CHAPTER ONE

Introduction

> . . . you have pleaded guilty to fourteen counts of what might conveniently be described as 'hacking' offences under Part 6A, being offences relating to computers. . . . You were 20 at the time of the commission of these offences. You are a final year accountancy student at the Royal Melbourne Institute of Technology . . . you have no previous convictions and have an unblemished record . . . it is accepted that your motive was no more than to test your computer skills . . . it was said by your counsel that you became addicted to your computer in much the same way as an alcoholic becomes addicted to the bottle . . .
>
> I formed the view that a custodial sentence is appropriate in respect of each of these offences because of the seriousness of them, and having regard to the need to demonstrate that the community will not tolerate this type of offence. Our society is being increasingly served by and dependent upon the use of computer technology. Conduct of the kind in which you engaged poses a threat to the usefulness of that technology, and I think it is incumbent upon the courts in appropriate cases to see to it that the sentences they impose reflect the gravity of this kind of criminality . . .
>
> You are convicted and sentenced to a term of imprisonment of six months . . . but you may be released forthwith upon your giving security by recognisance in each instance in the sum of $500 to be of good behaviour for a term of six months.
>
> County Court of Victoria, at Melbourne, 3 June 1993, *per* Judge Smith

The above sentencing remarks were made after the successful prosecution of a young hacker in Victoria, Australia, at a time when courts were just beginning to deal with the emerging phenomenon of cyber crime and its societal consequences (see **[Case No. 15]**). The case itself is not remarkable – on the contrary, it resembles many other prosecutions of computer-literate offenders motivated more by curiosity than obvious criminality, and the sentence imposed was also fairly typical. However, the judge's remarks illustrate the difficulties faced by prosecutors and courts in responding appropriately to emerging threats created by new technologies.

Since this case was heard over ten years ago, cyber crime has come a long way. Along with its inexorable growth has come a corresponding increase in the number of cases appearing in the courts. The trajectory of the growth of cyber crime and the emerging capacity of governments to respond will almost certainly lead to more and more cases entering the judicial process. These cases will pose some familiar challenges for prosecutors and judges, and also many new ones.

Until recently, both scholarly and journalistic accounts of cyber crime have tended to focus on the ways in which the crime has been committed and how it could have been prevented. This can be explained in part by the fact that most cyber crimes, like crimes in general, never result in prosecution – much less in conviction and punishment of the perpetrators.

This book provides the first international study of the manner in which cyber criminals are dealt with by the judicial process. Some of the most prominent cases from around the globe have been selected for presentation and discussion in an attempt to discern trends in the disposition of cases, and common factors and problems that emerged during the processes of prosecution, trial and sentencing.

Although the book does not purport to be a global handbook for prosecutors, lawyers, or judges with a professional interest in cases involving cyber crime, we hope that it will be a valuable resource for all those who seek to recall the facts of some of the world's most famous prosecutions and to know the reasons why particular sentences were imposed. As with other types of crime, to gain some understanding of sentencing it is necessary to have a detailed knowledge of the circumstances in which cyber crimes are committed and the personal characteristics of those found guilty of criminal conduct.

Although our inquiry encompasses cases adjudicated in courts from around the globe, responses to cyber crime in different jurisdictions have many common features, as offences of this nature are often committed for similar motivations of greed, curiosity or revenge. Offenders from different countries also tend to have similar characteristics, often being well-educated, middle-class, young and male. As digital technologies become more prevalent, however, it is to be expected that this profile will alter and that individuals from different social and educational backgrounds will become involved, as will female users of digital technologies.

Previous studies have carefully described the kinds of crimes that can take place in the digital age as well as a wide range of preventive measures that may be appropriate to address these crimes (Grabosky and Smith 1998; Grabosky, Smith and Dempsey 2001). In the present volume, however, we focus on the operation of what is known as 'tertiary crime prevention' – that is, criminal justice system action designed to prevent crime after offences have occurred. This can operate directly through deterrence, incapacitation, and rehabilitation of offenders, or indirectly through the promotion of social norms that seek to characterise criminal conduct as unacceptable in the eyes of the community generally (Layton-Mackenzie 2002).

Of course, the success of tertiary crime prevention requires that cases be prosecuted and come before the courts, with all the attendant publicity that this may involve. This is now starting to occur in the world of cyber crime, and it is hoped that the effects will be fruitful. Our objective is, therefore, to find out what has happened to cyber criminals who have been prosecuted and what impediments have arisen with respect to successful prosecution and punishment. The common theme lies not so much in the nature of the illegality, but in the fact that it resulted in prosecution and trial of those alleged to have committed such crimes. The focus is, therefore, on uncovering the ways in which prosecutors, lawyers, and judges have dealt with these often complex cases.

Structure and Plan

Three principal hypotheses are addressed in the chapters that follow. These are:

(a) that the prosecution and judicial disposition of cases involving cyber crime are no different from conventional crime;

(b) that the prosecutorial and judicial responses to cyber crime have been similar in North America, Britain and Australasia; and

(c) that the presence of computers in the commission of crime does not affect the severity with which courts deal with those convicted of crimes.

Each substantive chapter will be structured in such a way as to identify the key issues under discussion, to illustrate these by reference to decided cases and legislation, and to examine relevant evidence supporting and rebutting each of the hypotheses, where appropriate.

The remainder of this book is divided into eight chapters.

Chapter Two considers the definition and scope of cyber crime and its theoretical interaction with white collar crime, economic crime, intellectual property infringement, telecommunications crime and civil redress. A formal classification is proposed that is used to delimit the scope of the present discussion. We also review current knowledge concerning the incidence and threat of cyber crime as disclosed in official administrative data and victimisation surveys, particularly in the business and corporate environment.

Chapter Three focuses on the prosecution of cases in both adversarial and inquisitorial systems. It will examine the difficult policy and practical questions associated with deciding which cases to prosecute, and the application of the various prosecution policies that are used in the regions concerned. This chapter will also discuss the role of the prosecutor in criminal investigation, comparing the more direct 'upstream' involvement in the United States and in inquisitorial systems with the Anglo-Australian model of detached independence. It will also address the vexed question of whether to prosecute juveniles.

Chapter Four considers the problem of prosecuting cyber crime that involves a cross-border element (within federal systems as well as cross-nationally). The chapter includes discussion of legal questions of jurisdiction and conflicts of law as well as forensic and practical issues associated with obtaining evidence, extradition of offenders, and reliance on arrangements for mutual assistance internationally. It reviews, among others, the cases of a fifteen-year-old Canadian youth who was charged with the distributed denial-of-service attacks against major e-commerce sites in February 2000, and the Philippine former computer science student alleged to have been the architect of the 'Love Bug' virus, who avoided prosecution because of the lack of dual criminality under Philippine law. The chapter concludes with an examination of some of the practical impediments to the successful prosecution of cross-border cyber crimes.

Chapter Five concerns the trial of cyber criminals and, in particular, compares the contending strategies of prosecution and defence. It notes how in common law systems, the defence often seeks to exclude evidence likely to be inculpatory, by challenging the legality of the investigative processes by which the evidence was derived, and how the prosecution responds to these challenges. In addition, it compares defence tactics in jury trials to make the evidence appear unduly complex (and thereby introduce doubt) with the prosecution's efforts to make the evidence simple and intelligible to the jury. This is particularly challenging in circumstances where the evidence may have been rendered inaccessible or difficult to detect through technical means such as encryption. The chapter also discusses various defences that may be raised to suggest a lack of criminal intent on the part of the accused.

Chapter Six looks at the initiatives that have been taken to reform laws to accommodate cyber crime. It considers the applicability of existing criminal offences to a range of computer misconduct, noting areas in which new laws have had to be enacted, and reviews model legislative reforms and the processes of harmonisation that have been implemented globally to deal with these new offences. Foremost among these is the Council of Europe's *Convention on Cybercrime*.

Chapter Seven considers the nature and purposes of punishment for cyber crimes. It discusses the objectives of punishment, under the two broad categories of retributive and consequentialist approaches, and some of the specific features that punishment should have in order to achieve its purpose under one or the other of these approaches. The chapter then considers, with reference to recent cases, how each of these features applies in the case of cyber crime.

Chapter Eight examines the process of sentencing cyber criminals. It reviews questions of fact-finding and then examines the various factors that courts are required to take into consideration when determining sentence, including aggravating factors, or what are known in the United States as 'enhancements', as well as mitigating factors raised on behalf of the defendant. The vexed issue of consistency of approach is also addressed. Some empirical evidence is presented concerning the extent to which specific punishments are actually used in cases involving cyber crime. The chapter discusses novel sentencing options for dealing with often rationally motivated economic offenders and how conditional non-custodial sanctions can be used to achieve lasting deterrent effects. Finally, the role of publicity as a sanction is considered. Cases to be discussed include offenders whose substantial sentences and stringent release conditions have engendered public controversy.

Chapter Nine, the final chapter, draws the evidence together and provides an assessment of the extent to which each of the hypotheses referred to above has been accepted or rejected. It also identifies whether, and if so, why, cyber criminals are dealt with differently from other offenders in the judicial process, and how different countries' legal systems have responded to the continuing problem of cyber crime. We offer some suggestions for reforming laws and procedures in order to deal with such cases more efficiently, and to reduce the sometimes considerable resources that governments expend in the effort to achieve justice in cyberspace. Finally, we seek to identify the most productive ways in which legislatures, prosecutors and the courts can proceed in the future, as well as to isolate the most urgent areas for further data collection, reporting and research.

Conclusion

Our aim in this book is to shed light on how the prosecutorial and judicial process could be improved in order to handle more effectively the complex legal and technical difficulties that arise in cyber crime cases. We also seek to illuminate directions for policy and law reform in the future, in order to deal with the many problems that tend to be common across countries in cases of this nature. Finally, we respond to the basic question: how are cyber crime cases different from ordinary criminal cases?

CHAPTER TWO

Defining and Measuring Cyber Crime

Before proceeding with our substantive discussion it is important to examine the definition, nature and scope of cyber crime, in order to delimit our inquiry as well as to place the discussion of the cases we have chosen for analysis in some theoretical context. In the following discussion we shall examine some of the key terms and their relationship to other descriptive categories of crime that overlap to some extent with our topic of inquiry.

Clearly, digital technologies lie at the heart of cyber crime and these include computers, communication technologies and networked services. Grabosky and Smith (1998) describe the wide range of services included within the concept of digital technologies and for the purposes of the present discussion we shall assume that computers, communications technologies and other networked services form the infrastructure in which cyber crime may be committed. References to computers and digital technologies will be used interchangeably.

Cyber Crime Not Cybercrime

There is, at present, a wide range of adjectives used to describe computer crime – virtual, online, cyber-, digital, high-tech, computer-related, Internet-related, telecommunications-related, computer-assisted, electronic, and 'e-' (as in 'e-crime'). In the same way that the term 'white collar crime' sparked fifty years of discussion and controversy, these terms coined to delimit the scope of computer-related misconduct are likely to be similarly problematic.

For present purposes we have chosen to adopt the term 'cyber crime' to describe our subject matter, although any of the other terms could justifiably have been chosen. 'Cyber crime' is used generically to describe a range of criminal offences, only some of which specifically relate to computers and the telecommunications infrastructure that supports their use. In this sense, it is similar to terms such as 'fraud', which are generally not used in legislation (statute drafters preferring legalisms such as 'obtaining financial advantage by deception'), but rather, are used by criminal justice personnel to describe a range of offences, all of which contain an element of dishonesty. Similarly, 'cyber crime', spelt as a single word in the titles of some recent pieces of legislation such as the Australian *Cybercrime Act 2001* (Cth) and the Council of Europe's *Convention on Cybercrime*, is a way of

describing conduct that could entail a range of offences, many of which have nothing to do with computers in their legislative descriptions.

Defining the term 'cyber crime' raises conceptual complexities. The term 'cyberspace' was first coined by William Gibson in his novel *Neuromancer* (1984) to describe a high-tech society in which people inhabit a virtual world divorced from terrestrial life. It has been used since then in a wide range of contexts to describe almost anything to do with computers, communications systems, the Internet, or, indeed, life in the twenty-first century. Chatterjee (2001, p. 81) reviews the many ways in which the term 'cyberspace' has been used, as well as the disparate other terms used to describe computer-related activities including those that infringe criminal laws. She also refers to the observation by Crang, Crang and May (2001, pp. 1–18) that 'the value in cyberspace lies in its ability to resist singular interpretation, and . . . it would be a mistake to try to impose one'. Unfortunately, our discussion requires that cases which do involve cyberspace be distinguished from those which do not.

Arguably a distinction could be made between cybercrime (a singular concept of crime that could encompass new criminal offences perpetrated in new ways) and cyber crime (a descriptive term for a type of crime involving conventional crimes perpetrated using new technologies). Criminal offences that fall into the former category might include cyberstalking and cyberterrorism.

Some have argued that virtual crime should be characterised as separate from and less serious than terrestrial crime, although Williams (2001, pp. 152–3) believes that 'the "real" and the "virtual" are not separate experiences and as such the nature of online communication enables a perpetrator to inflict recognisable levels of harm upon a victim via textual slurs and abuse'. We prefer to use the term 'cyber crime' to encompass any proscribed conduct perpetrated through the use of, or against, digital technologies. Hence, we would argue that cyber stalking should simply be defined as the pursuit or harassment of a victim by means of computers, and that this does not normally entail any new type of crime; the only new element is the means by which it is committed. Similarly, the theft of funds electronically is no different in terms of financial loss from the theft of currency from a bank, and the display of obscene images online (whether involving real human actors or images of people created electronically) involves the same affront to those who view the images as when they see them in a magazine. There may be differences in the extent and scale of the impact, but the effects of the acts themselves remain the same.

Our view that cyber crime raises essentially conventional legal concepts is reinforced by the scope of our present study, which is restricted to cases that have been prosecuted before the courts under existing criminal laws. Some have involved the use of recently enacted laws targeting offences specifically related to computers, such as unauthorised access or modification of data, but the majority involve conventional crimes such as theft and other regulatory offences. The future will undoubtedly see new criminal laws enacted that have particular relevance to computers and new technologies, but we suspect that few will raise truly novel legal considerations. Rather, they will simply apply existing rules to digital technologies and computer-based activities. For the moment, however, we focus on those instances of cyber crime that have actually gone to court.

A Classification of Cyber Crime

The concept of cyber crime we have chosen to adopt derives from the now widely accepted conception of cyber crime as entailing conduct proscribed by legislation and/or common law as developed in the courts, that:

- involves the use of digital technologies in the *commission of the offence*; or
- is *directed at* computing and communications technologies themselves; or
- is *incidental* to the commission of other crimes.

Such activities may be prosecuted through the use of traditional offence categories such as theft or obtaining financial advantage by deception, or recently enacted offences such as gaining unauthorised access to computers or modifying data. Indeed, as the categories are not mutually exclusive (for example, where offenders hack into a bank's customer database in order to obtain credit details, which are then used to effect fraudulent transactions), a combination of such offences may be involved.

Within the first category are cases involving dissemination of offensive material electronically, online fraud and financial crime, electronic manipulation of sharemarkets, and the dissemination of misleading advertising information, to name but a few. Also included are traditional crimes such as fraud or deception in which the involvement of computers constitutes a statutory aggravating element. Examples within the second category include unauthorised access to computers and computer networks (so-called 'hacking' or 'cracking'), crimes involving vandalism and invasion of personal space, such as cyber stalking and denial of service attacks, and theft of telecommunications and Internet services. The third category involves conduct that has been described as 'computer-supported crime' (Kowalski 2002, p. 6). This includes the use of encryption (the translation of data into secret code) or steganography (in which information is embedded within other, seemingly harmless data such as pictures) to conceal communications or information from law enforcement. It also includes the use of electronic databases to store and to organise information concerning proposed or completed criminal activities. The issues raised for investigators therefore generally involve access to evidence rather than specifically proscribed conduct.

These are just some examples, and the full range of potential conduct is limited only by the extent of one's criminal imagination.

Causal Connection

The involvement of computers in the commission of crime can extend from being clear and direct to being peripheral and of minor importance. The definition of computer crime adopted by the National Criminal Intelligence Service's *Project Trawler* (1999) in Britain, for example, is 'an offence in which a computer network is directly and significantly instrumental in the commission of the crime. Computer interconnectivity is the essential characteristic.' Such a definition would exclude many instances involving non-networked computers and is, we believe, overly restrictive.

Clearly, there are certain crimes in which computing and communications technologies *facilitate* the commission of the offence but are not *essential* to its commission. Examples include the theft of funds by creating fictitious invoices on a company's computer, an offence which could just as easily be committed on paper. The opportunity to manipulate paper accounts might not, however, be immediately apparent to a potential offender, whereas the theft of funds electronically might seem more likely to be successful and not as easily detected. Hence there is a need to consider cases in which the use of a computer is of peripheral relevance.

A good example of the subtle differentiation between crimes in which computers are instrumental and crimes in which computers are incidental can be seen in instances of sexual abuse of children whom an offender has located online. In **[Case No. 159]**, for example, the offender met a number of young girls under the age of sixteen through an Internet chat room and, after winning their confidence, arranged to meet them in person. He then persuaded them to engage in various acts of indecency in return for money, cigarettes or alcohol which he provided. He also took obscene photographs of the girls, again in return for money and goods. He was convicted and sentenced to eight years' imprisonment with a non-parole period of six years.

Although such conduct could have been carried out without the use of the Internet – for example, following a chance meeting with a young person in any public place – it seems probable that chat rooms provided an easy and efficient way in which to meet potential victims and to cultivate their interest. The court in sentencing this offender imposed a heavy penalty because of the physical acts perpetrated rather than because the contact had been initiated electronically. Recently, however, legislators have begun to consider specifically proscribing so-called 'grooming' of children by online predators, which would make such discussions in chat rooms illegal even if a physical meeting did not eventuate. In the Australian state of Queensland, a recently enacted provision of the Criminal Code (s. 218A) prohibiting the use of the Internet or e-mail to procure a child under 16 has been used to charge a man after he allegedly sought sexual contact with a chat room visitor he believed was a 13-year-old girl – it was actually a Crime and Misconduct Commission officer using the name 'BettyBoo13' (Wenham 2004).

Such cases are likely to become more prevalent as investigative authorities devote greater resources to 'sting operations', which can include the creation by police of fake websites specifically designed to be attractive to those who search for images of child pornography (AHTCC 2003). Of course, any criminal prosecution based only on evidence that such a site was visited would raise defence arguments of entrapment, but it should be noted that in many jurisdictions, including Australia, the exclusion of illegally or improperly obtained evidence is a matter for judicial discretion rather than a general statutory prohibition (see *Evidence Act 1995* (Cth), s. 138).

In another recent case, a 17-year-old who had been befriended for the purpose of sexual contact by a man he had met in an Internet chat room was alleged to have attempted to murder the man during a sexual encounter they had arranged. As part of the youth's bail conditions, he was prohibited from using the Internet except for the purposes of schoolwork (Melbourne Magistrates Court, 28 October 2003; see Milovanovic 2003).

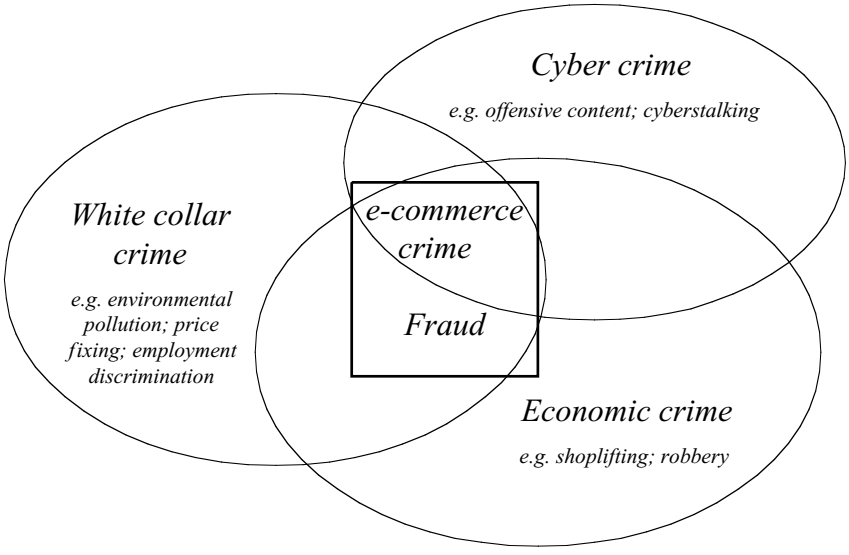

Figure 1 – The interrelationship between white collar crime, economic crime and cyber crime

There are other cases in which computers are involved in the *actus reus* (physical elements) of the crime as the object of the illegality, such as cases involving theft of computer hardware or components, but which have no other connection with digital technologies in terms of how the offence was perpetrated or the ultimate effect of the illegality. These cases, which could include theft of mobile telephones or hand-held personal organisers, or interference with automatic teller machines, vending machines or even modern motor vehicles which have computers on board, will not be considered in our present discussion.

Cyber Crime and Economic Crime

The interrelationship between cyber crime and economic crime raises difficult definitional questions. This is in part because most property crimes involving fraud or dishonesty that have been committed in recent years have involved the use of computers, simply because modern businesses rely so heavily on digital technologies for accounting purposes and for transfer of funds. Moreover, some (though not all) economic crime overlaps with 'white collar' crime, distinguished by its relative sophistication and the background of its usual perpetrators. Figure 1 provides an illustration of the interrelationship between the concepts of white collar crime, economic crime and cyber crime.

We can see that cyber crime has connections with both white collar crime and economic crime. Only a subset of cyber crimes has no economic component, that is, no financial benefit sought to be derived from the activity. Included are cases of cyber stalking or cyber vandalism in which computers are used to threaten or to harass. Many cases of hacking are also carried out for non-economic reasons. The dissemination of offensive content could be either financially motivated (for example, online businesses' distribution of child pornography for a fee) or not

(for example, the publication of other offensive content such as racist material generally, with no fee demanded for access).

Cyber Crime and White Collar Crime

The definition of white collar crime has been an enduring topic of debate over the past century (see Smith 2002 and the extensive review of definitions of white collar crime conducted by Geis 1991). It has been observed that white collar crime is 'a social rather than a legal concept, one invented not by lawyers but by social scientists' (Weisburd, Wheeler and Waring 1991, p. 3). There is no specific offence or group of offences that can be identified as white collar crime. As such, white collar crime is a concept similar to cyber crime in definitional difficulties.

The traditional definition of white collar crime focused on crimes committed by persons of high status and social repute in the course of their occupation (Sutherland 1940). Included in this definition were crimes committed by company officers, public servants, and professional people such as doctors and lawyers. The original emphasis was on economic crime, although over time, white collar crime has come to include any acts of occupational deviance involving a breach of the law or ethical principles. As such, it has been suggested that white collar crime now includes almost any form of illegality other than conventional street crimes (Freiberg 1992).

Technological developments over the past decade have created further complexities surrounding the types of persons able to commit white collar crime. The perpetrator of an online fraud, for example, might just as easily be a self-taught teenager using a personal computer at home as an educated professional in the workplace.

A simple categorisation distinguishes crimes committed by specified types of offenders (mainly professionals and individuals employed by corporations) from crimes perpetrated in specified ways (mainly economic crimes that involve sophistication, planning, or the use of technology in their commission). The essence of white collar crime, however, remains rooted in abuse of power and breach of trust, usually involving the pursuit of financial gain as a motive.

Clearly, not all white collar crimes involve the use of digital technologies, although in recent times the vast majority have. Examples of those which do not include acts of violence committed in the workplace, such as sexual assault of patients by doctors, and some environmental crimes such as pollution, although even the latter can be committed electronically (see for example **[Case No. 101]**, in which the offender manipulated a local council's computer system, deliberately releasing hundreds of thousands of litres of raw sewage into public waterways).

The category of fraud, or financial crimes of dishonesty, intersects with white collar crime, economic crime, and cyber crime. Overlying the other concepts are the categories of property crime and corporate crime. Property crime is sometimes used synonymously with economic crime, although trespass, for example, or acts of vandalism would not be economic but nonetheless clearly property-related. Problems also arise in relation to the types of property protected by the criminal law. Notably, at least until recently, information usually has been regarded as being outside the scope of criminal prosecutions, dealt with instead by a range of intellectual property regimes such as copyright, patents, designs, and protection of confidential information.