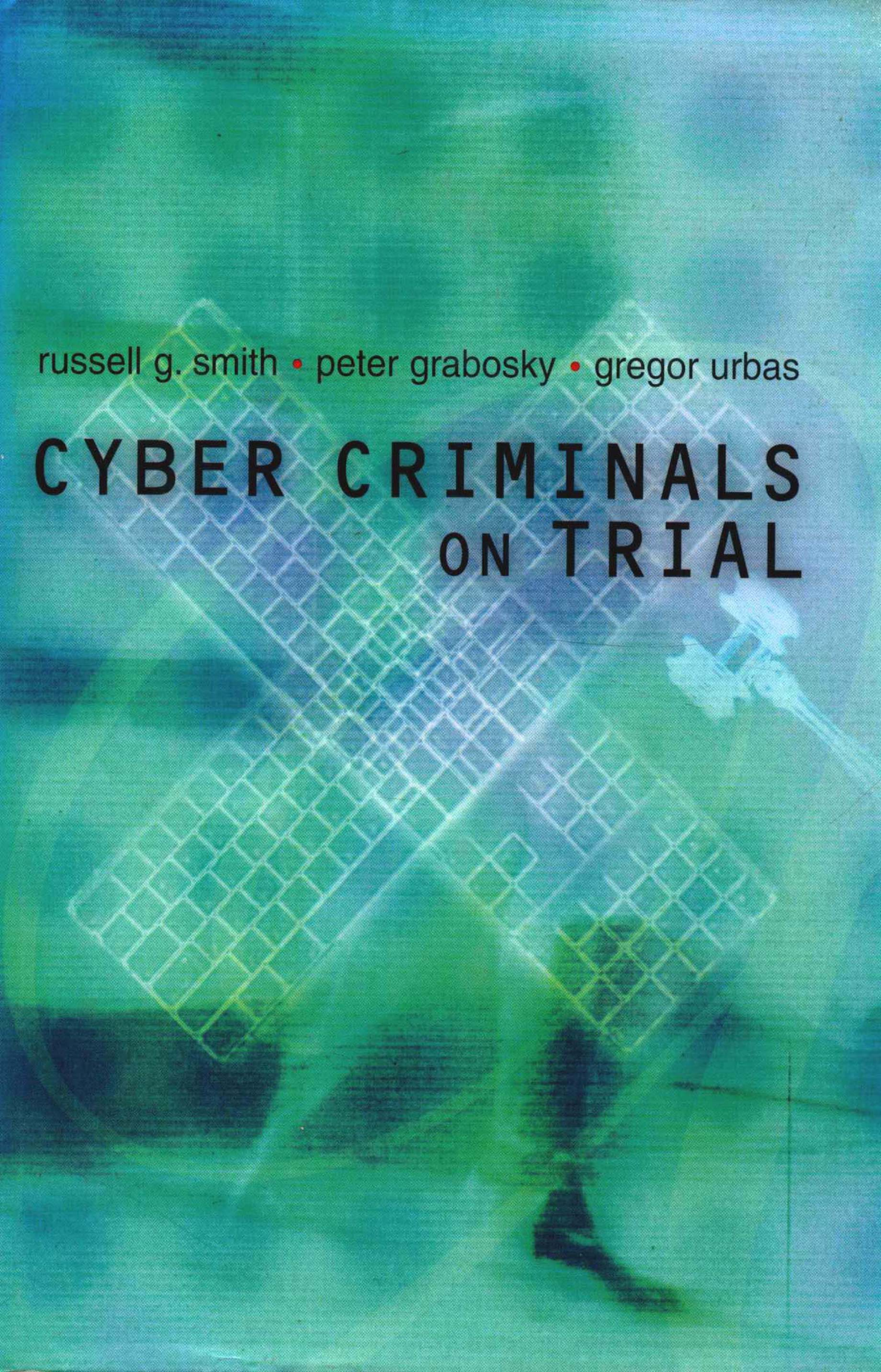
russell g. smith • peter grabosky • gregor urbas
CYBER CRIMINALS ON TRIAL

CYBER CRIMINALS ON TRIAL

RUSSELL G. SMITH
Australian Institute of Criminology

PETER GRABOSKY
Australian National University

GREGOR URBAS
Australian National University

CAMBRIDGE
UNIVERSITY PRESS

PUBLISHED BY THE PRESS SYNDICATE OF THE UNIVERSITY OF CAMBRIDGE
The Pitt Building, Trumpington Street, Cambridge, United Kingdom

CAMBRIDGE UNIVERSITY PRESS
The Edinburgh Building, Cambridge, CB2 2RU, UK
40 West 20th Street, New York, NY 10011–4211, USA
477 Williamstown Road, Port Melbourne, VIC 3207, Australia
Ruiz de Alarcón 13, 28014 Madrid, Spain
Dock House, The Waterfront, Cape Town 8001, South Africa

http://www.cambridge.org

First published by Cambridge University Press 2004

Printed in Australia by Ligare Pty Ltd

Typeface New Baskerville (Adobe) 10.5/12 pt. *System* LaTeX 2_ε [TB]

A catalogue record for this book is available from the British Library

National Library of Australia Cataloguing in Publication data
Smith, Russell G.
Cyber criminals on trial.
Bibliography.
Includes index.
ISBN 0 521 84047 3.
1. Internet fraud. 2. Computer crimes. 3. Trials.
I. Grabosky, Peter N., 1945–. II. Urbas, Gregor. III. Title.
345.0268

ISBN 0 521 84047 3 hardback

CYBER CRIMINALS ON TRIAL

As computer-related crime becomes more important globally, both scholarly and journalistic accounts tend to focus on the ways in which the crime has been committed and how it could have been prevented. Very little has been written about what follows: the capture, possible extradition, prosecution, sentencing and incarceration of the cyber criminal.

This book provides the first international study of the manner in which cyber criminals have been dealt with by the judicial process, and anticipates how prosecutors will try to bring criminals to the courts in future. It is a sequel to the groundbreaking *Electronic Theft: Unlawful Acquisition in Cyberspace* by Grabosky, Smith and Dempsey (Cambridge University Press, 2001). Some of the most prominent cases from around the world have been presented in an attempt to discern trends in the handling of cases, and common factors and problems that emerged during the processes of prosecution, trial and sentencing.

This is a valuable resource for all those who seek to understand how the difficult task of convicting cyber criminals can be achieved in a borderless world.

Russell G. Smith, BA (Hons), LLM, DipCrim (Melb.), PhD (London), Solicitor of the Supreme Court of England and Wales, Barrister and Solicitor of the Supreme Court of Victoria and the Federal Courts of Australia, is Deputy Director of Research at the Australian Institute of Criminology. He is co-author of the books *Electronic Theft: Unlawful Acquisition in Cyberspace* and *Crime in the Digital Age.*

Peter Grabosky, BA (Colby), MA, PhD (Northwestern), FASSA, is a Professor in the Regulatory Institutions Network at the Australian National University, a former Deputy Director at the Australian Institute of Criminology, and current Deputy Secretary General of the International Society of Criminology. He is a co-author of *Electronic Theft: Unlawful Acquisition in Cyberspace* and *Crime in the Digital Age*, and co-editor of *The Cambridge Handbook of Australian Criminology.*

Gregor Urbas, BA (Hons), LLB (Hons), PhD (ANU), Barrister and Solicitor of the Supreme Court of the Australian Capital Territory and the Federal Courts of Australia, is a Lecturer in Law at the Australian National University and a former Research Analyst at the Australian Institute of Criminology. With Russell Smith, he is a co-author of *Controlling Fraud on the Internet.*

Foreword

Crime has been with us since society began and will be with us forever. As long as we have rules to regulate the conduct of humans, we will have rule-breakers. The best we can ever hope to achieve in countering this tendency is a socially acceptable level of control of such behaviour. We exercise such control by prevention and, where that fails, punishment.

The motivations for rule-breaking have not changed greatly because they arise from human nature. Criminals are motivated by passion, greed, revenge, curiosity, need, abnormal perceptions of themselves or society, or just plain evil. Some simply enjoy the challenge of offending and not being caught. Sometimes, rules are broken because they are not appropriate to the people, the place or the time to which they purport to apply.

But the ways in which crime may be committed change significantly over time. In most developed countries, highway robbery is a thing of the past. Now, among other developments, we have moved into the realm of cyber crime.

The present authors are well qualified to write about it and they do so in a comprehensive and easily understandable fashion. They present an up-to-date and truly international perspective on responses to the novel legal problems thrown up by the criminal use of computer technology.

The authors define cyber crime as encompassing 'any proscribed conduct perpetrated through the use of, or against, digital technologies'. Simple! They focus on what is known as 'tertiary crime prevention' – criminal justice system action that might deter, incapacitate or rehabilitate offenders. Therefore the book will be of primary interest to investigators, prosecutors, judicial officers and others engaged in the process of bringing offenders to justice. It also provides valuable insights and suggestions for academics, students and lawmakers.

The criminal law is inherently conservative in its development (as it should be), but significant changes have occurred in response to social pressures. At one time in parts of the United States, as the authors point out, it was an offence to harbour a runaway slave, while in other parts slavery was prohibited. At the time of the industrial revolution in the United Kingdom the legislature was obliged to act to create statutory offences, on top of and superseding the common law, to provide a better measure of protection for factory and mine workers. In the information technology age it has become necessary to develop new approaches

to crimes that are motivated by the old forces but committed by new means in the 'wired world' of cyberspace.

There are many challenges to be confronted. At first prosecutors tried to squeeze new criminal acts into old laws; now laws are being made to address the conduct directly. The question of the appropriate jurisdiction in which to proceed is vexed, given that electronic impulses may traverse many nations before hitting their targets. What priority should be given to the pursuit of cyber criminals where in some cases there may be substantial loss and in others not much more than nuisance value? If there are no flesh and blood victims, does it make a difference? Juveniles are empowered as never before by information technology – how should juvenile cyber criminals be treated? What strategies have been adopted by investigators and prosecutors to meet the modern challenges? What are some of the defences that have been tried so far? And what punishments are appropriate for these types of offences? These issues and more are addressed in the chapters that follow, and compelling arguments are presented for the need for the law to develop and move in step with the enormous technological changes that have occurred in recent decades.

This is not just a book about the place of computers in the commission of crime. The reader is treated to an examination of specific cases in many jurisdictions, chosen to illustrate the ways in which novel problems are being addressed. Apparently simple measures, such as a greater degree of harmonisation of substantive and procedural laws between jurisdictions, would go a long way towards lowering the cost to societies of prevention and punishment. The authors describe ways in which such developments could occur and the extent to which they have begun. They raise specific issues that require further consideration by us all.

In the meantime, trial and punishment proceed under existing regimes and the ways in which they occur are the focus of the book.

This is a timely and trailblazing work. It is indeed, as the authors say: '. . . the first international study of the ways in which cyber criminals have been dealt with by the judicial process'. It provides extremely valuable assistance to those of us in the law, wherever we are, who are interested in learning how to deal with the novel considerations raised by the development of cyber crime.

Nicholas Cowdery AM QC
Director of Public Prosecutions, New South Wales, Australia
President, International Association of Prosecutors

Acknowledgments

In researching this book we have been fortunate in having had discussions with many people involved in the investigation, prosecution, trial and regulation of cyber crime around the world. Others have read drafts of chapters and provided important sources of information and advice. In particular we wish to thank the following.

In Australia: Paul Coghlan QC (Director, Victorian Office of Public Prosecutions), Richard Refshauge SC (Director, Director of Public Prosecutions, Australian Capital Territory), Geoff Gray (Office of the Commonwealth Director of Public Prosecutions), Geoff Denman (Office of the Director of Public Prosecutions, New South Wales), David Morters (Office of the Director of Public Prosecutions, Australian Capital Territory), and Alastair MacGibbon (Australian High Tech Crime Centre).

In the European Union: Henrik Kaspersen (Vrije Universiteit, Amsterdam).

In the United Kingdom: Evan Bell (Department of the Director of Public Prosecutions for Northern Ireland), Andrew Laing (Fraud and Special Services Unit, Crown Office, Scotland), Adrian Culley (Metropolitan Police, New Scotland Yard, Computer Crime Unit), Dick Woodman (Metropolitan Police, S06 Specialist Crime Unit), Len Hynds (Head, National High Tech Crime Unit, National Crime Squad), Sheridan Morris (Home Office, Policing and Reducing Crime Unit), Terry Palfrey (Casework Directorate, Crown Prosecution Service), Ian N. Walden (Centre for Commercial Law Studies, Senior Research Fellow, Queen Mary & Westfield College), Bill Wheeldon (Casework Directorate, Crown Prosecution Service), Peter Parker (Head Internet Unit, Financial Services Authority), John Doran (Internet Unit, Financial Services Authority), Tricia Howse (Assistant Director, Serious Fraud Office), Steve Edwards (Computer Crime Division, Serious Fraud Office) and Tim Wright (Head Hi Tech Crime Team, Home Office).

In the United States: Orin Kerr (George Washington University Law School) and his immensely informative website at <http://hermes.circ.gwu.edu/archives/cybercrime.html>, Chris Painter, Todd Hinnen, Joel Schwartz and Michael Sussmann (Computer Crime and Intellectual Property Section, Criminal Division, United States Department of Justice), Gregory Schaffer (PricewaterhouseCoopers) and Susan Brenner (University of Dayton School of Law).

We wish also to thank the Australian Institute of Criminology and the Australian National University for their institutional support and for generously providing

funding for the engagement of the following research assistants: Julie Ayling, Michael Cook, Simon MacKenzie, Yuka Sakurai, Alex Strang, Neale Williams and Heidi Yates. Sascha Walkley, a doctoral student at the Australian National University, also read and commented on the manuscript.

Finally, we are particularly grateful to our publishers, Cambridge University Press, for their guidance and encouragement, for Peter Debus's enthusiasm and support throughout and for Elaine Miller's meticulous editing of the manuscript which improved its accuracy and style immensely. We remain, of course, entirely responsible for this final published version.

Russell G. Smith
Melbourne
Peter N. Grabosky and Gregor F. Urbas
Canberra
March 2004

Preface

The material presented in this book comes from a wide range of sources. Apart from recourse to secondary sources and commentaries on the judicial process in this area, we have drawn on a number of government reports dealing with cyber crime. The Internet itself provides a good deal of information, and of course many unreported judicial decisions are now available online.

In addition, we sought input and advice from senior practitioners in the field. This was achieved through informal discussions with personal contacts and, more formally, by holding a number of Roundtable Discussions in which we called together the most senior people in a variety of jurisdictions who are involved in the investigation and prosecution of cyber crime. The purpose of these was to seek their understanding of the key issues that affect their daily work.

Two such Roundtable Discussions were held, one in Canberra on 4 April 2002 at the Australian Institute of Criminology and one in London on Tuesday 16 July 2002 at the Home Office. In the United States, discussions were held with key informants in Washington DC on 7 and 8 November 2002. Attending each were senior police, prosecutors and/or representatives from regulatory agencies in each country, with each discussion facilitated by one of the authors. Each discussion followed the plan of the chapters of this book.

Our primary focus was, however, on cases that have reached the courts, and we attempted to identify the most significant cases that have been dealt with by the courts in North America, the United Kingdom and Australasia. Of course, some cases have been omitted, but we are confident that we have examined the key decisions over the last thirty years. Each case was analysed with respect to the judicial processes involved in prosecution, trial and sentencing.

The present work does not purport to be a scientific, empirical analysis of cases decided in the courts, although we have presented some descriptive statistics of sentencing outcomes, aggravating and mitigating factors. We also present the results of a small study of sentencing in serious fraud cases involving computer-assisted crimes decided by Australian and New Zealand courts in the calendar years 1998 and 1999.

We have included a selection of cases involving cyber crimes that have been determined in the courts, identifying as many as we were able to locate from jurisdictions involving adversarial court processes (principally, Australia, the United

Table 1 – *Number of cyber crime cases examined, 1972–2003*

Year	USA	Australia and New Zealand	Asia	UK	Canada	EU	Subtotal	Total
Number Date	(2)						(2)	2
1972	1						1	1
1973		(1)					(1)	1
1974	(1)						(1)	1
1984				1			1	1
1986		1	1				2	2
1987		2			1		3	3
1988				(1)			(1)	1
1989			(1)				(1)	1
1990	(1)						(1)	1
1991	1 (1)			1			2 (1)	3
1992	1	1	(1)	2	(1)		4 (2)	6
1993	1	1		1 (1)	(2)		3 (3)	6
1994	1 (1)		(1)	1			2 (2)	4
1995		3		1	2 (1)		6 (1)	7
1996	2			2 (1)	1		5 (1)	6
1997	1 (2)		1	3(1)			5 (3)	8
1998	4 (1)	3	1	(2)			8 (3)	11
1999	7 (2)	3	6 (1)	3 (1)		(1)	19 (5)	24
2000	11 (7)	(1)	6 (1)	2			19 (9)	28
2001	16 (3)	4 (2)	3	3		1	27 (5)	32
2002	15 (10)	2 (2)	4 (4)	4	1		26 (16)	42
2003	15 (16)	12 (1)	1	2		1 (1)	31 (18)	49
sub-totals	76 (47)	32 (7)	23 (9)	26 (7)	5 (4)	2 (2)	164 (76)	240
Total	123	39	32	33	9	4	240	

Note: Numbers represent the number of cases from each jurisdiction set out in Appendix A and (in parentheses, the number of additional cases not included in Appendix A).
Information is current, and URLs were operational, at 31 March 2004 unless otherwise indicated.

Kingdom, United States, Canada, New Zealand and Hong Kong), with some reference to other countries to illustrate alternative ways in which cases have been dealt with. The work is not, however, a comparative analysis of prosecution and sentencing in the countries examined. Rather, it attempts to identify issues that are common to prosecutors and judges in these jurisdictions.

We conducted extensive online searches of databases of cases and legislation publicly available for legal research. Cases were identified for analysis if they resulted in a judicial determination and imposition of a sanction, although reference is also made to some striking examples of cases which could not be prosecuted due to legislative or procedural difficulties, or which resulted in an acquittal of the accused or in which the accused's appeal was successful. We were also only able to refer to cases that had been publicly reported, which of course excludes some cases heard in lower courts. We are confident that we have isolated for examination those cases which best illustrate the points under discussion from the various jurisdictions under consideration. This methodology reflects the way in which judges rely upon precedents in decision-making, reasoning analogically

from similar cases – although, strictly speaking, many of the decisions we cite would be of limited binding or persuasive authority, coming as they do in many cases from courts in other jurisdictions or from lower courts.

In all, we examined some 240 cases. Of these, 164 cases involved a conviction or a guilty plea by the accused (see Table 1). We have been able to locate sentencing outcomes in respect of 139 of these cases. To assist readers in understanding the salient facts and outcomes of the cases selected for examination, we include Appendix A, which contains the essential details of each case, identified by **[Case No.]** where referred to in the text. Again, this information is provided for illustrative purposes rather than as the basis of an empirical database. In time, when more cases have reached the courts, it may be possible to undertake a more rigorous analysis of the circumstances and outcomes of these cases. In the remaining 76 cases, the accused was acquitted at trial or the accused's appeal was allowed or conviction quashed. These latter cases have not been included in Appendix A, although some are referred to in the discussion. It is apparent that most cases have emanated from the United States and that there has been an increasing number of cases coming before the courts in recent times.

Abbreviations

Where cases are cited in the text, the following abbreviations are used. Some abbreviations refer to law report series; others simply provide case identification (if, for example, the case is unreported).

Australia

ACL Rep	Australian Current Law Reporter
A Crim R	Australian Criminal Reports
ACT CA	Australian Capital Territory Court of Appeal
ACT SC	Australian Capital Territory Supreme Court
CLR	Commonwealth Law Reports
FCA	Federal Court of Australia
NSWCCA	New South Wales Court of Criminal Appeal
Qd R	Queensland Reports
VICSC	Victorian Supreme Court
VSCA	Victorian Supreme Court, Court of Appeal
VR	Victorian Reports

Canada

BCJ	British Columbia Judgment (followed by court number)
BC Prov Court	British Columbia Provincial Court
LAC	Labour Arbitration Cases
OJ	Ontario Judgment (followed by court number)
ONCA	Ontario Court of Appeal
OR	Ontario Reports

Hong Kong

CACC	Court of Appeal Criminal Case (followed by court number/year)
DCCC	District Court Criminal Case (followed by court number/year)
HKC	Hong Kong Cases
HKCA	Hong Kong Court of Appeal

HCMA	Hong Kong Magistracy Appeal (followed by court number/year)

New Zealand

NZCA	Court of Appeal of New Zealand

United Kingdom

AC	Appeal Cases
All ER	All England Law Reports
CA (Crim Div)	Court of Appeal (Criminal Division)
Crim App R	Criminal Appeal Reports
Crim App R (S)	Criminal Appeal Reports (Sentencing)
Crim LR	Criminal Law Review
EWCA Crim	England and Wales Court of Appeal (Criminal) Reports
IPR	Intellectual Property Reports
QB	Law Reports, Queen's Bench Division
WLR	Weekly Law Reports

United States of America

F	Federal Reporter
F 2d	Federal Reporter, Second Series
F 3d	Federal Reporter, Third Series
F Supp	Federal Supplement (District Court Reports)
NY App Div	New York Appellate Division
NYS	New York Supreme Court
WI App	Wisconsin Court of Appeals

US Federal Courts

US federal judicial circuits comprise a number of districts from different states.

CD	Central District
Cir	Circuit
ND	Northern District
SD	Southern District

Currency exchange rates

Monetary amounts are generally provided in US dollars (US$). The conversions from other currencies were done using the following exchange rates.

Australia	A$1 = US$0.75
Canada	Can$1 = US$0.75
China	1 RMB = US$0.12
European Union	€1 = US$1.22
Hong Kong	HK$1 = US$0.13
New Zealand	NZ$1 = US$0.65
Philippines	P1 = US$0.017
Singapore	S$1 = US$0.58
United Kingdom	£1 = US$1.80

Contents

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: