applicable laws. The Committee cannot agree with this position. It is very complex indeed and would be difficult to implement in practice, as it would necessarily involve a judge assessing which were the possible applicable laws and what the appropriate verdict should be under each, presumably without the benefit of a jury verdict on any. It would also necessarily involve the application by a criminal court of the criminal law and practice to an inexplicable extent of another or other jurisdictions. The Committee does not believe that this would be an acceptable solution.

411 Submission, 19 September, 2000.

412 (1980) 142 CLR 308.

413 And not that taken by the majority in *Thompson* (1989) 169 CLR 1.

Model Criminal Code Chapters 1 and 2

MODEL CRIMINAL CODE

SCHEDULE

THE CRIMINAL CODE OF [(NAME OF STATE/TERRITORY)]

CHAPTER 1 - CODIFICATION

Division 1

Codification

- 1.1 The only offences against laws of [Name of State/Territory] are those offences created by, or under the authority of, this Code or any other Act of [Name of State/Territory].

CHAPTER 2 - GENERAL PRINCIPLES OF CRIMINAL RESPONSIBILITY

PART 2.1 - PURPOSE AND APPLICATION

Division 2

Purpose

- 2.1 The purpose of this Chapter is to codify the general principles of criminal responsibility under laws of [Name of State/Territory]. It contains all the general principles of criminal responsibility that apply to any offence, irrespective of how the offence is created.

Application

- 2.2 (1) This Chapter applies to all offences against this Code.
- (2) On and after the day occurring 5 years after the day on which the Criminal Code Act 1994 of [Name of State/Territory] receives the Royal Assent, this Chapter applies to all other offences.
- (3) Section 11.6 applies to all offences.

PART 2.2 - THE ELEMENTS OF AN OFFENCE

Division 3 - General

Elements

- 3.1 (1) An offence consists of physical elements and fault elements.
- (2) However, the law that creates the offence may provide that there is no fault element for one or more physical elements.
- (3) The law that creates the offence may provide different fault elements for different physical elements.

Establishing guilt in respect of offences

- 3.2 In order for a person to be found guilty of committing an offence the following must be proved:
 - (a) the existence of such physical elements as are, under the law creating the offence, relevant to establishing guilt;
 - (b) in respect of each such physical element for which a fault element is required, one of the fault elements for the physical element.

Note: See Part 2.6 on proof of criminal responsibility.

Division 4 - Physical elements

Physical elements

- 4.1 (1) A physical element of an offence may be:
 - (a) conduct; or
 - (b) a circumstance in which conduct occurs; or
 - (c) a result of conduct.
- (2) In this Code:

“conduct” means an act, an omission to perform an act or a state of affairs.

Voluntariness

- 4.2 (1) Conduct can only be a physical element if it is voluntary.
- (2) Conduct is only voluntary if it is a product of the will of the person whose conduct it is.
- (3) The following are examples of conduct that is not voluntary:
- (a) a spasm, convulsion or other unwilled bodily movement;
 - (b) an act performed during sleep or unconsciousness;
 - (c) an act performed during impaired consciousness depriving the person of the will to act.
- (4) An omission to perform an act is only voluntary if the act omitted is one which the person is capable of performing.
- (5) If the conduct constituting an offence consists only of a state of affairs, the state of affairs is only voluntary if it is one over which the person is capable of exercising control.
- (6) Evidence of self-induced intoxication cannot be considered in determining whether conduct is voluntary.
- (7) Intoxication is self-induced unless it came about:
- (a) involuntarily; or
 - (b) as a result of fraud, sudden or extraordinary emergency, accident, reasonable mistake, duress or force.

Omissions

- 4.3 An omission to perform an act can only be a physical element if:
- (a) the law creating the offence makes it so; or
 - (b) the law creating the offence impliedly provides that the offence is committed by an omission to perform an act that by law there is a duty to perform.

Division 5 - Fault elements

Fault elements

- 5.1 (1) A fault element for a particular physical element may be intention, knowledge, recklessness or negligence.
- (2) Subsection (1) does not prevent a law that creates a particular offence from specifying other fault elements for a physical element of that offence.

Note: Under subsection 5.4 (4), recklessness can be established by proving intention, knowledge or recklessness.

Intention

- 5.2 (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.

Knowledge

- 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.

Recklessness

- 5.4 (1) A person is reckless with respect to a circumstance if:
- (a) he or she is aware of a substantial risk that the circumstance exists or will exist; and
 - (b) having regard to the circumstances known to him or her, it is unjustifiable to take the risk.
- (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.

Negligence

- 5.5 A person is negligent with respect to a physical element of an offence if his or her conduct involves:
- (a) such a great falling short of the standard of care that a reasonable person would exercise in the circumstances; and
 - (b) such a high risk that the physical element exists or will exist; that the conduct merits criminal punishment for the offence.

Offences that do not specify fault elements

- 5.6 (1) If the law creating the offence does not specify a fault element for a physical element of an offence that consists only of conduct, intention is the fault element for that physical element.
- (2) If the law creating the offence does not specify a fault element for a physical element of an offence that consists of a circumstance or a result, recklessness is the fault element for that physical element.

Note: Under subsection 5.4(4), recklessness can be established by proving intention, knowledge or recklessness.

*Division 6 - Cases where fault elements are not required***Strict liability**

- 6.1 (1) If a law that creates an offence provides that the offence is an offence of strict liability:
- (a) there are no fault elements for any of the physical elements of the offence; and
 - (b) the defence of mistake of fact under section 9.2 is available.
- (2) If a law that creates an offence provides that strict liability applies to a particular physical element of the offence:
- (a) there are no fault elements for that physical element; and
 - (b) the defence of mistake of fact under section 9.2 is available in relation to that physical element.
- (3) The existence of strict liability does not make any other defence unavailable.

Absolute liability

- 6.2 (1) If a law that creates an offence provides that the offence is an offence of absolute liability:
- (a) there are no fault elements for any of the physical elements of the offence; and
 - (b) the defence of mistake of fact under section 9.2 is unavailable.
- (2) If a law that creates an offence provides that absolute liability applies to a particular physical element of the offence:
- (a) there are no fault elements for that physical element; and
 - (b) the defence of mistake of fact under section 9.2 is unavailable in relation to that physical element.
- (3) The existence of absolute liability does not make any other defence unavailable.

PART 2.3 - CIRCUMSTANCES IN WHICH THERE IS NO CRIMINAL RESPONSIBILITY

Note: This Part sets out defences that are generally available. Defences that apply to a more limited class of offences are dealt with elsewhere in this Code and in other laws.

Division 7 - Circumstances involving lack of capacity

Children under 10

- 7.1 A child under 10 years old is not criminally responsible for an offence.

Children over 10 but under 14

- 7.2 (1) A child aged 10 years or more but under 14 years old can only be criminally responsible for an offence if the child knows that his or her conduct is wrong.
- (2) The question whether a child knows that his or her conduct is wrong is one of fact. The burden of proving this is on the prosecution.

Mental impairment

- 7.3 (1) A person is not criminally responsible for an offence if, at the time of carrying out the conduct constituting the offence, the person was suffering from a mental impairment that had the effect that:

- (a) the person did not know the nature and quality of the conduct; or
 - (b) the person did not know that the conduct was wrong (that is, the person could not reason with a moderate degree of sense and composure about whether the conduct, as perceived by reasonable people, was wrong); or
 - (c) the person was unable to control the conduct.
- (2) The question whether the person was suffering from a mental impairment is one of fact.
- (3) A person is presumed not to have been suffering from such a mental impairment. The presumption is only displaced if it is proved on the balance of probabilities (by the prosecution or the defence) that the person was suffering from such a mental impairment.
- (4) The prosecution can only rely on this section if the court gives leave.
- (5) The tribunal of fact must return a special verdict that a person is not guilty of an offence because of mental impairment if and only if it is satisfied that the person is not criminally responsible for the offence only because of a mental impairment.
- (6) A person cannot rely on a mental impairment to deny voluntariness or the existence of a fault element but may rely on this section to deny criminal responsibility.
- (7) If the tribunal of fact is satisfied that a person carried out conduct as a result of a delusion caused by a mental impairment, the delusion cannot otherwise be relied on as a defence.
- (8) In this section: “mental impairment” includes senility, intellectual disability, mental illness, brain damage and severe personality disorder.
- (9) The reference in subsection (8) to mental illness is a reference to an underlying pathological infirmity of the mind, whether of long or short duration and whether permanent or temporary, but does not include a condition that results from the reaction of a healthy mind to extraordinary external stimuli. However, such a condition may be evidence of a mental illness if it involves some abnormality and is prone to recur.

Division 8 - Intoxication

Definition - self-induced intoxication

8.1 For the purposes of this Division, intoxication is self-induced unless it came about:

- (a) involuntarily; or
- (b) as a result of fraud, sudden or extraordinary emergency, accident, reasonable mistake, duress or force.

Intoxication (offences involving basic intent)

8.2 (1) Evidence of self-induced intoxication cannot be considered in determining whether a fault element of basic intent existed.

(2) A fault element of basic intent is a fault element of intention for a physical element that consists only of conduct.

Note: A fault element of intention with respect to a circumstance is not a fault element of basic intent.

(3) This section does not prevent evidence of self-induced intoxication being taken into consideration in determining whether conduct was accidental.

(4) This section does not prevent evidence of self-induced intoxication being taken into consideration in determining whether a person had a mistaken belief about facts if the person had considered whether or not the facts existed.

(5) A person may be regarded as having considered whether or not facts existed if:

- (a) he or she had considered, on a previous occasion, whether those facts existed in circumstances surrounding that occasion; and
- (b) he or she honestly and reasonably believed that the circumstances surrounding the present occasion were the same, or substantially the same, as those surrounding the previous occasion.

Intoxication (negligence as fault element)

8.3 (1) If negligence is a fault element for a particular physical element of an offence, in determining whether that fault element existed in relation to a person who is intoxicated, regard must be had to the standard of a reasonable person who is not intoxicated.

- (2) However, if intoxication is not self-induced, regard must be had to the standard of a reasonable person intoxicated to the same extent as the person concerned.

Intoxication (relevance to defences)

- 8.4 (1) If any part of a defence is based on actual knowledge or belief, evidence of intoxication may be considered in determining whether that knowledge or belief existed.
- (2) If any part of a defence is based on reasonable belief, in determining whether that reasonable belief existed, regard must be had to the standard of a reasonable person who is not intoxicated.
- (3) If a person's intoxication is not self-induced, in determining whether any part of a defence based on reasonable belief exists, regard must be had to the standard of a reasonable person intoxicated to the same extent as the person concerned.
- (4) If, in relation to an offence:
 - (a) each physical element has a fault element of basic intent; and
 - (b) any part of a defence is based on actual knowledge or belief; evidence of self-induced intoxication cannot be considered in determining whether that knowledge or belief existed.
- (5) A fault element of basic intent is a fault element of intention for a physical element that consists only of conduct.

Note: A fault element of intention with respect to a circumstance is not a fault element of basic intent.

Involuntary intoxication

- 8.5 A person is not criminally responsible for an offence if the person's conduct constituting the offence was as a result of intoxication that was not self-induced.

Division 9 - Circumstances involving mistake or ignorance

Mistake or ignorance of fact (fault elements other than negligence)

- 9.1 (1) A person is not criminally responsible for an offence that has a physical element for which there is a fault element other than negligence if:

Appendix 1

- (a) at the time of the conduct constituting the physical element, the person is under a mistaken belief about, or is ignorant of, facts; and
 - (b) the existence of that mistaken belief or ignorance negates any fault element applying to that physical element.
- (2) In determining whether a person was under a mistaken belief about, or was ignorant of, facts, the tribunal of fact may consider whether the mistaken belief or ignorance was reasonable in the circumstances.

Mistake of fact (strict liability)

- 9.2 (1) A person is not criminally responsible for an offence that has a physical element for which there is no fault element if:
- (a) at or before the time of the conduct constituting the physical element, the person considered whether or not facts existed, and is under a mistaken but reasonable belief about those facts; and
 - (b) had those facts existed, the conduct would not have constituted an offence.
- (2) A person may be regarded as having considered whether or not facts existed if:
- (a) he or she had considered, on a previous occasion, whether those facts existed in the circumstances surrounding that occasion; and
 - (b) he or she honestly and reasonably believed that the circumstances surrounding the present occasion were the same, or substantially the same, as those surrounding the previous occasion.

Note: Section 6.2 prevents this section applying in situations of absolute liability.

Mistake or ignorance of statute law

- 9.3 (1) A person can be criminally responsible for an offence even if, at the time of the conduct constituting the offence, he or she is mistaken about, or ignorant of, the existence or content of an Act that directly or indirectly creates the offence or directly or indirectly affects the scope or operation of the offence.
- (2) Subsection (1) does not apply, and the person is not criminally responsible for the offence in those circumstances, if:

- (a) the Act is expressly or impliedly to the contrary effect; or
- (b) the ignorance or mistake negates a fault element that applies to a physical element of the offence.

Mistake or ignorance of subordinate legislation

- 9.4 (1) A person can be criminally responsible for an offence even if, at the time of the conduct constituting the offence he or she is mistaken about, or ignorant of, the existence or content of the subordinate legislation that directly or indirectly creates the offence or directly or indirectly affects the scope or operation of the offence.
- (2) Subsection (1) does not apply, and the person is not criminally responsible for the offence in those circumstances, if:
- (a) the subordinate legislation is expressly or impliedly to the contrary effect; or
 - (b) the ignorance or mistake negates a fault element that applies to a physical element of the offence; or
 - (c) at the time of the conduct, copies of the subordinate legislation have not been made available to the public or to persons likely to be affected by it, and the person could not be aware of its content even if he or she exercised due diligence.
- (3) In this section:
- “**available**” includes available by sale;
- “**subordinate legislation**” means an instrument of a legislative character made directly or indirectly under an Act, or in force directly or indirectly under an Act.

Claim of right

- 9.5 (1) A person is not criminally responsible for an offence that has a physical element relating to property if:
- (a) at the time of the conduct constituting the offence, the person is under a mistaken belief about a proprietary or possessory right; and
 - (b) the existence of that right would negate a fault element for any physical element of the offence.
- (2) A person is not criminally responsible for any other offence arising necessarily out of the exercise of the proprietary or possessory right that he or she mistakenly believes to exist.

- (3) This section does not negate criminal responsibility for an offence relating to the use of force against a person.

Division 10 - Circumstances involving external factors

Intervening conduct or event

- 10.1 A person is not criminally responsible for an offence that has a physical element to which absolute liability or strict liability applies if:
- (a) the physical element is brought about by another person over whom the person has no control or by a non-human act or event over which the person has no control; and
 - (b) the person could not reasonably be expected to guard against the bringing about of that physical element.

Duress

- 10.2 (1) A person is not criminally responsible for an offence if he or she carries out the conduct constituting the offence under duress.
- (2) A person carries out conduct under duress if and only if he or she reasonably believes that:
- (a) a threat has been made that will be carried out unless an offence is committed; and
 - (b) there is no reasonable way that the threat can be rendered ineffective; and
 - (c) the conduct is a reasonable response to the threat.
- (3) This section does not apply if the threat is made by or on behalf of a person with whom the person under duress is voluntarily associating for the purpose of carrying out conduct of the kind actually carried out.

Sudden or extraordinary emergency

- 10.3 (1) A person is not criminally responsible for an offence if he or she carries out the conduct constituting the offence in response to circumstances of sudden or extraordinary emergency.
- (2) This section applies if and only if the person carrying out the conduct reasonably believes that:
- (a) circumstances of sudden or extraordinary emergency exist; and

- (b) committing the offence is the only reasonable way to deal with the emergency; and
- (c) the conduct is a reasonable response to the emergency.

Self-defence

- 10.4 (1) A person is not criminally responsible for an offence if he or she carries out the conduct constituting the offence in self-defence.
- (2) A person carries out conduct in self-defence if and only if he or she believes the conduct is necessary:
- (a) to defend himself or herself or another person; or
 - (b) to prevent or terminate the unlawful imprisonment of himself or herself or another person; or
 - (c) to protect property from unlawful appropriation, destruction, damage or interference; or
 - (d) to prevent criminal trespass to any land or premises; or
 - (e) to remove from any land or premises a person who is committing criminal trespass;
- and the conduct is a reasonable response in the circumstances as he or she perceives them.
- (3) This section does not apply if the person uses force that involves the intentional infliction of death or really serious injury:
- (a) to protect property; or
 - (b) to prevent criminal trespass; or
 - (c) to remove a person who is committing criminal trespass.
- (4) This section does not apply if:
- (a) the person is responding to lawful conduct; and
 - (b) he or she knew that the conduct was lawful.
- However, conduct is not lawful merely because the person carrying it out is not criminally responsible for it.

PART 2.4 - EXTENSIONS OF CRIMINAL RESPONSIBILITY

Division 11

Attempt

- 11.1 (1) A person who attempts to commit an offence is guilty of the offence of attempting to commit that offence and is punishable as if the offence attempted had been committed.
- (2) For the person to be guilty, the person's conduct must be more than merely preparatory to the commission of the offence. The question whether conduct is more than merely preparatory to the commission of the offence is one of fact.
- (3) For the offence of attempting to commit an offence, intention and knowledge are fault elements in relation to each physical element of the offence attempted.
- Note: Under section 3.2, only one of the fault elements of intention or knowledge would need to be established in respect of each physical element of the offence attempted.
- (4) A person may be found guilty even if:
- (a) committing the offence attempted is impossible; or
 - (b) the person actually committed the offence attempted.
- (5) A person who is found guilty of attempting to commit an offence cannot be subsequently charged with the completed offence.
- (6) Any defences, procedures, limitations or qualifying-provisions that apply to an offence apply also to the offence of attempting to commit that offence.
- (7) It is not an offence to attempt to commit an offence against section 11.2 (complicity and common purpose) or section 11.5 (conspiracy).

Complicity and common purpose

- 11.2 (1) A person who aids, abets, counsels or procures the commission of an offence by another person is taken to have committed that offence and is punishable accordingly.
- (2) For the person to be guilty:
- (a) the person's conduct must have in fact aided, abetted, counselled or procured the commission of the offence by the other person; and

- (b) the offence must have been committed by the other person.
- (3) For the person to be guilty, the person must have intended that:
 - (a) his or her conduct would aid, abet, counsel or procure the commission of any offence (including its fault elements) of the type the other person committed; or
 - (b) his or her conduct would aid, abet, counsel or procure the commission of an offence and have been reckless about the commission of the offence (including its fault elements) that the other person in fact committed.
- (4) A person cannot be found guilty of aiding, abetting, counselling or procuring the commission of an offence if, before the offence was committed, the person:
 - (a) terminated his or her involvement; and
 - (b) took all reasonable steps to prevent the commission of the offence.
- (5) A person may be found guilty of aiding, abetting, counselling or procuring the commission of an offence even if the principal offender has not been prosecuted or has not been found guilty.

Innocent agency

11.3 A person who:

- (a) has, in relation to each physical element of an offence, a fault element applicable to that physical element; and
- (b) procures conduct of another person that (whether or not together with the conduct of the procurer) would have constituted an offence on the part of the procurer if the procurer had engaged in it;

is taken to have committed that offence and is punishable accordingly.

Incitement

- 11.4 (1) A person who urges the commission of an offence is guilty of the offence of incitement.
- (2) For the person to be guilty, the person must intend that the offence incited be committed.
- (3) A person may be found guilty even if committing the offence incited is impossible.

Appendix 1

- (4) Any defences, procedures, limitations or qualifying provisions that apply to an offence apply also to the offence of incitement in respect of that offence.
- (5) It is not an offence to incite the commission of an offence against section 11.1 (attempt), this section or section 11.5 (conspiracy).

Maximum penalty:

- (a) if the offence incited is punishable by life imprisonment - imprisonment for 10 years; or
- (b) if the offence incited is punishable by imprisonment for 14 years or more, but is not punishable by life imprisonment - imprisonment for 7 years; or
- (c) if the offence incited is punishable by imprisonment for 10 years or more, but is not punishable by imprisonment for 14 years or more - imprisonment for 5 years; or
- (d) if the offence is otherwise punishable by imprisonment - imprisonment for 3 years or for the maximum term of imprisonment for the offence incited, whichever is the lesser; or
- (e) if the offence incited is not punishable by imprisonment - the number of penalty units equal to the maximum number of penalty units applicable to the offence incited.

Note: Under section 4D of the Crimes Act 1914, these penalties are only maximum penalties. Subsection 4B (2) of that Act allows a court to impose an appropriate fine instead of, or in addition to, a term of imprisonment. If a body corporate is convicted of the offence, subsection 4B (3) of that Act allows a court to impose a fine of an amount not greater than 5 times the maximum fine that the court could impose on an individual convicted of the same offence. Penalty units are defined in section 4AA of that Act.

[*Drafting note:* The note will have to be adapted to suit the relevant jurisdiction.]

Conspiracy

- 11.5 (1) A person who conspires with another person to commit an offence punishable by imprisonment for more than 12 months, or by a fine of 200 penalty units or more, is guilty of the offence of conspiracy to commit that offence and is punishable as if the offence to which the conspiracy relates had been committed.

Note: Penalty units are defined in section 4AA of the Crimes Act 1914.

[*Drafting note:* The note will have to be adapted to suit the relevant jurisdiction.]

- (2) For the person to be guilty:
 - (a) the person must have entered into an agreement with one or more other persons; and
 - (b) the person and at least one other party to the agreement must have intended that an offence would be committed pursuant to the agreement; and
 - (c) the person or at least one other party to the agreement must have committed an overt act pursuant to the agreement.
- (3) A person may be found guilty of conspiracy to commit an offence even if:
 - (a) committing the offence is impossible; or
 - (b) the only other party to the agreement is a body corporate; or
 - (c) each other party to the agreement is at least one of the following:
 - (i) a person who is not criminally responsible;
 - (ii) a person for whose benefit or protection the offence exists; or
 - (d) subject to paragraph (4)(a), all other parties to the agreement have been acquitted of the conspiracy.
- (4) A person cannot be found guilty of conspiracy to commit an offence if:
 - (a) all other parties to the agreement have been acquitted of the conspiracy and a finding of guilt would be inconsistent with their acquittal; or
 - (b) he or she is a person for whose benefit or protection the offence exists.
- (5) A person cannot be found guilty of conspiracy to commit an offence if, before the commission of an overt act pursuant to the agreement, the person:
 - (a) withdrew from the agreement; and
 - (b) took all reasonable steps to prevent the commission of the offence.
- (6) A court may dismiss a charge of conspiracy if it thinks that the interests of justice require it to do so.

- (7) Any defences, procedures, limitations or qualifying provisions that apply to an offence apply also to the offence of conspiracy to commit that offence.
- (8) Proceedings for an offence of conspiracy must not be commenced without the consent of the Director of Public Prosecutions. However, a person may be arrested for, charged with, or remanded in custody or on bail in connection with, an offence of conspiracy before the necessary consent has been given.

References in Acts to offences

- 11.6 (1) A reference in an Act to an offence against an Act (including this Code) includes a reference to an offence against section 11.1 (attempt), 11.4 (incitement) or 11.5 (conspiracy) of this Code that relates to such an offence.
- (2) A reference in an Act (including this Code) to a particular offence includes a reference to an offence against section 11.1 (attempt), 11.4 (incitement) or 11.5 (conspiracy) of this Code that relates to that particular offence.
 - (3) Subsection (1) or (2) does not apply if an Act is expressly or impliedly to the contrary effect.

Note: Sections 11.2 (complicity and common purpose) and 11.3 (innocent agency) of this Code operate as extensions of principal offences and are therefore not referred to in this section.

PART 2.5 - CORPORATE CRIMINAL RESPONSIBILITY

Division 12

General principles

- 12.1 (1) This Code applies to bodies corporate in the same way as it applies to individuals. It so applies with such modifications as are set out in this Part, and with such other modifications as are made necessary by the fact that criminal liability is being imposed on bodies corporate rather than individuals.
- (2) A body corporate may be found guilty of any offence, including one punishable by imprisonment.

Note: Section 4B of the Crimes Act 1914 enables a fine to be imposed for offences that only specify imprisonment as a penalty.

[*Drafting note:* The note will have to be adapted to suit the relevant jurisdiction.]

Physical elements

- 12.2 If a physical element of an offence is committed by an employee, agent or officer of a body corporate acting within the actual or apparent scope of his or her employment, or within his or her actual or apparent authority, the physical element must also be attributed to the body corporate.

Fault elements other than negligence

- 12.3 (1) If intention, knowledge or recklessness is a fault element in relation to a physical element of an offence, that fault element must be attributed to a body corporate that expressly, tacitly or impliedly authorised or permitted the commission of the offence.
- (2) The means by which such an authorisation or permission may be established include:
- (a) proving that the body corporate's board of directors intentionally, knowingly or recklessly carried out the relevant conduct, or expressly, tacitly or impliedly authorised or permitted the commission of the offence; or
 - (b) proving that a high managerial agent of the body corporate intentionally, knowingly or recklessly engaged in the relevant conduct, or expressly, tacitly or impliedly authorised or permitted the commission of the offence; or
 - (c) proving that a corporate culture existed within the body corporate that directed, encouraged, tolerated or led to non-compliance with the relevant provision; or
 - (d) proving that the body corporate failed to create and maintain a corporate culture that required compliance with the relevant provision.
- (3) Paragraph (2) (b) does not apply if the body corporate proves that it exercised due diligence to prevent the conduct, or the authorisation or permission.
- (4) Factors relevant to the application of paragraph (2) (c) or (d) include:
- (a) whether authority to commit an offence of the same or a similar character had been given by a high managerial agent of the body corporate; and
 - (b) whether the employee, agent or officer of the body corporate who committed the offence believed on reasonable grounds, or entertained a reasonable expectation, that a high

managerial agent of the body corporate would have authorised or permitted the commission of the offence.

- (5) If recklessness is not a fault element in relation to a physical element of an offence, subsection (2) does not enable the fault element to be proved by proving that the board of directors, or a high managerial agent, of the body corporate recklessly engaged in the conduct or recklessly authorised or permitted the commission of the offence.
- (6) In this section:
 - “**board of directors**” means the body (by whatever name called) exercising the executive authority of the body corporate;
 - “**corporate culture**” means an attitude, policy, rule, course of conduct or practice existing within the body corporate generally or in the part of the body corporate in which the relevant activities takes place;
 - “**high managerial agent**” means an employee, agent or officer of the body corporate with duties of such responsibility that his or her conduct may fairly be assumed to represent the body corporate’s policy.

Negligence

- 12.4 (1) The test of negligence for a body corporate is that set out in section 5.5.
- (2) If:
 - (a) negligence is a fault element in relation to a physical element of an offence; and
 - (b) no individual employee, agent or officer of the body corporate has that fault element;that fault element may exist on the part of the body corporate if the body corporate’s conduct is negligent when viewed as a whole (that is, by aggregating the conduct of any number of its employees, agents or officers).
- (3) Negligence may be evidenced by the fact that the prohibited conduct was substantially attributable to:
 - (a) inadequate corporate management, control or supervision of the conduct of one or more of its employees, agents or officers; or

- (b) failure to provide adequate systems or conveying relevant information to relevant persons in the body corporate.

Mistake of fact (strict liability)

- 12.5 (1) A body corporate can only rely on section 9.2 (mistake of fact (strict liability)) in respect of conduct that would, apart from this section, constitute an offence on its part if:
- (a) the employee, agent or officer of the body corporate who carried out the conduct was under a mistaken but reasonable belief about facts that, had they existed, would have meant that the conduct would not have constituted an offence; and
 - (b) the body corporate proves that it exercised due diligence to prevent the conduct.
- (2) A failure to exercise due diligence may be evidenced by the fact that the prohibited conduct was substantially attributable to:
- (a) inadequate corporate management, control or supervision of the conduct of one or more of its employees, agents or officers; or
 - (b) failure to provide adequate systems for conveying relevant information to relevant persons in the body corporate.

Intervening conduct or event

- 12.6 A body corporate cannot rely on section 10.1 (intervening conduct or event) in respect of a physical element of an offence brought about by another person if the other person is an employee, agent or officer of the body corporate.

PART 2.6 - PROOF OF CRIMINAL RESPONSIBILITY**Division 13****Legal burden of proof prosecution**

- 13.1 (1) The prosecution bears a legal burden of proving every element of an offence relevant to the guilt of the person charged.

Note: See section 3.2 on what elements are relevant to a person's guilt.

- (2) The prosecution also bears a legal burden of disproving any matter in relation to which the defendant has discharged an evidential burden of proof imposed on the defendant.

- (3) In this Code:
“**legal burden**”, in relation to a matter, means the burden of proving the existence of the matter.

Standard of proof prosecution

- 13.2 (1) A legal burden of proof on the prosecution must be discharged beyond reasonable doubt.
- (2) Subsection (1) does not apply if the law creating the offence specifies a different standard of proof.

Evidential burden of proof - defence

- 13.3 (1) Subject to section 13.4, a burden of proof that a law imposes on a defendant is an evidential burden only.
- (2) A defendant who wishes to deny criminal responsibility by relying on a provision of Part 2.3 (other than section 7.3) bears an evidential burden in relation to that matter.
- (3) A defendant who wishes to rely on any exception, exemption, excuse, qualification or justification provided by the law creating an offence bears an evidential burden in relation to that matter. The exception, exemption, excuse, qualification or justification need not accompany the description of the offence.
- (4) The defendant no longer bears the evidential burden in relation to a matter if evidence sufficient to discharge the burden is adduced by the prosecution or by the court.
- (5) The question whether an evidential burden has been discharged is one of law.
- (6) In this Code:
“**evidential burden**”, in relation to a matter, means the burden of adducing or pointing to evidence that suggests a reasonable possibility that the matter exists or does not exist.

Legal burden of proof - defence

- 13.4 A burden of proof that a law imposes on the defendant is a legal burden if and only if the law expressly:
- (a) specifies that the burden of proof in relation to the matter in question is a legal burden; or
- (b) requires the defendant to prove the matter; or
- (c) creates a presumption that the matter exists unless the contrary is proved.

Standard of proof - defence

- 13.5 A legal burden of proof on the defendant must be discharged on the balance of probabilities.

Use of averments

- 13.6 A law that allows the prosecution to make an averment is taken not to allow the prosecution:
- (a) to aver any fault element of an offence; or
 - (b) to make an averment in prosecuting for an offence that is directly punishable by imprisonment.

Part 2.7 - Geographical jurisdiction**2.7.1 Application and effect of Part**

- (1) This Part applies to all offences.
- (2) This Part extends the application of a law of this State/Territory that creates an offence beyond the territorial limits of this State/Territory if there is the nexus required by this Part between this State/Territory and the offence.
- (3) If the law that creates an offence makes provision with respect to any geographical consideration concerning the offence, that provision prevails over any inconsistent provision of this Part.

Note: Examples of special provisions made by the law creating an offence are as follows:

Part 8.1 (offences relating to contamination of goods) -see section 8.1.5;
Part 9.1 (offences relating to slavery and sexual servitude) - see section 9.1.8; Part 5.1 (offences relating to stalking) - see section 5.1.22;
Part 5.1 (offences relating to genital mutilation) - see section 5.1.35;
Chapter 5.2 (offence relating to persistent sexual abuse) - see section 5.2.14.

2.7.2 Interpretation

- (1) For the purposes of this Part, the necessary geographical nexus is the nexus required by section 2.7.3.
- (2) For the purposes of this Part, the place in which an offence is committed is the place in which the physical elements of the offence occur.
- (3) For the purposes of this Part, the place in which an offence has an

effect includes:

- (a) any place whose peace, welfare or good government is threatened by the offence; and
 - (b) any place in which the offence would have an effect (or would cause such a threat) if the criminal activity concerned were carried out.
- (4) A reference in this Part to this State/Territory includes a reference to the coastal waters of this State/Territory in which the criminal laws of this State/Territory apply by virtue of the [here insert relevant Act of this State/Territory].

2.7.3 Extension of offences if there is a geographical nexus

- (1) If:
- (a) all elements necessary to constitute an offence against a law of this State/Territory exist (disregarding geographical considerations); and
 - (b) a geographical nexus exists between this State/Territory 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 this State/Territory and an offence if:
- (a) the offence is committed wholly or partly in this State/Territory (whether or not the offence has any effect in this State/Territory); or
 - (b) the offence is committed wholly outside this State/Territory, but the offence has an effect in this State/Territory.

2.7.4 Provisions relating to double criminality

- (1) This Part applies to an offence that is committed partly in this State/Territory and partly in another place outside this State/Territory, irrespective of whether it is also an offence in that other place.
- (2) This Part applies to an offence that is committed wholly in a place outside this State/Territory only if:
- (a) it is also an offence in that place; or
 - (b) it is not also an offence in that place, but the trier of fact is

satisfied that the offence constitutes such a threat to the peace, welfare or good government of this State/Territory that the offence warrants criminal punishment in this State/Territory.

2.7.5 Procedural and other provisions

- (1) The existence of the necessary geographical nexus for an offence will be presumed and the presumption is conclusive unless rebutted under subsection (2).
- (2) If a person charged with an offence disputes the existence of the necessary geographical nexus, the court will proceed with the trial of the offence in the usual way. If, at the conclusion of the trial, the trier of fact is satisfied on the balance of probabilities that the necessary geographical nexus does not exist, it must (subject to subsection (3)) make or return a finding to that effect and the charge will be dismissed.
- (3) If the trier of fact would, disregarding any geographical considerations, find the person not guilty of the offence, it must make or return a finding of not guilty. The trier of fact must make or return a finding of not guilty on the grounds of mental impairment in any such case if they were the only grounds on which the trier of fact would have found the person not guilty of the offence.
- (4) This section also applies to any alternative verdict available by law to the trier of fact in respect of another offence with which the person was not charged. A finding of guilt may be made or returned in any such case, unless the trier of fact is satisfied on the balance of probabilities that the necessary geographical nexus for that other offence does not exist.
- (5) The issue of whether the necessary geographical nexus exists must, if raised before the trial, be reserved for consideration at the trial.
- (6) A power or authority exercisable on reasonable suspicion or belief that an offence has been committed may be exercised in this State/Territory if the person in whom the power or authority is vested suspects on reasonable grounds or believes that the elements necessary to constitute the offence exist (whether or not the person suspects or believes or has any ground to suspect or believe that the necessary geographical nexus with this State/Territory exists).

Model Criminal Code - Chapter 4

Property damage and computer offences

Part 4.1 - Property damage offences

Division 1 - Definitions

4.1.1 Property

In this Part:

property means any real or personal property of a tangible nature, including:

- (a) a wild creature that is tamed or ordinarily kept in captivity or that is reduced (or in the course of being reduced) into the possession of a person, and
- (b) any organ or part of a human body and any blood, ova, semen or other substance extracted from the human body.

4.1.2 Damage to property

For the purposes of this Part, *damage* to property includes:

- (a) destroying the property, or
- (b) causing the physical loss of the property by interfering with the property (including by removing any restraint over the property or abandoning the property), or
- (c) causing any loss of a use or function of the property by interfering with the property, or
- (d) defacing the property, or
- (e) in the case of a document—obliterating or rendering illegible the whole or any part of the document, or
- (f) in the case of an animal—harming or killing the animal, or
- (g) in the case of a plant or other thing forming part of land—severing it from the land.

4.1.3 Person to whom property belongs

- (1) For the purposes of this Part, property *belongs* to any person having possession or control of it, or having in it any proprietary right or interest (not being an equitable interest arising only from an agreement to transfer or grant an interest or from a constructive trust).
- (2) If property is subject to a trust, the persons to whom it belongs include any person having a right to enforce the trust.
- (3) If property belongs to 2 or more persons, a reference in this Part to the person to whom the property belongs is a reference to all those persons.

4.1.4 Threats

For the purposes of this Part:

- (a) a threat may be made by any conduct, and may be explicit or implicit and conditional or unconditional, and
- (b) a threat to a person includes a threat to a group of persons, and
- (c) fear that a threat will be carried out includes apprehension that it will be carried out.

4.1.5 Causing damage or other result

For the purpose of an offence under this Part, a person causes damage or any other result if the person's conduct substantially contributes to the damage or other result.

*Division 2 - Offences***4.1.6 Damaging property**

- (1) A person who:
 - (a) causes damage to property belonging to another person, and
 - (b) intends to cause or is reckless as to causing, damage to that or any other such property,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 4.2.5 (Unauthorised modification of data to cause impairment), or

- (b) an offence against section 4.2.6 (Unauthorised impairment of electronic communications).

Note. Section 4.1.11 provides a defence for persons who damage property with consent. The defence applies to other offences against this Part other than sabotage.

4.1.7 Arson

- (1) A person who:

- (a) causes damage to a building or conveyance by means of fire or explosive, and
- (b) intends to cause or is reckless as to causing, damage to that or any other building or conveyance,

is guilty of an offence.

Maximum penalty: Imprisonment for 15 years.

- (2) A person who:

- (a) makes to another person a threat to damage any building or conveyance belonging to that other person or a third person by means of fire or explosives, and
- (b) intends that other person to fear that the threat will be carried out or is reckless as to causing that other person to fear that the threat will be carried out,

is guilty of an offence.

Maximum penalty: Imprisonment for 7 years.

- (3) In the prosecution of an offence against subsection (2) it is not necessary to prove that the person threatened actually feared that the threat would be carried out.

- (4) In this section:

building includes:

- (a) part of a building, or
- (b) any structure (whether or not moveable) that is used, designed or adapted for residential purposes.

conveyance means motor vehicle, motorised vessel or aircraft.

4.1.8 Bushfires

- (1) A person:
- (a) who causes a fire, and
 - (b) who intends or is reckless as to causing a fire, and
 - (c) who is reckless as to the spread of the fire to vegetation on property belonging to another,

is guilty of an offence.

Maximum penalty: Imprisonment for 15 years.

- (2) In this section:

causing a fire includes:

- (a) lighting a fire, or
- (b) maintaining a fire, or
- (c) failing to contain a fire, except where the fire was lit by another person or the fire is beyond the control of the person who lit the fire.

spread of a fire means spread of a fire beyond the capacity of the person who caused the fire to extinguish it.

4.1.9 Threat to cause property damage—fear of death or serious harm

- (1) A person who:
- (a) makes to another person a threat to damage property, and
 - (b) is reckless as to causing that other person to fear that the carrying out of the threat will kill or cause serious harm to that other person or a third person,

is guilty of an offence.

Maximum penalty: Imprisonment for 7 years.

- (2) In the prosecution of an offence against this section it is not necessary to prove that the person threatened actually feared that the threat would be carried out.
- (3) In this section, *serious harm* has the same meaning as it has in Part 5.1.

Summary Offence

Threat to cause property damage

- (1) A person who:
 - (a) makes to another person a threat to damage property belonging to that other person or a third person, and
 - (b) intends that other person to fear that the threat will be carried out,is guilty of an offence.
Maximum penalty: Imprisonment for 2 years.
- (2) In the prosecution of an offence against this section it is not necessary to prove that the person threatened actually feared that the threat would be carried out.

4.1.10 Possession of thing with intent to damage property

- (1) A person who possesses any thing, with the intention that the person or another person will use it to damage property belonging to another, is guilty of an offence.
Maximum penalty: Imprisonment for 3 years.
- (2) In this section:
possession of a thing includes:
 - (a) having control over the disposition of the thing (whether or not the thing is in the custody of the person), or
 - (b) having joint possession of the thing.

Summary Offence

Poaching of wild creatures

- (1) A person who intentionally takes, kills or injures any wild creature on land belonging to another is guilty of an offence.
Maximum penalty: Imprisonment for 2 years.
- (2) A person is not criminally responsible for an offence against this section if:
 - (a) the person engaged in conduct constituting the offence with the consent of the owner or occupier of the land;

- (b) at the time of the conduct constituting the offence, the person believed that he or she had a right or interest in the wild creatures which authorised the person to engage in that conduct; or
 - (c) the person's conduct constituting the offence is justified or excused by any Act or other law.
- (3) In this section, *wild creature* means any live bird, mammal, fish (including crustacean) or amphibian that is not tamed or ordinarily kept in captivity or not reduced (or in the course of being reduced) into the possession of a person.

Division 3 - Defences

4.1.11 Consent

A person is not criminally responsible for an offence against this Part if, at the time of the conduct constituting the offence:

- (a) the person entitled to consent to the damage to the property concerned had so consented, or
- (b) he or she believed that the person whom he or she believed was entitled to consent to the damage to the property concerned had so consented, or
- (c) he or she believed that that person would have so consented if that person had known about the damage to the property and its circumstances.

4.1.12 Claim of right

- (1) A person is not criminally responsible for an offence against this Part if, at the time of the conduct constituting the offence, the person believed that he or she had a right or interest in the property concerned which authorised the person to engage in that conduct.
- (2) In this section, a right or interest in property includes a right or privilege in or over land or waters, whether created by grant, licence or otherwise.

4.1.13 Self-defence

To avoid doubt, section 10.4 (Self-defence) applies to an offence against this Part.

Part 4.2 - Computer offences

4.2.1 General definitions

In this Part:

Computer offence means:

- (a) an offence against this Part; or
- (b) conduct in another jurisdiction that is an offence against this Part if the conduct occurred in this jurisdiction

data includes:

- (a) information in any form, or
- (b) any program (or part of a program).

data held in a computer includes:

- (a) data entered or copied into the computer, 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.

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.

4.2.2 Meaning of access to data, modification of data and impairment of electronic communication

(1) In this Part, *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.

(2) In this Part, *modification* of data held in a computer or data storage device means:

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

- (b) an addition to the data.
- (3) In this Part, *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.
- (4) A reference in this Part to any such access, modification or impairment is limited to access, modification or impairment caused (whether directly or indirectly) by the execution of a function of a computer.

4.2.3 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.

4.2.4 Unauthorised access, modification or impairment with intention to commit serious offence

- (1) A person who causes any unauthorised computer function:
 - (a) knowing it is unauthorised, and
 - (b) with the intention of committing a serious offence, or facilitating the commission of a serious 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 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 communications to or from any computer.
- (3) For the purposes of this section, a *serious offence* is:
- (a) an offence in this jurisdiction punishable by imprisonment for a period of 5 years or more, or
 - (b) an offence in any other jurisdiction, being an offence so punishable if committed in this jurisdiction.
- (4) A person may be found guilty of an offence against this section:
- (a) even if committing the serious offence concerned is impossible, or
 - (b) whether the serious offence is to be committed at the time of the unauthorised conduct or at a later time.
- (6) It is not an offence to attempt to commit an offence against this section.

4.2.5 Unauthorised modification of data 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 4.1.6 (Damaging property), or
 - (b) an offence against section 4.2.6 (Unauthorised impairment of electronic communications).

4.2.6 Unauthorised impairment of electronic communication

- (1) A person who:
 - (a) causes any unauthorised impairment of electronic communications 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 4.1.6 (Damaging property), or
 - (b) an offence against section 4.2.5 (Unauthorised modification of data to cause impairment).

Summary Offence**Unauthorised access to or modification of restricted data held in computer**

- (1) A person who:
 - (a) causes any unauthorised access to or modification of restricted data held in a computer, and
 - (b) knows that the access or modification is unauthorised, and
 - (c) intends to cause that access or modification,is guilty of an offence.
Maximum penalty: Imprisonment for 2 years.
- (2) 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.

Summary Offence

Unauthorised impairment of data held in computer disc, credit card etc

- (1) A person who:
 - (a) causes any unauthorised impairment of the reliability, security or operation of any data held on a computer disc, credit card or other device used to store data by electronic means, and
 - (b) knows that impairment is unauthorised, and
 - (c) intends to cause that impairment,is guilty of an offence.
maximum penalty: Imprisonment for 2 years.
- (2) 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.

4.2.7 Possession of data with intent to commit computer offence

- (1) A person who is in possession or control of data:
 - (a) with the intention of committing a computer offence, or
 - (b) with the intention of facilitating the commission of a 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 computer offence concerned is impossible.
- (4) It is not an offence to attempt to commit an offence against this section.

4.2.8 Producing, supplying or obtaining data with intent to commit computer offence

- (1) A person who produces, supplies or obtains data:
 - (a) with the intention of committing a computer offence, or
 - (b) with the intention of facilitating the commission of a 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, *produce, 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 computer offence concerned is impossible.

Part 4.3 - Sabotage

4.3.1 General definitions

In this Part:

property offence means:

- (a) an offence against Part 4.1, or
- (b) conduct in another jurisdiction that is an offence in that jurisdiction and that would constitute an offence against Part 4.1 if the conduct occurred in this jurisdiction.

public facility means any of the following (whether publicly or privately owned):

- (a) government facilities, including premises used by government employees in connection with official duties,
- (b) public infrastructure facilities, including facilities providing water, sewerage, energy, fuel, communication or other services to the public,
- (c) public information systems, including systems used to

generate, send, receive, store or otherwise process electronic communications,

- (d) public transport facilities, including conveyances used to transport people or goods,
- (e) public places, including any premises, land or water open to the public.

unauthorised computer function means any of the following (within the meaning of Part 4.2):

- (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.

4.3.2 Meaning of damage to public facility

- (1) In this Part, *damage* a public facility means:
 - (a) cause damage to the facility or any part of the facility, or
 - (b) cause disruption to the use or operation of the facility.
- (2) For the purposes of an offence under this Part, a person causes any such damage or disruption if the person's conduct substantially contributes to the damage or disruption.

4.3.3 Sabotage

A person:

- (a) who damages a public facility by committing a property offence or by causing an unauthorised computer function, and
- (b) who intends to cause:
 - (i) major disruption to government functions, or
 - (ii) major disruption to the use of services by the public, or
 - (iii) major economic loss,

is guilty of an offence.

Maximum penalty: Imprisonment for 25 years.

4.3.4 Threaten sabotage

- (1) A person who:
 - (a) makes to another person a threat to damage a public facility by committing a property offence or by causing an unauthorised computer function, and
 - (b) intends that person to fear that the threat will be carried out and will cause:
 - (i) major disruption to government functions, or
 - (ii) major disruption to the use of services by the public, or
 - (iii) major economic loss,is guilty of an offence.
Maximum penalty: Imprisonment for 15 years.
- (2) In the prosecution of an offence against this section it is not necessary to prove that the person threatened actually feared that the threat would be carried out.
- (3) For the purposes of this section:
 - (a) a threat may be made by any conduct, and may be explicit or implicit and conditional or unconditional, and
 - (b) a threat to a person includes a threat to a group of persons, and
 - (c) fear that a threat will be carried out includes apprehension that it will be carried out.

Computer Misuse Act 1990 (UK)

An Act to make provision for securing computer material against unauthorised access or modification; and for connected purposes.

Be it enacted by the Queen's most Excellent Majesty, by and with the advice and consent of the Lords Spiritual and Temporal, and Commons, in this present Parliament assembled, and by the authority of the same, as follows:

Computer misuse offences

1. (1) A person is guilty of an offence if -
 - (a) he causes a computer to perform any function with intent to secure access to any program or data held in any computer;
 - (b) the access he intends to secure is unauthorised; and
 - (c) he knows at the time when he causes the computer to perform the function that that is the case.
 - (2) The intent a person has to have to commit an offence under this section need not be directed at -
 - (a) any particular program or data;
 - (b) a program or data of any particular kind; or
 - (c) a program or data held in any particular computer.
 - (3) A person guilty of an offence under this section shall be liable on summary conviction to imprisonment for a term not exceeding six months or to a fine not exceeding level 5 on the standard scale or to both.
2. (1) A person is guilty of an offence under this section if he commits an offence under section 1 above ("the unauthorised access offence") with intent -
 - (a) to commit an offence to which this section applies; or
 - (b) to facilitate the commission of such an offence (whether by himself or by any other person);and the offence he intends to commit or facilitate is referred to below in this section as the further offence.
 - (2) This section applies to offences -
 - (a) for which the sentence is fixed by law; or
 - (b) for which a person of twenty-one years of age or over (not previously convicted) may be sentenced to imprisonment for a term of five years (or, in England and Wales, might be

so sentenced but for the restrictions imposed by section 33 of the Magistrates' Courts Act 1980).

- (3) It is immaterial for the purposes of this section whether the further offence is to be committed on the same occasion as the unauthorised access offence or on any future occasion.
 - (4) A person may be guilty of an offence under this section even though the facts are such that the commission of the further offence is impossible.
 - (5) A person guilty of an offence under this section shall be liable -
 - (a) on summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or to both; and
 - (b) on conviction on indictment, to imprisonment for a term not exceeding five years or to a fine or to both.
3. (1) A person is guilty of an offence if -
- (a) he does any act which causes an unauthorised modification of the contents of any computer; and
 - (b) at the time when he does the act he has the requisite intent and the requisite knowledge.
- (2) For the purposes of subsection (1)(b) above the requisite intent is an intent to cause a modification of the contents of any computer and by so doing -
- (a) to impair the operation of any computer;
 - (b) to prevent or hinder access to any program or data held in any computer; or
 - (c) to impair the operation of any such program or the reliability of any such data.
- (3) The intent need not be directed at -
- (a) any particular computer;
 - (b) any particular program or data or a program or data of any particular kind; or
 - (c) any particular modification or a modification of any particular kind.

Appendix 3

- (4) For the purposes of subsection (1)(b) above the requisite knowledge is knowledge that any modification he intends to cause is unauthorised.
- (5) It is immaterial for the purposes of this section whether an unauthorised modification or any intended effect of it of a kind mentioned in subsection (2) above is, or is intended to be, permanent or merely temporary.
- (6) For the purposes of the Criminal Damage Act 1971 a modification of the contents of a computer shall not be regarded as damaging any computer or computer storage medium unless its effect on that computer or computer storage medium impairs its physical condition.
- (7) A person guilty of an offence under this section shall be liable -
 - (a) on summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or to both; and
 - (b) on conviction on indictment, to imprisonment for a term not exceeding five years or to a fine or to both.

Jurisdiction

4. (1) Except as provided below in this section, it is immaterial for the purposes of any offence under section 1 or 3 above
 - (a) whether any act or other event proof of which is required for conviction of the offence occurred in the home country concerned; or
 - (b) whether the accused was in the home country concerned at the time of any such act or event.
- (2) Subject to subsection (3) below, in the case of such an offence at least one significant link with domestic jurisdiction must exist in the circumstances of the case for the offence to be committed.
- (3) There is no need for any such link to exist for the commission of an offence under section 1 above to be established in proof of an allegation to that effect in proceedings for an offence under section 2 above.
- (4) Subject to section 8 below, where -
 - (a) any such link does in fact exist in the case of an offence under section 1 above; and

- (b) commission of that offence is alleged in proceedings for an offence under section 2 above;

section 2 above shall apply as if anything, the accused intended to do or facilitate in any place outside the home country concerned which would be an offence to which section 2 applies if it took place in the home country concerned were the offence in question.

- (5) This section is without prejudice to any jurisdiction exercisable by a court in Scotland apart from this section.
- (6) References in this Act to the home country concerned are references -
 - (a) in the application of this Act to England and Wales, to England and Wales;
 - (b) in the application of this Act to Scotland, to Scotland; and
 - (c) in the application of this Act to Northern Ireland, to Northern Ireland.

- 5. (1) The following provisions of this section apply for the interpretation of section 4 above.
 - (2) In relation to an offence under section 1, either of the following is a significant link with domestic jurisdiction -
 - (a) that the accused was in the home country concerned at the time when he did the act which caused the computer to perform the function; or
 - (b) that any computer containing any program or data to which the accused secured or intended to secure unauthorised access by doing that act was in the home country concerned at that time.
 - (3) In relation to an offence under section 3, either of the following is a significant link with domestic jurisdiction -
 - (a) that the accused was in the home country concerned at the time when he did the act which caused the unauthorised modification; or
 - (b) that the unauthorised modification took place in the home country concerned.
- 6. (1) On a charge of conspiracy to commit an offence under this Act the following questions are immaterial to the accused's guilt -
 - (a) the question where any person became a party to the conspiracy; and

Appendix 3

- (b) the question whether any act, omission or other event occurred in the home country concerned.
 - (2) On a charge of attempting to commit an offence under section 3 above the following questions are immaterial to the accused's guilt -
 - (a) the question where the attempt was made; and
 - (b) the question whether it had an effect in the home country concerned.
 - (3) On a charge of incitement to commit an offence under this Act the question where the incitement took place is immaterial to the accused's guilt.
 - (4) This section does not extend to Scotland.
7. (1) The following subsections shall be inserted after subsection (1) of section 1 of the Criminal Law Act 1977 -
- “(1A) Subject to section 8 of the Computer Misuse Act 1990 (relevance of external law), if this subsection applies to an agreement, this Part of this Act has effect in relation to it as it has effect in relation to an agreement falling within subsection (1) above.
- (1B) Subsection (1A) above applies to an agreement if -
- (a) a party to it, or a party's agent, did anything in England and Wales in relation to it before its formation; or
 - (b) a party to it became a party in England and Wales (by joining it either in person or through an agent); or
 - (c) a party to it, or a party's agent, did or omitted anything in England and Wales in pursuance of it;
- and the agreement would fall within subsection (1) above as an agreement relating to the commission of a computer misuse offence but for the fact that the offence would not be an offence triable in England and Wales if committed in accordance with the parties' intentions.”.
- (2) The following subsections shall be inserted after subsection (4) of that section -
- “(5) In the application of this Part of this Act to an agreement to which subsection (1A) above applies any reference to an offence shall be read as a reference to what would be the computer misuse offence in question but for the fact that it is not an offence triable in England and Wales.

- (6) In this section “computer misuse offence” means an offence under the Computer Misuse Act 1990.”
- (3) The following subsections shall be inserted after section 1(1) of the Criminal Attempts Act 1981 -
- “(1A) Subject to section 8 of the Computer Misuse Act 1990 (relevance of external law), if this subsection applies to an act, what the person doing it had in view shall be treated as an offence to which this section applies.
- (1B) Subsection (1A) above applies to an act if -
- (a) it is done in England and Wales; and
 - (b) it would fall within subsection (1) above as more than merely preparatory to the commission of an offence under section 3 of the Computer Misuse Act 1990 but for the fact that the offence, if completed, would not be an offence triable in England and Wales.”
- (4) Subject to section 8 below, if any act done by a person in England and Wales would amount to the offence of incitement to commit an offence under this Act but for the fact that what he had in view would not be an offence triable in England and Wales -
- (a) what he had in view shall be treated as an offence under this Act for the purposes of any charge of incitement brought in respect of that act; and
 - (b) any such charge shall accordingly be triable in England and Wales.
8. (1) A person is guilty of an offence triable by virtue of section 4(4) above only if what he intended to do or facilitate would involve the commission of an offence under the law in force where the whole or any part of it was intended to take place.
- (2) A person is guilty of an offence triable by virtue of section 1(1A) of the Criminal Law Act 1977 only if the pursuit of the agreed course of conduct would at some stage involve -
- (a) an act or omission by one or more of the parties; or
 - (b) the happening of some other event;
- constituting an offence under the law in force where the act, omission or other event was intended to take place.
- (3) A person is guilty of an offence triable by virtue of section 1(1A) of the Criminal Attempts Act 1981 or by virtue of section 7(4)

Appendix 3

above only if what he had in view would involve the commission of an offence under the law in force where the whole or any part of it was intended to take place.

- (4) Conduct punishable under the law in force in any place is an offence under that law for the purposes of this section, however it is described in that law.
 - (5) Subject to subsection (7) below, a condition specified in any of subsections (1) to (3) above shall be taken to be satisfied unless not later than rules of court may provide the defence serve on the prosecution a notice -
 - (a) stating that, on the facts as alleged with respect to the relevant conduct, the condition is not in their opinion satisfied;
 - (b) showing their grounds for that opinion; and
 - (c) requiring the prosecution to show that it is satisfied.
 - (6) In subsection (5) above “the relevant conduct” means -
 - (a) where the condition in subsection (1) above is in question, what the accused intended to do or facilitate;
 - (b) where the condition in subsection (2) above is in question, the agreed course of conduct; and
 - (c) where the condition in subsection (3) above is in question, what the accused had in view.
 - (7) The court, if it thinks fit, may permit the defence to require the prosecution to show that the condition is satisfied without the prior service of a notice under subsection (5) above.
 - (8) If by virtue of subsection (7) above a court of solemn jurisdiction in Scotland permits the defence to require the prosecution to show that the condition is satisfied, it shall be competent for the prosecution to examine any witness or to put in evidence any production not included in lists lodged by it.
 - (9) In the Crown Court the question whether the condition is satisfied shall be decided by the judge alone.
 - (10) In the High Court of Justiciary and in the sheriff court the question whether the condition is satisfied shall be decided by the judge or, as the case may be, the sheriff alone.
9. (1) In any proceedings brought in England and Wales in respect of any offence to which this section applies it is immaterial to guilt whether or not the accused was a British citizen at the time of any

act, omission or other event proof of which is required for conviction of the offence.

- (2) This section applies to the following offences -
 - (a) any offence under this Act;
 - (b) conspiracy to commit an offence under this Act;
 - (c) any attempt to commit an offence under section 3 above; and
 - (d) incitement to commit an offence under this Act.

Miscellaneous and general

10. Section 1(1) above has effect without prejudice to the operation -
 - (a) in England and Wales of any enactment relating to powers of inspection, search or seizure; and
 - (b) in Scotland of any enactment or rule of law relating to powers of examination, search or seizure.
11. (1) A magistrates' court shall have jurisdiction to try an offence under section 1 above if -
 - (a) the accused was within its commission area at the time when he did the act which caused the computer to perform the function; or
 - (b) any computer containing any program or data to which the accused secured or intended to secure unauthorised access by doing that act was in its commission area at that time.
- (2) Subject to subsection (3) below, proceedings for an offence under section 1 above may be brought within a period of six months from the date on which evidence sufficient in the opinion of the prosecutor to warrant the proceedings came to his knowledge.
- (3) No such proceedings shall be brought by virtue of this section more than three years after the commission of the offence.
- (4) For the purposes of this section, a certificate signed by or on behalf of the prosecutor and stating the date on which evidence sufficient in his opinion to warrant the proceedings came to his knowledge shall be conclusive evidence of that fact.
- (5) A certificate stating that matter and purporting to be so signed shall be deemed to be so signed unless the contrary is proved.
- (6) In this section "commission area" has the same meaning as in the Justices of the Peace Act 1979.

Appendix 3

- (7) This section does not extend to Scotland.
12. (1) If on the trial on indictment of a person charged with -
- (a) an offence under section 2 above; or
 - (b) an offence under section 3 above or any attempt to commit such an offence;
- the jury find him not guilty of the offence charged, they may find him guilty of an offence under section 1 above if on the facts shown he could have been found guilty of that offence in proceedings for that offence brought before the expiry of any time limit under section 11 above applicable to such proceedings.
- (2) The Crown Court shall have the same powers and duties in relation to a person who is by virtue of this section convicted before it of an offence under section I above as a magistrates' court would have on convicting him of the offence.
- (3) This section is without prejudice to section 6(3) of the Criminal Law Act 1967 (conviction of alternative indictable offence on trial on indictment).
- (4) This section does not extend to Scotland.
13. (1) A sheriff shall have jurisdiction in respect of an offence under section I or 2 above if -
- (a) the accused was in the sheriffdom at the time when he did the act which caused the computer to perform the function; or
 - (b) any computer containing any program or data to which the accused secured or intended to secure unauthorised access by doing that act was in the sheriffdom at that time.
- (2) A sheriff shall have jurisdiction in respect of an offence under section 3 above if -
- (a) the accused was in the sheriffdom at the time when he did the act which caused the unauthorised modification; or
 - (b) the unauthorised modification took place in the sheriffdom.
- (3) Subject to subsection (4) below, summary proceedings for an offence under section 1, 2 or 3 above may be commenced within a period of six months from the date on which evidence sufficient in the opinion of the procurator fiscal to warrant proceedings came to his knowledge.

- (4) No such proceedings shall be commenced by virtue of this section more than three years after the commission of the offence.
 - (5) For the purposes of this section, a certificate signed by or on behalf of the procurator fiscal and stating the date on which evidence sufficient in his opinion to warrant the proceedings came to his knowledge shall be conclusive evidence of that fact.
 - (6) A certificate stating that matter and purporting to be so signed shall be deemed to be so signed unless the contrary is proved.
 - (7) Subsection (3) of section 331 of the Criminal Procedure (Scotland) Act 1975 (date of commencement of proceedings) shall apply for the purposes of this section as it applies for the purposes of that section.
 - (8) In proceedings in which a person is charged with an offence under section 2 or 3 above and is found not guilty or is acquitted of that charge, he may be found guilty of an offence under section 1 above if on the facts shown he could have been found guilty of that offence in proceedings for that offence commenced before the expiry of any time limit under this section applicable to such proceedings.
 - (9) Subsection (8) above shall apply whether or not an offence under section 1 above has been libelled in the complaint or indictment.
 - (10) A person found guilty of an offence under section 1 above by virtue of subsection (9) above shall be liable, in respect of that offence, only to the penalties set out in section 1.
 - (11) This section extends to Scotland only.
- 14.** (1) Where a circuit judge is satisfied by information on oath given by a constable that there are reasonable grounds for believing -
- (a) that an offence under section 1 above has been or is about to be committed in any premises; and
 - (b) that evidence that such an offence has been or is about to be committed is in those premises;
- he may issue a warrant authorising a constable to enter and search the premises, using such reasonable force as is necessary.
- (2) The power conferred by subsection (1) above does not extend to authorising a search for material of the kinds mentioned in section 9(2) of the Police and Criminal Evidence Act 1984 (privileged, excluded and special procedure material).
 - (3) A warrant under this section -

Appendix 3

- (a) may authorise persons to accompany any constable executing the warrant; and
 - (b) remains in force for twenty-eight days from the date of its issue.
 - (4) In executing a warrant issued under this section a constable may seize an article if he reasonably believes that it is evidence that an offence under section 1 above has been or is about to be committed.
 - (5) In this section “premises” includes land, buildings, movable structures, vehicles, vessels, aircraft and hovercraft.
 - (6) This section does not extend to Scotland.
- 15.** The offences to which an Order in Council under section 2 of the Extradition Act 1870 can apply shall include -
- (a) offences under section 2 or 3 above;
 - (b) any conspiracy to commit such an offence; and
 - (c) any attempt to commit an offence under section 3 above.
- 16.** (1) The following provisions of this section have effect for applying this Act in relation to Northern Ireland with the modifications there mentioned.
- (2) In section 2(2)(b) -
 - (a) the reference to England and Wales shall be read as a reference to Northern Ireland; and
 - (b) the reference to section 33 of the Magistrates’ Courts Act 1980 shall be read as a reference to Article 46(4) of the Magistrates’ Courts (Northern Ireland) Order 1981.
 - (3) The reference in section 3(6) to the Criminal Damage Act 1971 shall be read as a reference to the Criminal Damage (Northern Ireland) Order 1977.
 - (4) Subsections (5) to (7) below apply in substitution for subsections (1) to (3) of section 7; and any reference in subsection (4) of that section to England and Wales shall be read as a reference to Northern Ireland.
 - (5) The following paragraphs shall be inserted after paragraph (1) of Article 9 of the Criminal Attempts and Conspiracy (Northern Ireland) Order 1983 -
 - “(1A) Subject to section 8 of the Computer Misuse Act 1990 (relevance of external law), if this paragraph applies to an agreement, this

Part has effect in relation to it as it has effect in relation to an agreement falling within paragraph (1).

- (1B) Paragraph (1A) applies to an agreement if -
- (a) a party to it, or a party's agent, did anything in Northern Ireland in relation to it before its formation;
 - (b) a party to it became a party in Northern Ireland (by joining it either in person or through an agent); or
 - (c) a party to it, or a party's agent, did or omitted anything in Northern Ireland in pursuance of it;
- and the agreement would fall within paragraph (1) as an agreement relating to the commission of a computer misuse offence but for the fact that the offence would not be an offence triable in Northern Ireland if committed in accordance with the parties' intentions.”.
- (6) The following paragraph shall be inserted after paragraph (4) of that Article -
- “(5) In the application of this Part to an agreement to which paragraph (1A) applies any reference to an offence shall be read as a reference to what would be the computer misuse offence in question but for the fact that it is not an offence triable in Northern Ireland.
- (6) In this Article “computer misuse offence” means an offence under the Computer Misuse Act 1990.”.
- (7) The following paragraphs shall be inserted after Article 3(l) of that Order -
- “(1A) Subject to section 8 of the Computer Misuse Act 1990 (relevance of external law), if this paragraph applies to an act, what the person doing it had in view shall be treated as an offence to which this Article applies.
- (1B) Paragraph (1A) above applies to an act if -
- (a) it is done in Northern Ireland; and
 - (b) it would fall within paragraph (1) as more than merely preparatory to the commission of an offence under section 3 of the Computer Misuse Act 1990 but for the fact that the offence, if completed, would not be an offence triable in Northern Ireland.”.

(8) In section 8 -

 - (a) the reference in subsection (2) to section 1(1A) of the

Appendix 3

- Criminal Law Act 1977 shall be read as a reference to Article 9(1A) of that Order; and
- (b) the reference in subsection (3) to section 1(1A) of the Criminal Attempts Act 1981 shall be read as a reference to Article 3(1A) of that Order.
- (9) The references in sections 9(1) and 10 to England and Wales shall be read as references to Northern Ireland.
- (10) In section 11, for subsection (I) there shall be substituted -
- “(1) A magistrates’ court for a county division in Northern Ireland may hear and determine a complaint charging an offence under section 1 above or conduct a preliminary investigation or preliminary inquiry into an offence under that section if -
- (a) the accused was in that division at the time when he did the act which caused the computer to perform the function; or
 - (b) any computer containing any program or data to which the accused secured or intended to secure unauthorised access by doing that act was in that division at that time.”;
- and subsection (6) shall be omitted.
- (11) The reference in section 12(3) to section 6(3) of the Criminal Law Act 1967 shall be read as a reference to section 6(2) of the Criminal Law Act (Northern Ireland) 1967.
- (12) In section 14 -
- (a) the reference in subsection (1) to a circuit judge shall be read as a reference to a county court judge; and
 - (b) the reference in subsection (2) to section 9(2) of the Police and Criminal Evidence Act 1984 shall be read as a reference to Article 11(2) of the Police and Criminal Evidence (Northern Ireland) Order 1989.
17. (1) The following provisions of this section apply for the interpretation of this Act.
- (2) A person secures access to any program or data held in a computer if by causing a computer to perform any function he -
- (a) alters or erases the program or data;
 - (b) copies or moves it to any storage medium other than that in which it is held or to a different location in the storage medium in which it is held;

- (c) uses it; or
 - (d) has it output from the computer in which it is held (whether by having it displayed or in any other manner);
- and references to access to a program or data (and to an intent to secure such access) shall be read accordingly.
- (3) For the purposes of subsection (2)(c) above a person uses a program if the function he causes the computer to perform -
 - (a) causes the program to be executed; or
 - (b) is itself a function of the program.
 - (4) For the purposes of subsection (2)(d) above -
 - (a) a program is output if the instructions of which it consists are output; and
 - (b) the form in which any such instructions or any other data is output (and in particular whether or not it represents a form in which, in the case of instructions, they are capable of being executed or, in the case of data, it is capable of being processed by a computer) is immaterial.
 - (5) Access of any kind by any person to any program or data held in a computer is unauthorised if -
 - (a) he is not himself entitled to control access of the kind in question to the program or data; and
 - (b) he does not have consent to access by him of the kind in question to the program or data from any person who is so entitled.
 - (6) References to any program or data held in a computer include references to any program or data held in any removable storage medium which is for the time being in the computer; and a computer is to be regarded as containing any program or data held in any such medium.
 - (7) A modification of the contents of any computer takes place if, by the operation of any function of the computer concerned or any other computer -
 - (a) any program or data held in the computer concerned is altered or erased; or

Appendix 3

- (b) any program or data is added to its contents;
and any act which contributes towards causing such a modification shall be regarded as causing it.
 - (8) Such a modification is unauthorised if -
 - (a) the person whose act causes it is not himself entitled to determine whether the modification should be made; and
 - (b) he does not have consent to the modification from any person who is so entitled.
 - (9) References to the home country concerned shall be read in accordance with section 4(6) above.
 - (10) References to a program include references to part of a program.
- 18.**
- (1) This Act may be cited as the Computer Misuse Act 1990.
 - (2) This Act shall come into force at the end of the period of two months beginning with the day on which it is passed.
 - (3) An offence is not committed under this Act unless every act or other event proof of which is required for conviction of the offence takes place after this Act comes into force.

United Nations International Convention for the Suppression of Terrorist Bombings (52/164)

Date: 15 December 1997

Meeting: 72

Adopted without a vote

Report: A/52/653

The General Assembly,

Recalling its resolution 49/60 of 9 December 1994, by which it adopted the Declaration on Measures to Eliminate International Terrorism, and its resolution 51/210 of 17 December 1996,

Having considered the text of the draft convention for the suppression of terrorist bombings prepared by the Ad Hoc Committee established by General Assembly resolution 51/210 of 17 December 1996 (63) and the Working Group of the Sixth Committee,(64)

1. Adopts the text of the International Convention for the Suppression of Terrorist Bombings annexed to the present resolution and opens the instrument for signing at United Nations Headquarters from 12 January 1998 until 31 December 1999;
2. Urges all States to sign and ratify, accept or approve or to accede to the annexed Convention.

ANNEX**International Convention for the Suppression of Terrorist Bombings**

The States Parties to this Convention,

Having in mind the purposes and principles of the Charter of the United Nations concerning the maintenance of international peace and security and the promotion of good-neighbourliness and friendly relations and cooperation among States,

Deeply concerned about the worldwide escalation of acts of terrorism in all its forms and manifestations,

Recalling the Declaration on the Occasion of the Fiftieth Anniversary of the United Nations of 24 October 1995, (65)

Recalling also the Declaration on Measures to Eliminate International Terrorism, annexed to General Assembly resolution 49/60 of 9 December 1994, in which, inter alia, "the States Members of the United Nations solemnly reaffirm their unequivocal condemnation of all acts, methods and practices of terrorism as

Appendix 4

criminal and unjustifiable, wherever and by whomever committed, including those which jeopardize the friendly relations among States and peoples and threaten the territorial integrity and security of States”.

Noting that the Declaration also encouraged States “to review urgently the scope of the existing international legal provisions on the prevention, repression and elimination of terrorism in all its forms and manifestations, with the aim of ensuring that there is a comprehensive legal framework covering all aspects of the matter”,

Recalling further General Assembly resolution 51/210 of 17 December 1996 and the Declaration to Supplement the 1994 Declaration on Measures to Eliminate International Terrorism, annexed thereto,

Noting also that terrorist attacks by means of explosives or other lethal devices have become increasingly widespread,

Noting further that existing multilateral legal provisions do not adequately address these attacks,

Being convinced of the urgent need to enhance international cooperation between States in devising and adopting effective and practical measures for the prevention of such acts of terrorism, and for the prosecution and punishment of their perpetrators,

Considering that the occurrence of such acts is a matter of grave concern to the international community as a whole,

Noting that the activities of military forces of States are governed by rules of international law outside the framework of this Convention and that the exclusion of certain actions from the coverage of this Convention does not condone or make lawful otherwise unlawful acts, or preclude prosecution under other laws,

Have agreed as follows:

Article 1

For the purposes of this Convention:

1. “State or government facility” includes any permanent or temporary facility or conveyance that is used or occupied by representatives of a State, members of Government, the legislature or the judiciary or by officials or employees of a State or any other public authority or entity or by employees or officials of an intergovernmental organization in connection with their official duties.
2. “Infrastructure facility” means any publicly or privately owned facility providing or distributing services for the benefit of

the public, such as water, sewage, energy, fuel or communications.

3. “Explosive or other lethal device” means:
 - (a) An explosive or incendiary weapon or device that is designed, or has the capability, to cause death, serious bodily injury or substantial material damage; or
 - (b) A weapon or device that is designed, or has the capability, to cause death, serious bodily injury or substantial material damage through the release, dissemination or impact of toxic chemicals, biological agents or toxins or similar substances or radiation or radioactive material.
4. “Military forces of a State” means the armed forces of a State which are organized, trained and equipped under its internal law for the primary purpose of national defence or security, and persons acting in support of those armed forces who are under their formal command, control and responsibility.
5. “Place of public use” means those parts of any building, land, street, waterway or other location that are accessible or open to members of the public, whether continuously, periodically or occasionally, and encompasses any commercial, business, cultural, historical, educational, religious, governmental, entertainment, recreational or similar place that is so accessible or open to the public.
6. “Public transportation system” means all facilities, conveyances and instrumentalities, whether publicly or privately owned, that are used in or for publicly available services for the transportation of persons or cargo.

Article 2

1. Any person commits an offence within the meaning of this Convention if that person unlawfully and intentionally delivers, places, discharges or detonates an explosive or other lethal device in, into or against a place of public use, a State or government facility, a public transportation system or an infrastructure facility:
 - (a) With the intent to cause death or serious bodily injury; or
 - (b) With the intent to cause extensive destruction of such a place, facility or system, where such destruction results in or is likely to result in major economic loss.

Appendix 4

2. Any person also commits an offence if that person attempts to commit an offence as set forth in paragraph 1.
3. Any person also commits an offence if that person:
 - (a) Participates as an accomplice in an offence as set forth in paragraph 1 or 2; or
 - (b) Organizes or directs others to commit an offence as set forth in paragraph 1 or 2; or
 - (c) In any other way contributes to the commission of one or more offences as set forth in paragraph 1 or 2 by a group of persons acting with a common purpose; such contribution shall be intentional and either be made with the aim of furthering the general criminal activity or purpose of the group or be made in the knowledge of the intention of the group to commit the offence or offences concerned.

Article 3

This Convention shall not apply where the offence is committed within a single State, the alleged offender and the victims are nationals of that State, the alleged offender is found in the territory of that State and no other State has a basis under article 6, paragraph 1, or article 6, paragraph 2, of this Convention to exercise jurisdiction, except that the provisions of articles 10 to 15 shall, as appropriate, apply in those cases.

Article 4

Each State Party shall adopt such measures as may be necessary:

- (a) To establish as criminal offences under its domestic law the offences set forth in article 2 of this Convention;
- (b) To make those offences punishable by appropriate penalties which take into account the grave nature of those offences.

Article 5

Each State Party shall adopt such measures as may be necessary, including, where appropriate, domestic legislation, to ensure that criminal acts within the scope of this Convention, in particular where they are intended or calculated to provoke a state of terror in the general public or in a group of persons or particular persons, are under no circumstances justifiable by considerations of a political, philosophical, ideological, racial, ethnic, religious or other similar nature and are punished by penalties consistent with their grave nature.

Article 6

1. Each State Party shall take such measures as may be necessary to establish its jurisdiction over the offences set forth in article 2 when:
 - (a) The offence is committed in the territory of that State; or
 - (b) The offence is committed on board a vessel flying the flag of that State or an aircraft which is registered under the laws of that State at the time the offence is committed; or
 - (c) The offence is committed by a national of that State.
2. A State Party may also establish its jurisdiction over any such offence when:
 - (a) The offence is committed against a national of that State; or
 - (b) The offence is committed against a State or government facility of that State abroad, including an embassy or other diplomatic or consular premises of that State; or
 - (c) The offence is committed by a stateless person who has his or her habitual residence in the territory of that State; or
 - (d) The offence is committed in an attempt to compel that State to do or abstain from doing any act; or
 - (e) The offence is committed on board an aircraft which is operated by the Government of that State.
3. Upon ratifying, accepting, approving or acceding to this Convention, each State Party shall notify the Secretary-General of the United Nations of the jurisdiction it has established in accordance with paragraph 2 under its domestic law. Should any change take place, the State Party concerned shall immediately notify the Secretary-General.
4. Each State Party shall likewise take such measures as may be necessary to establish its jurisdiction over the offences set forth in article 2 in cases where the alleged offender is present in its territory and it does not extradite that person to any of the States Parties which have established their jurisdiction in accordance with paragraph 1 or 2.

5. This Convention does not exclude the exercise of any criminal jurisdiction established by a State Party in accordance with its domestic law.

Article 7

1. Upon receiving information that a person who has committed or who is alleged to have committed an offence as set forth in article 2 may be present in its territory, the State Party concerned shall take such measures as may be necessary under its domestic law to investigate the facts contained in the information.
2. Upon being satisfied that the circumstances so warrant, the State Party in whose territory the offender or alleged offender is present shall take the appropriate measures under its domestic law so as to ensure that person's presence for the purpose of prosecution or extradition.
3. Any person regarding whom the measures referred to in paragraph 2 are being taken shall be entitled to:
 - (a) Communicate without delay with the nearest appropriate representative of the State of which that person is a national or which is otherwise entitled to protect that person's rights or, if that person is a stateless person, the State in the territory of which that person habitually resides;
 - (b) Be visited by a representative of that State;
 - (c) Be informed of that person's rights under subparagraphs (a) and (b).
4. The rights referred to in paragraph 3 shall be exercised in conformity with the laws and regulations of the State in the territory of which the offender or alleged offender is present, subject to the provision that the said laws and regulations must enable full effect to be given to the purposes for which the rights accorded under paragraph 3 are intended.
5. The provisions of paragraphs 3 and 4 shall be without prejudice to the right of any State Party having a claim to jurisdiction in accordance with article 6, subparagraph 1 (c) or 2 (c), to invite the International Committee of the Red Cross to communicate with and visit the alleged offender.
6. When a State Party, pursuant to this article, has taken a person into custody, it shall immediately notify, directly or through

the Secretary-General of the United Nations, the States Parties which have established jurisdiction in accordance with article 6, paragraphs 1 and 2, and, if it considers it advisable, any other interested States Parties, of the fact that such person is in custody and of the circumstances which warrant that person's detention. The State which makes the investigation contemplated in paragraph 1 shall promptly inform the said States Parties of its findings and shall indicate whether it intends to exercise jurisdiction.

Article 8

1. The State Party in the territory of which the alleged offender is present shall, in cases to which article 6 applies, if it does not extradite that person, be obliged, without exception whatsoever and whether or not the offence was committed in its territory, to submit the case without undue delay to its competent authorities for the purpose of prosecution, through proceedings in accordance with the laws of that State. Those authorities shall take their decision in the same manner as in the case of any other offence of a grave nature under the law of that State.
2. Whenever a State Party is permitted under its domestic law to extradite or otherwise surrender one of its nationals only upon the condition that the person will be returned to that State to serve the sentence imposed as a result of the trial or proceeding for which the extradition or surrender of the person was sought, and this State and the State seeking the extradition of the person agree with this option and other terms they may deem appropriate, such a conditional extradition or surrender shall be sufficient to discharge the obligation set forth in paragraph 1.

Article 9

1. The offences set forth in article 2 shall be deemed to be included as extraditable offences in any extradition treaty existing between any of the States Parties before the entry into force of this Convention. States Parties undertake to include such offences as extraditable offences in every extradition treaty to be subsequently concluded between them.
2. When a State Party which makes extradition conditional on the existence of a treaty receives a request for extradition from another State Party with which it has no extradition treaty, the

requested State Party may, at its option, consider this Convention as a legal basis for extradition in respect of the offences set forth in article 2. Extradition shall be subject to the other conditions provided by the law of the requested State.

3. States Parties which do not make extradition conditional on the existence of a treaty shall recognize the offences set forth in article 2 as extraditable offences between themselves, subject to the conditions provided by the law of the requested State.
4. If necessary, the offences set forth in article 2 shall be treated, for the purposes of extradition between States Parties, as if they had been committed not only in the place in which they occurred but also in the territory of the States that have established jurisdiction in accordance with article 6, paragraphs 1 and 2.
5. The provisions of all extradition treaties and arrangements between States Parties with regard to offences set forth in article 2 shall be deemed to be modified as between State Parties to the extent that they are incompatible with this Convention.

Article 10

1. States Parties shall afford one another the greatest measure of assistance in connection with investigations or criminal or extradition proceedings brought in respect of the offences set forth in article 2, including assistance in obtaining evidence at their disposal necessary for the proceedings.
2. States Parties shall carry out their obligations under paragraph 1 in conformity with any treaties or other arrangements on mutual legal assistance that may exist between them. In the absence of such treaties or arrangements, States Parties shall afford one another assistance in accordance with their domestic law.

Article 11

None of the offences set forth in article 2 shall be regarded, for the purposes of extradition or mutual legal assistance, as a political offence or as an offence connected with a political offence or as an offence inspired by political motives. Accordingly, a request for extradition or for mutual legal assistance based on such an offence may not be refused on the sole ground that it concerns a political offence or an offence connected with a political offence or an offence inspired by political motives.

Article 12

Nothing in this Convention shall be interpreted as imposing an obligation to extradite or to afford mutual legal assistance, if the requested State Party has substantial grounds for believing that the request for extradition for offences set forth in article 2 or for mutual legal assistance with respect to such offences has been made for the purpose of prosecuting or punishing a person on account of that person's race, religion, nationality, ethnic origin or political opinion or that compliance with the request would cause prejudice to that person's position for any of these reasons.

Article 13

1. A person who is being detained or is serving a sentence in the territory of one State Party whose presence in another State Party is requested for purposes of testimony, identification or otherwise providing assistance in obtaining evidence for the investigation or prosecution of offences under this Convention may be transferred if the following conditions are met:
 - (a) The person freely gives his or her informed consent; and
 - (b) The competent authorities of both States agree, subject to such conditions as those States may deem appropriate.
2. For the purposes of this article:
 - (a) The State to which the person is transferred shall have the authority and obligation to keep the person transferred in custody, unless otherwise requested or authorized by the State from which the person was transferred;
 - (b) The State to which the person is transferred shall without delay implement its obligation to return the person to the custody of the State from which the person was transferred as agreed beforehand, or as otherwise agreed, by the competent authorities of both States;
 - (c) The State to which the person is transferred shall not require the State from which the person was transferred to initiate extradition proceedings for the return of the person;
 - (d) The person transferred shall receive credit for service of the sentence being served in the State from which he was transferred for time spent in the custody of the State to which he was transferred.

3. Unless the State Party from which a person is to be transferred in accordance with this article so agrees, that person, whatever his or her nationality, shall not be prosecuted or detained or subjected to any other restriction of his or her personal liberty in the territory of the State to which that person is transferred in respect of acts or convictions anterior to his or her departure from the territory of the State from which such person was transferred.

Article 14

Any person who is taken into custody or regarding whom any other measures are taken or proceedings are carried out pursuant to this Convention shall be guaranteed fair treatment, including enjoyment of all rights and guarantees in conformity with the law of the State in the territory of which that person is present and applicable provisions of international law, including international law of human rights.

Article 15

States Parties shall cooperate in the prevention of the offences set forth in article 2, particularly:

- (a) By taking all practicable measures, including, if necessary, adapting their domestic legislation, to prevent and counter preparations in their respective territories for the commission of those offences within or outside their territories, including measures to prohibit in their territories illegal activities of persons, groups and organizations that encourage, instigate, organize, knowingly finance or engage in the perpetration of offences as set forth in article 2;
- (b) By exchanging accurate and verified information in accordance with their national law, and coordinating administrative and other measures taken as appropriate to prevent the commission of offences as set forth in article 2;
- (c) Where appropriate, through research and development regarding methods of detection of explosives and other harmful substances that can cause death or bodily injury, consultations on the development of standards for marking explosives in order to identify their origin in post-blast investigations, exchange of information on preventive measures, cooperation and transfer of technology, equipment and related materials.

Article 16

The State Party where the alleged offender is prosecuted shall, in accordance with its domestic law or applicable procedures, communicate the final outcome of the proceedings to the Secretary-General of the United Nations, who shall transmit the information to the other States Parties.

Article 17

The States Parties shall carry out their obligations under this Convention in a manner consistent with the principles of sovereign equality and territorial integrity of States and that of non-intervention in the domestic affairs of other States.

Article 18

Nothing in this Convention entitles a State Party to undertake in the territory of another State Party the exercise of jurisdiction and performance of functions which are exclusively reserved for the authorities of that other State Party by its domestic law.

Article 19

1. Nothing in this Convention shall affect other rights, obligations and responsibilities of States and individuals under international law, in particular the purposes and principles of the Charter of the United Nations and international humanitarian law.
2. The activities of armed forces during an armed conflict, as those terms are understood under international humanitarian law, which are governed by that law, are not governed by this Convention, and the activities undertaken by military forces of a State in the exercise of their official duties, inasmuch as they are governed by other rules of international law, are not governed by this Convention.

Article 20

1. Any dispute between two or more States Parties concerning the interpretation or application of this Convention which cannot be settled through negotiation within a reasonable time shall, at the request of one of them, be submitted to arbitration. If, within six months from the date of the request for arbitration, the parties are unable to agree on the organization of the arbitration, any one of those parties may refer the dispute to the International Court of Justice, by application, in conformity with the Statute of the Court.

2. Each State may at the time of signature, ratification, acceptance or approval of this Convention or accession thereto declare that it does not consider itself bound by paragraph 1. The other States Parties shall not be bound by paragraph 1 with respect to any State Party which has made such a reservation.
3. Any State which has made a reservation in accordance with paragraph 2 may at any time withdraw that reservation by notification to the Secretary-General of the United Nations.

Article 21

1. This Convention shall be open for signature by all States from 12 January 1998 until 31 December 1999 at United Nations Headquarters in New York.
2. This Convention is subject to ratification, acceptance or approval. The instruments of ratification, acceptance or approval shall be deposited with the Secretary-General of the United Nations.
3. This Convention shall be open to accession by any State. The instruments of accession shall be deposited with the Secretary-General of the United Nations.

Article 22

1. This Convention shall enter into force on the thirtieth day following the date of the deposit of the twenty-second instrument of ratification, acceptance, approval or accession with the Secretary-General of the United Nations.
2. For each State ratifying, accepting, approving or acceding to the Convention after the deposit of the twenty-second instrument of ratification, acceptance, approval or accession, the Convention shall enter into force on the thirtieth day after deposit by such State of its instrument of ratification, acceptance, approval or accession.

Article 23

1. Any State Party may denounce this Convention by written notification to the Secretary-General of the United Nations.
2. Denunciation shall take effect one year following the date on which notification is received by the Secretary-General of the United Nations.

Article 24

The original of this Convention, of which the Arabic, Chinese, English, French, Russian and Spanish texts are equally authentic, shall be deposited with the Secretary-General of the United Nations, who shall send certified copies thereof to all States.

IN WITNESS WHEREOF, the undersigned, being duly authorized thereto by their respective Governments, have signed this Convention, opened for signature at New York on 12 January 1998.

63. See Official Records of the General Assembly, Fifty-second Session, Supplement No. 37 (A/52/37).

64. A/C.6/52/L.3, annex I.

65. General Assembly resolution 50/6.

Extracts from Commonwealth *Criminal Code Amendment (Theft, Fraud, Bribery and Related Offences) Bill 1999* and Explanatory Memorandum concerning Geographical Jurisdiction

Extract from Explanatory Memorandum introducing proposed Part 2.7 of the *Criminal Code*

- “15. The purpose of Part 2.7 is to clarify, and to provide in an orderly way for, the geographical application of Commonwealth offences. There are several instances where the geographical reach of Commonwealth offences is not clear, or where general application provisions are not adapted to the purpose of particular offence provisions. Commonwealth offence provisions are usually enacted to give effect to a specific governmental purpose. Depending on that purpose, and considerations of international law, practice and comity, it might be appropriate for an offence to have a broad or narrow application.
16. The scheme of Part 2.7 is to provide for the most appropriate of those categories to be chosen. First, for a ‘standard geographical jurisdiction’ to govern the geographical application of future offences in the absence of any provision to the contrary. Provision is then made for four categories of ‘extended geographical jurisdiction’. One of those categories might be chosen for express application to govern the geographical application of a particular offence. The five options for geographical jurisdiction set out in Part 2.7 make available a convenient way of covering most offence provisions, although it is possible that for some reason a future law might need to specify yet another kind of jurisdiction.”

PROPERTY DAMAGE AND COMPUTER OFFENCES
OFFENCE COMPARISON CHART

| Model Criminal Code | Australian Capital Territory | New South Wales | Northern Territory | Queensland | South Australia | Tasmania | Victoria | Western Australia | Commonwealth |
|--|------------------------------|----------------------|------------------------------|----------------------|-----------------|-----------------------------|----------------------------|----------------------------|--------------|
| 4.1.6 Damaging Property 10 years | 10 years | 5 years | 7 years | 5 years | 10 years | 2 or 21 years ^a | 10 years | 10 years | 10 years |
| 4.1.7(1) Arson 15 years | 15 years | 10 years | life | life | life | 2 or 21 years ^a | 15 years | 14 years | N/E |
| 4.1.7(2) Threat of arson 7 years | 10 years ^b | 5 years ^b | 5 years | 7 years ^c | N/E | 2 or 21 years ^a | 5 years ^b | 3 years | N/E |
| 4.1.8 Bushfire 15 years | N/E | N/E | N/E | N/E | N/E | N/E | N/E | 14 years | N/E |
| 4.3.3 Sabotage 25 years | 7-10 years ^d | 25 years | 7 years to life ^d | 7 years to life | 15 years | 2 or 21 years ^{ad} | 5 to 15 years ^d | 7 to 20 years ^d | 15 years |

| Model Criminal Code | Australian Capital Territory | New South Wales | Northern Territory | Queensland | South Australia | Tasmania | Victoria | Western Australia | Commonwealth |
|--|-------------------------------------|------------------------|---------------------------|-------------------|------------------------|-----------------|-----------------|--------------------------|---------------------|
| 4.3.4 Threat of sabotage 15 years | N/E | 15 years | N/E | N/E | 15 years | N/E | N/E | N/E | N/E |
| 4.1.9 Threat to cause property damage - fear of death or serious harm 7 years | N/E | 5 years | N/E | N/E | 5 years | N/E | 5 years | 7 years | N/E |
| 4.1.10 Possession of thing with intent to damage property 3 years | 10 years | 3 years | N/E | N/E | 2 years | N/E | 5 years | N/E | N/E |

| Model Criminal Code | Australian Capital Territory | New South Wales | Northern Territory | Queensland | South Australia | Tasmania | Victoria | Western Australia | Commonwealth |
|--|-------------------------------------|------------------------|---------------------------|-------------------|------------------------|------------------------|-----------------------|--------------------------|----------------------|
| 4.2.4 Unauthorised access, modification or impairment with intent to commit serious offence (penalty same as serious offence) | 10 years ^c | 2 years ^c | 7 years ^c | 10 years | N/E | 21 years ^{ac} | 10 years ^c | N/E | 2 years ^c |
| 4.2.5 Unauthorised modification of data to cause impairment 10 years | 10 years | 10 years | N/E | 5 years | N/E | 21 years ^a | N/E | N/E | 10 years |
| 4.2.6 Unauthorised impairment of electronic communications 10 years | N/E | N/E | N/E | N/E | N/E | N/E | N/E | N/E | 10 years |

NOTES:

- a All Tasmanian offences attract a maximum penalty of 21 years imprisonment unless otherwise stated the offences can be charged with a 2 year maximum offence.
- b No specific offence of arson: here, the offence is threatening to destroy property in any manner.
- c Tas and Qld offences are sending a letter ect. threatening to burn or destroy property.
- d No specific offence of sabotage: reference here is to a number of offences under State and Territory law respectively which criminalise damage to specific property, generally mines, sea-banks, dams, railways, railway signals, buoys, sluice gates, navigation works and aircraft.
- e No exactly comparable offence: offence described here is 'access with fraudulent intent.