Partnership Policing of Electronic Crime:
An Evaluation of Public and Private Police Investigative Relationships

Shane E.H. McKenzie
BA(Hons), MA (Melb)

A thesis submitted in fulfilment of the requirements for the degree of Doctor of Philosophy in the Department of Criminology, Faculty of Arts, University of Melbourne

May 2006
For my wife, Jennifer,
who has taught me so much about partnership.
Declaration of authorship

I declare that this thesis comprises only my own original work, except where due acknowledgment has been made and that the thesis is less than 100,000 words in length, exclusive of tables, maps, bibliographies and appendices.

Shane E.H. McKenzie

This publication is copyright. Other than for the purposes of and subject to the conditions prescribed under the Copyright Act 1968 (Commonwealth of Australia), no part of it may in any form or by any means (electronic, mechanical, microcopying, photocopying, recording or otherwise) be reproduced, stored in a retrieval system or transmitted or communicated without prior permission. Enquiries should be directed to the author.

Disclaimer: This thesis is not a substitute for proper legal advice. The author disclaims any liability for any errors or for any loss or other consequence that may arise from any person relying on any information in this publication.

Where the views of individual members of Victoria Police, the Australian High Tech Crime Centre or government departments are quoted in this thesis, these views are personal and are not necessarily representative of Victoria Police, the AHTCC or the Australian government.
Abstract

Law enforcement agencies worldwide, including those in Australia, have declared partnerships with the private sector to police e-crime as “critical”. However, this strategy faces uncertainties about appropriate formats and the potential for fostering corruption. Sarre and Prenzler’s (2000) Regulated Intersections model proposes that, to avoid corruption, cooperation must be limited and regulated closely.

Consequently, this thesis examines the conditions under which investigative partnership policing of e-crime at the state police level can be mutually beneficial to police and the private sectors, while maintaining public interests. The thesis aims, therefore, to establish normative standards and guidelines for configuring effective and ethical public-private partnerships for e-crime investigation.

An exploratory analysis of 3529 e-crime incidents, reported to and cleared by Victoria Police during 1999/00 to 2003/04, investigated the nature of reported e-crime, routine factors affecting its successful investigation and whether partnership was one of those factors. A pilot survey canvassed private sector responses to these issues and partnered e-crime investigation. Thirty-seven interviews were conducted with police, private investigators and e-crime victims. During the research, three Australian attempts at public-private investigative partnership formed to varying success, including the Joint Banking and Finance Sector Investigation Team (JBFSIT) at the Australian High Tech Crime Centre. These were examined as case studies. The Regulated Intersections model was evaluated through respondents’ reactions to and analysis of the regulatory character it proposes.
The incident record analysis did not reveal reliance on public-private partnerships for successful resolution of e-crime incidents. Only 20% of cases involved private sector personnel, mainly investigators, and most often in response to search warrants. Interviews confirmed an absence of formal partnerships and many other factors that affect e-crime investigation more. Private investigation firms did not emerge as a panacea to jurisdictional or geographical issues as they face similar constraints.

These results cast doubt on the necessity of formal investigative partnership to successful e-crime investigation, when considering the powers and constraints of public police. Partnerships appeared more important to achieving efficiencies and cost-savings. However, the JBFSIT demonstrated the possible synergistic benefit of cross-sector, investigative partnerships.

Responses to the Regulated Intersections model were divided between those opposed to stifling cooperation and those who favoured excluding “maverick” investigators. The thesis argues that this model provides prudent minimum standards for public and private police relationships. Yet as a normative model, its caution would fail to exploit fully the benefits that could accrue from ongoing, symbiotic relationships that prioritise and preserve public interests, and for which police should strive. Regulated Intersections—regulated to promote not limit cooperation—provides a model to work incrementally towards acceptable mutualism.

The study concludes that pursuing investigative partnerships requires first establishing the collaborative advantage, clear projects, roles, funding and most importantly engaging monitoring, accountability and integrity mechanisms. Reforms are proposed to assist policing e-crime, including a taxonomic hierarchy of e-crime jargon and suggestions for oversight mechanisms and situational corruption prevention for partnered
investigations. Joint investigations and secondment of private investigators into public police forces are more justifiable in terms of public interest criteria than outsourcing or referral of investigations. Rigorous evaluation should confirm partnerships are successful, maintain public interests and promote proactive intelligence-led policing of e-crime.
# Table of contents

Declaration of authorship ................................................................. i  
Abstract ........................................................................................... ii  
Table of contents .............................................................................. v  
List of figures ................................................................................... viii  
List of tables ..................................................................................... ix  
Acknowledgements .......................................................................... xi  

## Chapter 1 : Introduction ...............................................................1  
   Aim and scope of the study ............................................................... 7  
   Overview of the thesis ........................................................................ 9  

## Chapter 2 : Background – investigating e-crime .......................... 13  
   From computer abuse to electronic crime ........................................ 14  
   Defining public and private policing ............................................... 22  
   Police investigation of e-crime in Australia ........................................ 26  
   Private investigation of e-crime in Victoria ........................................ 40  
   Partnership in e-crime policing strategy ......................................... 47  
   Concerns arising from joint public-private investigation .................. 49  
   Chapter conclusions ......................................................................... 55  

## Chapter 3 : Partnership policing in perspective ......................... 57  
   Distinguishing partnership policing ............................................... 57  
   Policing partnerships as projects .................................................. 67  
   Standards of public and private policing ........................................ 72  
   Prescribing relationships between public and private police .......... 80  
   Chapter conclusions ........................................................................ 91  

## Chapter 4 : Research design and methods .................................. 93  
   Research questions and hypotheses .............................................. 93  
   Methodology .................................................................................. 95  
   Research methods and case studies .............................................. 100  

## Chapter 5 : The nature of reported e-crime and police e-crime investigations in Victoria .................................................... 122  
   Respondent demographics ............................................................ 123  
   Data sample demographics .......................................................... 127  
   E-crime incident and investigation characteristics ....................... 130  
   Chapter conclusions ....................................................................... 171  

## Chapter 6 : Factors affecting the investigation of e-crime in Victoria ................................................................................. 175  
   Shared understandings of ‘e-crime’ or syntax discrepancy? ............ 176  
   Detection of incidents ..................................................................... 182  
   Under-reporting of e-crime ............................................................ 184  
   The model computer crime offences ............................................. 194
Appendix J : Consent form for non-police interviewees .......... 476
Appendix K : Consent form for police interviewees ............... 477
Appendix L : Schedule for interviews of non-police personnel... 478
Appendix M : Schedule for interviews of police ..................... 486
Appendix N : Handouts used during police & private sector interviews ............................................................................. 494
Appendix O : LEAP sample demographics............................ 498
Appendix P : Respondents’ views of police e-crimes priorities... 512
Appendix Q : Forms for ISPs and online merchants to report incidents .................................................................................. 519
Appendix R : EFTA Mission and objectives............................ 523
Abbreviations ........................................................................... 524
Glossary ................................................................................ 526
Index of authors ...................................................................... 529
Subject index ............................................................................ 533
List of figures

Figure 3.1: The partnership life cycle ................................................................. 68
Figure 3.2: Spheres of interest in partnership policing .................................. 80
Figure 3.3: Dimensions of regulatory character ............................................ 89
Figure 3.4: Regulatory character proposed by Regulated Intersections model... 89
Figure 4.1: The realist evaluation cycle ............................................................ 99
Figure 5.1: Age of respondents ...................................................................... 124
Figure 5.2: Who reported e-crime to Victoria Police, 1999/00-2003/04 .......... 145
Figure 5.3: E-crime complainants by industry sector ..................................... 146
Figure 5.4: Map of the top ten response zones for e-crime incidents in Victoria 1999/00-2003/04 ................................................................. 151
Figure 5.5: References to squad involvement in e-crime incident narratives* ............................................................................................. 152
Figure 5.6: Analysis jobs by offence type performed by Computer Crime Squad 1 July 2001 - 30 June 2002 ...................................................... 156
Figure 5.7: Analysis jobs by offence type performed by Computer Crime Squad 1 July 2002 - 30 June 2003 ..................................................... 157
Figure 5.8: Analysis jobs by offence type performed by Computer Crime Squad 1 July 2003 - 30 June 2004 ...................................................... 158
Figure 5.9: Analysis jobs by offence type performed by Computer Crime Squad 1 July 2004 - 30 June 2005 ..................................................... 159
Figure 5.10: Average time between conclusion of an incident and report to police ................................................................................................. 165
Figure 5.11: Outcomes of cleared e-crime investigations .................................. 167
Figure 8.1: Regulatory character surrounding police and private investigator interaction in Victoria .......................................................... 344
Figure 8.2: Relationships between the taxonomic e-crime jargon ................. 348
Figure 8.3: Deficiencies in regulation of e-crime investigators in Victoria ......... 358
Figure App A.1: Example of a "phishing" email ............................................... 426
Figure App A.2: Anatomy of a phishing scam ............................................... 427
Figure App A.3: Example of HTML code used in phishing emails to redirect unsuspecting users ............................................................... 428
Figure App A.4: Example “mule” recruitment email ....................................... 431
Figure App A.5: Anatomy of a distributed denial of service (DDoS) attack .... 432
List of tables

Table 2.1: Grabosky and Smith’s categories of digital crime.........................16
Table 2.2: Button’s classification of policing .................................................23
Table 2.3: Australian police e-crime investigation units .................................34
Table 2.4: Comparison of Victorian investigator license holders to other security license holders, 1980-2004.................................................................44
Table 2.5: Membership of the Australian Institute of Professional Investigators, 2005.............................................................................................45
Table 2.6: Factors that do and do not predict (non) reporting of hacking........52
Table 3.1: Partnering grid................................................................................69
Table 3.2: Characteristics of successful and failed partnerships .....................70
Table 3.3: Sarre and Prenzler’s models of police / private security relationships ......................................................................................................................85
Table 5.1: Respondents by sector .................................................................123
Table 5.2: Respondents by methods of participation.....................................124
Table 5.3: Sex of respondents .......................................................................125
Table 5.4: Highest level of education attained by respondents.....................126
Table 5.5: E-crime incidents by offence group .............................................130
Table 5.6: Comparative distribution of e-crime incidents to total cleared incidents by offence group and year* ..............................................................134
Table 5.7: Breakdown of deception incidents by e-crime activity ..................135
Table 5.8: Breakdown of harassment incidents by e-crime activity ................136
Table 5.9: Breakdown of regulated public order incidents by e-crime activity .................................................................................................................137
Table 5.10: Breakdown of ‘other’ incidents by e-crime activity .....................138
Table 5.11: Breakdown of sex (non rape) incidents by e-crime activity ..........139
Table 5.12: Breakdown of “pure” e-crime offences by e-crime activity ..........141
Table 5.13: Top 20 modi operandi recorded for e-crime incidents, 1999/00-2003/04 .................................................................................................142
Table 5.14: How e-crime incidents came to police attention .........................144
Table 5.15: Sex of alleged e-crime offenders in sampled incidents, 1999/00-2003/04 ...............................................................................................147
Table 5.16: Sex of e-crime victims in sampled incidents, 1999/00-2003/04 ...148
Table 5.17: Relationship of alleged offenders to victim in e-crime incidents....149
Table 5.18: Location of alleged e-crime offenders ..........................................149
Table 5.19: Location of e-crime victims ..............................................................150
Table 5.20: Jobs received by Computer Crime Squad 1 July 2000 to 30 June 2005 .................................................................................................153
Table 5.21: Jobs completed by Computer Crime Squad 1 July 2000 to 30 June 2005 ......................................................................................................154
Table 5.22: Gigabytes of data analysed by Computer Crime Squad by region or division, 1 July 2000-30 June 2005* ..........................................................160
Table 5.23: Involvement of private sector personnel in e-crime investigations ............................................................................................................................162
Table 5.24: Length of e-crime investigations conducted by Victoria Police, 1999/00-2003/04* ..............................................................................................166
Table 5.25: Comparison of e-crime sample and Victoria Police Crime Statistics for single year clearances by offence group* ..............................................168
Table 5.26: Breakdown of outcomes recorded as “offender processed” for e-crime incidents ...........................................................................................................169
Table 5.27: Reasons for “No Offence Disclosed” outcomes for e-crime incidents ......................................................................................................................170
Table 5.28: Reasons complaints were withdrawn for e-crime incidents........171
Table 6.1: Ranked importance of factors in reporting decisions* ....................189
Table 6.2: Investigation success factors identifiable from LEAP e-crime incident narratives ..............................................................................................230
Table 6.3: Investigation difficulties identifiable from LEAP e-crime incident narratives ..............................................................................................231
Table 7.1: Ranking of agreement with statements about partnership policing of e-crime ..............................................................................................280
Table 7.2: Potential private sector-police partners for e-crime investigation.286
Table 8.1: Principles to guide decision making about partnered investigations of e-crime ..............................................................................................361
Table 8.2: Examples of benefits of investigative partnership that might combine to produce collaborative advantage.........................................................362
Table 8.3: Examples of harms that would outweigh benefits of investigative partnerships ..............................................................................................363
Table 8.4: Intersections where police and private investigators of e-crime interact ..............................................................................................373
Table 8.5: Situational corruption and misconduct prevention techniques for partnership policing of e-crime ..............................................................374
Table App O.1: E-crime incidents sampled from LEAP, 1999/00-2003/04......498
Table App O.2: “Pure” e-crime offences sampled from LEAP, 1999/00-2003/04 ..............................................................................................508
Table App O.3: Number of e-crime incidents reported to Victoria Police by financial year, 1999/00-2003/04..............................................................502
Table App P.1: Respondents views of police priorities for e-crimes ..............504
Table App P.2: Combined views of police priorities for e-crimes ...............509
Acknowledgements

I would like to acknowledge and express my gratitude to the many people who assisted and encouraged me throughout the thesis process:

My deepest thanks to Associate Professor Steve James for his excellent supervision, wise academic mentoring and wicked sense of humour. Also to Associate Professor Fiona Haines, my associate supervisor, for discussing regulatory theory and her concept of regulatory character.

Thank you to my wife, Jennifer, for her patience, love and for sticking by me through yet another thesis. Here’s to our new life together “post-theses”. I am grateful to my father, Ross, for commenting on draft chapters. When are you starting your PhD, Dad? Thank you to the rest of my family also for their interest in the topic and my progress.

I would also like to express my appreciation of the Victorian Department of Justice and Multimedia Victoria for recognising the importance of this research and generously sponsoring a Melbourne Special Postgraduate Studentship so that I could conduct it. Thank you.

From Victoria Police, I would like to thank Chief Commissioner Christine Nixon, Detective Inspector Peter Wilkins, Detective Superintendents Phil Masters and Jack Blayney and Dr. Joseph Poznanski for facilitating this research. Thanks to Rod Mills, David Walker, Neil Jepsen, Jeff Bartolo, Brad Shallies and all the guys at the Computer Crime Squad for making me feel welcome. Special thanks to Terrie Earle, Amy Kirkwright, Nicole Fabien and all others who escorted me into the Major Fraud Investigation Division each day during my data collection. My extra thanks to Michael Howell of the
Geographic Intelligence Unit, State Intelligence Division of Victoria Police for his technical assistance in extracting the LEAP data.

My gratitude also goes to Kevin Zuccato, Director of the Australian High Tech Crime Centre for facilitating my field trip to the Centre to interview members of the Joint Banking and Finance Sector Investigation Team.

Thank you to the academic staff in the Department of Criminology at the University of Melbourne for the many opportunities to teach during my candidature. The time spent lecturing the department’s introductory research methods course was invaluable to designing this research. To Toni Campbell, formerly of Melbourne University Private, who offered me a wonderful opportunity to teach on the topics of this thesis in the Graduate Certificate of E-Crime Investigation, thank you. To Peter Wilkins, Roger Clay and Mick Nolan from Victoria Police with whom I taught the subject, thank you for your camaraderie and insight. Thank you to all my students in *Electronic Crime Fundamentals* for letting me bounce ideas at you and for responding so generously.

Others who provided helpful information to me include Associate Professor Adam Sutton, Sandy Cook (Drugs and Crime Prevention Committee, Parliament of Victoria), Tony Ward, Michael Wheelahan and Brendan Facey (Department of Justice Victoria), Wayne Gladman (Australian Institute of Professional Investigators), Katherine Smith (Media Help Desk, University of Melbourne), Malcolm Feiner (Corrections Victoria Resource Centre), Tom Finlay (Library, Centre of Criminology, University of Toronto) and Dr. Don Weatherburn (NSW Bureau of Crime Statistics and Research). Others simply provided collegial encouragement to persevere, which made me enjoy this all the more: Professor Peter Grabosky (Australian National University), Dr.
Russell Smith and Dr. Tony Krone (Australian Institute of Criminology), Dr. David Tait (University of Canberra), Dr. Austin Lovegrove and Dr. Paul Gruba (University of Melbourne), Professor Ross Homel (Griffith University), Judith Jefferson (ex NZ Police, now with South Australia Police) and all my postgraduate colleagues in the department, especially Chris Ngo, Shasta Holland, David Barton and Emma Ryan. As always, thank you to the departmental administrative staff, Marlene Chaitra, Jack Fagan, Louisa Stewart, Heidi Chung, Dolores Makris and Jean Rodrigues for their support in all things administrivial.

Finally, I would like to thank most of all the many people who took part in this research as survey and interview respondents. Your insight and generosity with your time has been invaluable and is appreciated.

Shane McKenzie, May 2006
Chapter 1: Introduction

In response to the increasing incidence, scope and complexity of crime involving information and communication technologies (ICT), law enforcement agencies around the world, including those in Australia, have declared in their crime-fighting strategies the need to pursue “partnerships” with the private sector. In Australia at the national level, partnerships with the private sector have been identified as paramount to the successful policing of electronic crime due to the specialist nature of the latest technologies (Parliamentary Joint Committee of the National Crime Authority, 2001: 72). Increasingly, corporations, telecommunications providers and Internet Service Providers own the information networks and infrastructure, which are often sources of digital evidence. Partnership, more so than coercive power, has been considered important because of the volatile and transient nature of digital evidence before it is seized, which makes the early stages of these investigations time-sensitive.

Christine Nixon, Chief Commissioner of Victoria Police has described partnership policing as:

> adopting a proactive, problem-oriented response to crime and community safety. It is driven by data and other information that demonstrates needs and priorities for policing services. It relies on evidence—research on best practice—to determine the most appropriate and effective responses. The emphasis on analysis of trends and performance enables earlier intervention and prevention of crime. More proactive and targeted policing increases police efficiency and effectiveness and results in the community being better protected (Nixon, 2002: ¶63).
The more serious varieties of electronic crime, such as child pornography rings, Internet banking fraud, money laundering, hacking, malicious code and copyright infringement often challenge the traditional boundaries of nation states. The Commissioner of the Australian Federal Police, Mick Keelty, has argued that:

Any law enforcement agency that believes that it is capable of containing the domestic manifestations of transnational organised crime without embracing meaningful international co-operation is at a substantial disadvantage. Those who do not at least pay reference to the international and regional factors risk losing control of their anti-crime agendas (Keelty, 21 March, 2002: ¶43).

However, one of the major challenges to policing electronic crime in Australia has been engaging the private sector successfully (Etter, 2001). It has been argued by police that too many corporate CEOs consider e-crime a technical issue rather than a corporate governance issue or that they simply lack interest (Etter, 2001: 18). The Australian Federal Police has noted the challenges of heavy reliance on cooperation and assistance from telecommunications providers and Internet Service Providers (AFP, 2002). Law enforcement and corporations that employ private security often have conflicting goals and guiding principles, especially when it comes to the issues of reporting crime and prosecuting offenders (Sarre and Prenzler, 2000: 107). Securing convictions is an important aim of law enforcement, whilst protecting profits and commercial reputation are greater concerns of the private sectors (Shearing and Stenning, 1981; Prenzler and Sarre, 1998; Etter, 2000). In turn, the interests of private security are generally client-driven and contractual, while police are held to standards of the public interest (Swanton, 1993).
As an example of the reported difficulties, a 1998 survey of the largest 350 Australian companies revealed that a third of them were attacked electronically; however 42% of these did not report the incident outside their own company (Deloitte Touche Tohmatsu and Victoria Police, 1999). Other national surveys since have shown a trend towards even less reporting of e-crime to our law enforcement agencies (AusCERT, NSW Police and Deloitte Touche Tohmatsu, 2002; AusCERT, AFP, Queensland Police, South Australia Police and Western Australia Police, 2003; AusCERT et al, 2004; AusCERT et al, 2005). In late 2004, the Superintendent of the Victoria Police Major Fraud Investigation Division lamented that probably only 3% of all fraud is reported to police in Victoria (Blayney, 2004). Police concerns with under-reporting of e-crime do not stem from a lack of an investigative workload. The problem, police argue, is that they need information from the private sector to appropriately focus their resources and make an impact on the problem (Etter, 2001). The private sector is considered central to defining the e-crime problem (Etter, 2000: 15).

Police also note the challenge in “ensuring security, confidentiality and flexibility of response”, dealing with privacy regulations and achieving timely mutual assistance (AFP, 2002: ¶7). When it comes to e-crime, expertise among public police forces varies dramatically (Stephenson, 2000: 12). The Chief Commissioner of Victoria Police has admitted that that agency has found it “extremely difficult to anticipate and cope with the pace and complexity of social change” (Nixon, 2002: ¶29). While law enforcement agencies are beginning to run specialist-training courses in forensic computing and investigation, in the short-term at least, they have also seen a need for their
members to achieve certifications offered by the private sector and tertiary institutions, leading to educational partnerships.¹

The appropriate format of partnership relationships is contested. At one end of the possible spectrum, there are jointly funded and operated law enforcement agencies; at the other, there is the contract employment of private sector experts in public agencies. In the middle, there are partnerships in the sense of joint working parties and consultative forums (Parliamentary Joint Committee of the NCA, 2001: 72, ¶2.127). It has been argued forums have failed generally (Etter, 2001). The Australian Federal Police, ASIC and AUSTRAC each have contracted IT expertise to assist investigations, “however [AUSTRAC] also maintained sufficient in-house expertise to ensure that it was not being ‘conned’” (Parliamentary Joint Committee of the NCA, 2001: 73). In 2002, South Australia Police floated the idea of outsourcing their e-crime investigations (Douglas, Sept 26, 2002).

At stake first and foremost with partnership policing is the effectiveness of public police forces to combat electronic crime. Also at stake is the potential to inadvertently create opportunities for corruption at a number of levels: from police taking kickbacks for recommending particular private investigation services, breaching civil liberties or inviting “extrajudicial investigations” (Cochrane, 3 June 2003: 3) to inappropriate leaking of police information to the private sector, compromises of security or the introduction of poor quality information into police intelligence databases. The potential for arrangements

¹ The IT industry offers a multitude of product specific and non-specific certifications, such as the Cisco Certified Security Professional. As an example of an educational partnership, Melbourne University Private offered a Graduate Certificate in E-Crime Investigation aimed at police and private investigators and taught by academics, Victoria Police and consultants from industry. The author helped develop and lecture in this program. With the closure of MU Private in 2005, the course continued at the University of Melbourne.
to include public police in “commercial-in-confidence” situations may reduce transparency and elicit crises such as those experienced in the state of Victoria, Australia involving privatisation of prisons (George, A., 1997; Freiberg, 1999). There is also the possibility that referral of cases to “for-fee” private investigators may result in incidents not being investigated at all if victims cannot or choose not to pay. Questions of trust, accountability and expertise must be raised when the sheer omnipotence of companies, many transnational, may have influence over national security policy, as is likely in terms of the National Information Infrastructure that is increasingly owned privately (see generally, Johnston, L., 2000; Cherney, 1997). Managing the ethical aspects of partnership with the private sector and conflicts of interest, whether real or perceived, is a high priority according to one of Australia’s leading police e-crime experts (Wilkins, 2001).

Partnership policing “assumes that everyone—not just the police—owns and is responsible for tackling the problems that undermine community safety” (Nixon, 2002: ¶118). This rhetoric of “responsibilisation” has traditionally called for the public to embrace crime prevention. However, as Marcus Sachs, Director of the Internet Storm Centre, argues “there is absolutely no way you’re going to make everything perfectly safe and secure” when it comes to electronic crime (Sachs interviewed in Lebihan, 17 Feb 2004). E-crime occurs regularly as evidenced by simply opening the technology section of any newspaper. Partnership policing needs to look also at incident and investigative responses. The rhetoric of “responsibilisation” can then be dangerous if it is generalised too literally and used as an abdication or denial of criminal investigative responsibility by state law enforcement agencies. The challenge for partnership policing is to “determine how problems should be tackled and who should be involved in providing effective and lasting solutions” (Nixon, 2002: ¶124).
The issue of private policing is not new (see for example, Kakalik, 1971; Kakalik and Wildhorn, 1977; Shearing and Stenning, 1987). Nor is the private policing of computer crime. Famous instances have been published as novels, such as the investigation by Clifford Stoll of the Hanover hackers described in *The Cuckoo’s Egg* (Stoll, 1989) and the chase and capture of Kevin Mitnick in the book *Takedown* (Shimomura and Markoff, 1996). Peter Grabosky and Russell Smith have provided foundational typologies of electronic crime (see especially, Grabosky and Smith, 1998; Grabosky, Smith and Dempsey, 2001; Grabosky and Smith, 2003) and identified many general difficulties associated with regulating these.

However, the routine investigation of complex crime, such as electronic crime, is under-researched compared to traditional policing activities and crime types. There is an emerging body of literature to describe aspects of the work undertaken by private investigators (Gill and Hart, 1997a; Gill and Hart, 1997b; Button, 2002), but little on the interactions between police and private personnel who investigate these crimes. Button (2002: 108) notes a lack of research in the UK on the investigative relationships between police and their private sector counterparts. This gap appears to exist in Australia also. Even recent theory and discussion of relationships between police and private security, such as Sarre and Prenzler (2000; 2005: 195-96), focuses upon relationships with providers of physical security for foot patrols, guarding premises and people and event security. What little research exists on the interaction between transnational private security and public police has focused upon the privatisation of corrections (Johnston, L. 2000: 36). Bayley and Shearing’s (2001: 35) agenda for researching the changing structures of policing highlights the lack of and fragmented nature of research in the area.
of modern policing and calls for basic research to provide foundational description.

**Aim and scope of the study**

Given the uncertainties outlined above, the central aim of this thesis is to examine critically the conditions under which investigative partnership policing of e-crime at the state police level can be mutually beneficial to law enforcement and the private sectors, while maintaining public interests. The thesis aims, therefore, to establish normative standards and guidelines for configuring effective and ethical public-private partnerships for e-crime investigation.

The thesis focuses upon investigative public-private partnerships, because joint criminal investigation represents one of the most controversial types of partnership that public police could undertake with the private sector. Partnerships that focus upon crime prevention have been considered extensively in the criminological literature already (Abbey and Butten, 1997; Sarre, 1997; Golsby, 1998; McKenzie, 2000; Balfour and Sanders, 2003; James, Graycar and Mayhew, 2003 and numerous others). Initiatives focused on public education are not controversial. Previous work by Fairchild (1994) has examined partnership between law enforcement and other public-sector agencies and so this is only considered peripherally in this thesis. Fairchild (1994: 112) notes that previous analyses have focused upon the reasons for cooperation rather than the mechanics of information sharing, such as partnership arrangements, which are considered by this thesis. This study does not delve deeply into factors affecting the trial of offenders at court, which have already been well documented (see for example, Smith, Grabosky and Urbas, 2004).
A local focus on the routine, everyday investigation of e-crime in the Australian state of Victoria has been taken in this thesis. Alternate approaches could have been taken, such as analysing international policy responses. However, it is important to describe and examine the issues at the local level of state police services and individual officers, because it is within these local contexts that most public police perform their duties. That the emergent e-crime problems challenge those boundaries has not removed the organisational and geographical constraints on the majority of investigators, police or otherwise. As Christine Nixon noted:

Organised crime has moved quickly to exploit global openness and technology, using the Internet and electronic money transfer to systematically commit crimes on a major scale. These crimes may be global in nature and origin, but they are local in their impact upon victims (Nixon, 2002).

The impact is local for police also and it is through a local analysis, within the wider national and international contexts, that this research can best comprehend the implications of present and potential future practices upon serving police. It is considered axiomatic that change, if needed, should not be considered without first understanding current practice.

In devising a normative model for e-crime investigative partnerships, the views of the major stakeholders are examined. These viewpoints need to be considered not only in terms of appropriate structure and effectiveness, but also in terms of accountability and ‘just’ outcomes. Given the vulnerability of partnered criminal investigations to various improprieties, the perspectives of stakeholders can usefully be assessed against externalist, objective standards for police (Cohen and Feldberg, 1991; Kleinig, 1996a, 1996b; Miller, Blackler and Alexandra, 1997; Delattre, 2002) and private investigators (Stenning, 1989;
Sarre, 1998; Sarre and Prenzler, 2005) that are well documented and to which they are formally accountable. There is also a strong literature examining ethical design and decision making for IT professionals in the private sector (see for example, Jonas, 1984; Ladd, 1989; Brankovic and Estivill-Castro, 1999; Lind, 1999; Gotterbarn, 1999; Johnston, D.G. 2001). So it is appropriate that guidelines for police interactions with private e-crime investigators are justified by analysis and application of both the practical and ethical necessities.

**Overview of the thesis**

Chapter Two examines the literature on electronic crime and its investigation from early Australian cases and the development of computer crime investigation units to some of the most recent cases and initiatives such as Operation Auxin, which was coordinated globally by law enforcement with private sector involvement (The Courier Mail, 4 October, 2004; Keelty, 2004). This chapter identifies the issues and difficulties facing law enforcement and introduces the arguments for cross-sector partnership policing of e-crime that have emerged as a result.

Chapter Three locates the strategy of “partnership policing” within the criminological literature on public and private policing and the business literature on strategic alliances. Previous attempts to develop normative relationships including Sarre and Prenzler’s (2000) *Regulated Intersections* model of law enforcement and private security intersection are examined as a basis for developing more detailed guidance for investigative partnerships to police electronic crime.

Based on issues and questions identified in previous chapters, Chapter Four outlines the research methods used to conduct an empirical study of the
investigation of e-crime in Victoria. The study involved an online pilot survey that helped focus later enquiries. An examination was made of e-crime cases reported to and cleared by Victoria Police during 1999/00-2003/04. Finally, interviews were conducted with members of law enforcement agencies, private sector investigators and people who experienced electronic crime as victims. The chapter highlights the management of ethical issues involved in embarking on research involving police data, undertaken at a time when alleged police misuse of criminal history data was prominent in the local media and there were calls for a Royal Commission into police corruption.

Chapter Five presents findings on the nature of e-crime reported to police in Victoria between 1999/00 and 2003/04 and the investigations that resulted. Most statistics and information about the nature of electronic crime in Australia come from victim surveys, such as the AusCERT Computer Crime and Security survey. These studies often focus upon a few distinct types of electronic crime, such as network intrusions or fraud and represent a select sample from the business community. The analysis undertaken for this thesis presents the most comprehensive study to date of e-crime based on police incident records.

Chapter Six examines factors affecting the successful investigation of electronic crime in Victoria by police and private sector investigators. Presented and discussed are the responses to electronic crime by the different sectors, such as reporting decisions and the priorities given to different types of offences. The chapter explores the problematic definition of “electronic crime”, which was contested by some respondents to this study. Included is an examination of Victorian legislation, including the model computer crime legislation. Of importance, the study examines structures within the financial and legal frameworks in Victoria that have permitted law enforcement and
the private sectors to redefine who is considered the “victim” in electronic crime cases and thus modify the policing response in these cases. Police in Victoria have actually discouraged reporting of e-crime. The interviews revealed a culture of denigrating certain victims of electronic crime, blaming them for their own victimisation when investigators were not in a position to investigate successfully.

Having examined the current status of e-crime policing in Victoria, Chapter Seven examines responses to investigative partnership policing as a proposed proactive strategy for e-crime. The chapter examines the different sector beliefs about “partnerships”, reasons for partnering and responses to potential configurations for investigative partnerships. To highlight the issues surrounding investigative partnerships, Chapter Seven examines three Australian attempts at investigative partnerships: the Joint Banking and Finance Sector Investigation Team initiated by the Australian High Tech Crime Centre (AHTCC); an attempt by the private sector to form a new industry association called the E-Crime and Forensic Technology Association of Australia (EFTA); and preliminary discussions between a forensic investigation firm and the Computer Crime Squad of Victoria Police to explore the potential for commercial partnership. The chapter discusses the very different philosophies driving these attempts at partnership.

Chapter Eight draws together the issues and lessons from the thesis to discuss and draw conclusions about the defensibility of implementing investigative partnerships between state police and private sector investigators. The Regulated Intersections model is assessed in terms of its regulatory character. The chapter proposes reforms to assist policing e-crime, including a taxonomic hierarchy of e-crime jargon. The chapter summarises the legal, ethical and performance criteria derived from the literature and this research
that either must or should guide establishment of investigative partnerships and examines these through discussion of seven forms of investigative partnership. Guidelines on oversight mechanisms and situational corruption prevention for partnered investigations are provided.
Chapter 2: Background – investigating e-crime

Inevitably, many details about investigating e-crime have remained confined to law enforcement practitioners lest they coach criminals to evade capture. Consequently, accounts in the literature about early law enforcement responses to e-crime have been partial, often focusing on the introduction of this or that piece of legislation, court cases or generic investigation and prosecution difficulties (see Hollinger, 1997; Grabosky and Smith, 1998; Akindemowo, 1999; EFA, 2000; Forder and Quirk, 2001; Smith, Grabosky and Urbas, 2004). Much of the e-crime literature focuses on incidents and offenders, sometimes even rejecting the topic of law enforcement agencies literally (see Dreyfus, 1997: xi). So too, little is known publicly about private sector investigations of e-crime. The history of e-crime investigation is yet to be written; however this falls outside the scope of this thesis.

Instead, this chapter locates for the reader current (and some historical) issues facing e-crime investigators. The chapter first discusses the evolution of offences facilitated by and against digital technologies and their treatment by academia and law enforcement. The chapter then compares the development of public and private policing of e-crime in Australia, particularly within the state of Victoria as the focus of this research. Subsequently, the arguments given for cross-sector partnership policing of e-crime that have emerged because of investigative difficulties and concerns that arise from pursuing partnered e-crime investigation are canvassed.
From computer abuse to electronic crime

In the past 30 years, the range of offences involving computers and other increasingly digital technologies has been labelled variously and often interchangeably. The original term was computer abuse (Parker, Nycum, and Oüra, 1973) or computer crime (McKnight, 1973), which later included computer-related crime (United Nations Commission on Crime and Criminal Justice, 1995; Stephenson, 2000). Early definitions of “computer abuse” highlighted physical attacks on computers. For instance, Donn Parker in 1976 wrote sincerely of three incidents as “computer abuse”: in 1968, an unknown perpetrator fired two shots at an IBM 1401 at the State Unemployment Office in Olympia Washington. The bullets dented the metal cabinet and it continued working. In 1972, a person fired shots through a window at a tax-processing computer in Johannesburg, South Africa. And in 1973, in Melbourne anti-war demonstrators shot a computer belonging to a US manufacturer with a shotgun destroying it completely. Nowadays, readers would be hard pressed to find mention of such incidents in discussions of computer-related crime. What Parker did in his work was recognise that computers could be:

- the object of an attack;
- they can be the instrument of the act; and
- they can be the environment in which unauthorised activities can occur.

In the last element, Parker was referring to storage of computer programs on magnetic media; not till William Gibson’s (1984) novel Neuromancer did the concept of cyberspace or virtual reality become commonplace. With the advent and popularity of the World Wide Web and offences committed using it or against it came the terms ‘Internet crime’ (Clarke R., 1998; Sutton, Tait,
Bavinton and McKenzie, 1998), ‘telecommunications-related crime’ (Grabosky and Smith, 1998) and ‘computer-facilitated crime’ (McKenzie, 2000). Even more recently, other terms have joined these: ‘cybercrime’ (National Criminal Intelligence Service (UK), 1999; Thomas and Loader B.D., 2000), ‘electronic crime’ (abbreviated to e-crime) (Etter, 2001; AFP, 2002; Nixon, 2002), ‘high tech crime’ (Etter, 2002), ‘digital crime’ (Grabosky and Smith, 2003), ‘cyberspace crime’ (Wall, 2003) and ‘cyber crime’ (Smith, Grabosky and Urbas, 2004). In 1998, Grabosky and Smith offered a classification of offences, which they updated in 2003 (see Table 2.1).

This development of nomenclature reflects not so much a peeling away of the proverbial layers of an onion to reveal a truer core of the phenomenon, but recognition that the phenomenon itself has broadened and mutated. It reflects attempts to add layers around the previous understandings of computer crime to capture an emerging picture. However, there is no single, formally recognised and accepted definition (Wall, 1999). Kowalski (2002: 19-22) noted five different formal and three different informal definitions used by Canadian police forces. Big business has also weighed into the debate arguing for instance that:

any chosen definition of ‘e-crime’ should place its emphasis on crimes against the information infrastructure itself rather than on traditional crimes whose commission the information society infrastructure incidentally makes easier (ICL Corporate Affairs, 2001).

The term “e-crime” is a buzzword used mainly by law enforcement. The term arose following others such as e-mail, e-commerce, e-zines, e-tailer and e-government. The prefix “e-” has been applied almost indiscriminately to

2 That is with a space and to be distinguished from “cybercrime” (Smith, Grabosky and Urbas, 2004: 5-6).
Table 2.1: Grabosky and Smith’s categories of digital crime

<table>
<thead>
<tr>
<th>Category</th>
<th>Examples</th>
</tr>
</thead>
</table>
| Theft of telecommunications services          | obtaining free calls, selling fraudulent telephone cards, cloning telephones; also known as “phreaking”.
| Communications in criminal conspiracies       | online baby-selling rackets, child pornography rings, “grooming” children |
| Information piracy                            | copyright infringement of software or music                                |
| Dissemination of offensive content             | child pornography, defamatory and racial hate materials, instructions for committing crime, spam |
| Electronic money laundering and tax evasion    | laundering via, eg online gambling or e-cash                              |
| Electronic vandalism and terrorism             | Hacking or cracking, viruses, worms, Trojans and other malicious code, website defacement, denial of service attacks, hacktivism |
| Electronic sales and investment fraud          | advance fee (aka Nigerian or 419) scams, other scam emails, online pharmacies |
| Illegal interception of digital information   | telephone tapping, dataveillance including keyloggers, spyware           |
| Electronic funds transfer crime                | credit card fraud                                                        |
| Digital extortion                              | threats of denial of service attacks against online retailers, Mr Water case (*The Age*, 31 Jan 2003) |
| Cyberstalking                                  | harassing email, SMS, telephone calls, websites; DPP v Sutcliffe          |
| Identity-related crime                         | identity theft and fraud, “spoofing”                                     |

Source: Categories from Grabosky and Smith, 2003.
Note: Italicised categories were added in 2003 to their original 1998 classifications.

anything that involves information technology or the Internet. However, the term electronic crime has been given a working definition by law enforcement, reminiscent of Parker’s work, that focuses on digital technologies as:

---

3 In an issue of the European Respiratory Journal, New Zealand researchers report the case of a 32-year-old man who died from deep-vein thrombosis after sitting for extended periods at a computer screen. They suggested the condition be called “e-thrombosis” (*The Age*, 29 Jan 2003).
- The tool used in the commission of an offence;
- The target of an offence; or
- The storage medium for illicit data or information (Etter, 2000: 1).

Grabosky and Smith used the term digital crime previously to describe this “crime that involves information systems as instruments or as targets of illegality” (Grabosky and Smith, 2003: 180), because

information systems operate by reducing data to streams of “1s” and “0s”. Almost every type of information can thus be transmitted across telecommunications networks, which are connected by wires or radio communication (Grabosky and Smith, 2003: 180).

Information systems have now developed to the point that it is insufficient to focus only upon computers as the sole loci of these crimes. For example, since the 1960s, most telephone networks have been digital (Bellamy, 1991: 1). In 2005, there were over 2 billion mobile telephones in use worldwide (Sheriff, 19 Sept 2005). While much electronic crime is technically simple, such as harassing someone via a telephone call, technically sophisticated attacks are developing rapidly. “High tech crime” has been used to refer to sophisticated e-crime, particularly where it has a multi-jurisdictional element (Etter, Dec 2002).

The first two elements of Etter’s tripartite definition of e-crime have been accepted increasingly; however the third is often modified. Kowalski (2002: 6), who uses cybercrime as the catch-all term, excludes “the use of computers by criminals for communication and document or data storage” from her definition terming it “computer-supported crime”, but provides no reason for this. Smith, Grabosky and Urbas include this in their definition of cyber crime as proscribed conduct involving digital technologies that “is incidental to the
commission of other crimes” (Smith, Grabosky and Urbas, 2004: 7, italics in original).

A common distinction made about electronic crime is whether the offence in question is “new” or “pure” and cannot be committed without the involvement of a computer or other digital technology or whether it is a traditional offence simply facilitated by the use of new technologies (DCPC, 2004; Smith, Grabosky and Urbas, 2004: 6). Examples of the first include denial of service attacks, page-jacking and malicious software, such as viruses and spyware (see Etter, 2000). Examples of the latter would include fraud, child sex offences, theft of funds, property or services, manipulation of stock markets (through ramping up of stock prices and ‘pump and dump’ schemes using the Internet) and the above-mentioned harassment by telephone (see Etter, 2000). A further, common distinction is made between insider and external attacks (AusCERT, NSW Police and Deloitte Touche Tohmatsu, 2002).

Given the definition of e-crime, there is no straightforward list of e-crime offences. With a little imagination, almost any illegal activity could be conducted using digital technologies and termed e-crime. However, it is important not to obscure the fundamental nature of an offence, simply because of the involvement of information technology. Thus, it is not useful to consider an assault occasioned using a computer keyboard as electronic crime. Nor should one class a stabbing homicide as e-crime even if the offender planned the crime using his computer. The main offence is homicide. A further, lesser offence may exist if the offender used encryption to cover his planning. Only
the latter is e-crime; under section 3LA, *Cybercrime Act 2001* (Cth).\(^4\) Similarly, Krone (2005a: 1-2) restricts “high tech crime” to that involving ICT to distinguish it from other criminal use of advanced technology, such as genetically modified organisms or modern motor vehicles. However, the involvement of digital technologies in any manner may be important to law enforcement, if there is a need to employ digital evidence analysis\(^5\) in the policing of that incident. In that light, it is easy to see how such diverse crimes as theft, fraud, child sex offences, stalking, drug trafficking, extortion and terrorism are included increasingly under the umbrella of ‘electronic crimes’ (see Nixon, 2002).

The seriousness of e-crime is often communicated by noting the increasing complexity (or ease) of offences. “Click-kiddy” tools that are easily downloaded from the Internet facilitate today’s average hacker. In 2003, “phishing”\(^6\) scams emerged as a major threat to financial institutions and their clients and attacks have become increasingly technical, focused also on identity theft (see Appendix A: Phishing, Pharming and DDoS). Extortion has gone high tech also utilising distributed denial of service attacks and “ransomware” viruses that takes files hostage by encrypting them and demanding ransom payments (F-Secure, 2005; see also Vitek Boden v R).

---

\(^4\) In the future, there might be homicides that could be termed e-crime correctly if remote controlled military systems such as the Special Weapons Observation Reconnaissance Detection Systems (SWORDS) (Regan, 2005) are misused.

\(^5\) Often the term “computer forensics” is used, however this is a syntactical mess, using the noun as an adjective and the adjective as a noun (see especially, Casey, 2004: 31). Forensic computing (McKemmish, 1999) or digital evidence analysis (Casey, 2004: 31) are preferred descriptors for the process of forensic examination of digital evidence.

\(^6\) Early forms of telecommunications theft were called “phreaking” by hackers, replacing the letter with the “ph” from “phone”. It has become common practice to replace the letter f with “ph” in terms such as phishing and pharming (see DCITA, June 2004).
Malicious code is increasingly polymorphic, mutating as it spreads and collecting personal information, as did the Bugbear virus. The trend is for increasing automation and camouflage. In a sickening development, child sex offenders not only use the Internet and peer-to-peer networks to distribute child pornography, but also use web camera technology to participate remotely in the live abuse of children (Gillan, 3 Nov 2003).

Who commits e-crime is used to signal significance (see also Chandler, 1996). Even prior to September 11, 2001, government officials and security experts feared that organised crime groups and extremists were preparing cyberwarfare attacks. According to an article in *Jane’s Intelligence Review* (Galeotti, 2000, cited in Etter 2001) the Chinese triads have employed computer programmers since 1998. The Aum Shinrikyo sect, responsible for the 1995 sarin gas attacks on the Tokyo subway, reportedly diversified into the IT industry installing over a hundred computer systems into Japanese government ministries and major companies, potentially facilitating attacks via these government computers (O’Balance 2001, cited in Etter, 2001). However, fears of a “digital Pearl Harbour” have not yet materialised (Rojas, 2003). They now believe phishing scams are used to fund traditional terrorism and organised crime (Gaudin, 7 March 2005).

Estimates of annual losses and anecdotes of the most severe incidents are also used to indicate the scale of the problem. Perpetual Trustees was left with a AUS$600,000 bill from only two weeks of phreaking activity and the annual cost of phreaking has been estimated by the US Communications Fraud Control Association at US$35-45 billion (Macquarie Telecom, 23 November 2005). Queensland police in Australia reported recently that advance fee scams had netted over AUS$7 million from just 25 people (The Age, 2 Feb 2006). A TruSecure survey suggested that the cost to average-sized companies
of the Blaster worm was US$475,000 (Varghese, 23 Sept 2003). In 2005, denial of service attacks (DoS) were reported as causing the most financial loss to Australian public and private sectors (AusCERT et al, 2005: 4) and incidents such as the United States Post Office investigation of a couple running a child pornography bulletin board system (BBS) that uncovered over 293,000 clients underline the extent of that problem (Nixon, 2002; see also Krone, 2005a).

However, it is particularly difficult to estimate the cost of e-crime to the Australian community. Australian police crime statistics do not report on e-crime, generally because, as discussed above, e-crime relates to modi operandi rather than a single category of crime. What is known about the extent and cost of e-crime in Australia comes primarily from victimisation surveys of Australia’s largest companies (Deloitte Touche Tohmatsu and Victoria Police, 1999; AusCERT, NSW Police and Deloitte Touche Tohmatsu, 2002; AusCERT, AFP, Queensland Police, South Australia Police and Western Australia Police, 2003; AusCERT et al, 2004; AusCERT et al, 2005). Thus, what is reported is subject to the common problems of victimisation surveys such as low response rates and under-reporting, telescoping, non-representative sampling, leading questions (Smith, 2001: 5) and inconsistent definitions.7 Often figures are “guesstimates”. For example, the 2003 TruSecure survey quoted above did not believe their respondents, arguing, “technical people who participated in this study underestimate total costs by about seven-fold” and so extrapolated higher figures. One is cautioned about accepting claims about the exorbitant cost of e-crime wholeheartedly that might belie self-interest in the security industry or attaining a greater share of scarce policing resources (Wall, 1998: 214; Smith, 2001: 13).

7 For example, in the 2002 AusCERT survey a security incident might have been either “real or perceived”.
**Defining public and private policing**

This thesis is concerned with policing of e-crime as performed by public police and their private sector counterparts. Reiner (1994: 722) defines “policing” as:

> an aspect of social control processes which occurs universally in all social situations in which there is at least the potential for conflict, deviance, or disorder. It involves surveillance to discover actual or anticipated breaches, and the threat or mobilization of sanctions to ensure the security of order. The order in question may be based upon consensus, or conflict and oppression, or an ambiguous amalgam of the two, which is usually the case in modern societies.

From Reiner’s definition we see that policing is just one form of social control aimed at maintaining security and that as a process policing is not the province of only taxpayer funded, government police forces. A spectrum of actors undertakes policing; who are often labelled as either public or private police. What distinguishes private from public policing? Stenning and Shearing (1979: 7) first wrote that it “is the fact that they are (a) privately employed and (b) employed on jobs whose principal component is some security function”. These two criteria distinguished public, private and other members of the public “who may perform security functions as an incident to, rather than as a central component of their regular occupations.” However policing is no longer dichotomous (if it ever was) and includes a myriad of

---

8 The topic of this thesis should not be confused with “e-policing”, which is the enhanced service delivery of policing using information technology. Chan J., Brereton, Legosz and Doran (2001) used the term “e-policing” to title their book about the impact of information technology on the Queensland Police Service and do not discuss e-crime (see also Judge, 2002).
“hybrid” examples, again often characterised by varying their degree of
“publicness” and “privateness” (see especially, Button, 2002; Table 2.2).
Worldwide there has been a separation of those who authorise policing and
who provide it; and both functions are moving away from government
(Bayley and Shearing, 2001). Bayley and Shearing prefer to term this as
“multilateralisation” rather than privatisation, because of the various
combinations apparent between those who now authorise and fund and those
who provide policing. They have observed auspice-provider combinations
that are public-public, public-private, private-public and private-private.
Further, they have noted a transfer of policing functions to transnational and
international agencies, placing them beyond traditional nation-state
boundaries (Bayley and Shearing, 2001). This is indicative of new economies
characterised by economic rationalism, managerialism, microeconomic reform
(Davids and Hancock, 1998), deregulation, increasing integration of capital
markets and the relentless pace of technological advancement (Geis and Geis,
2001: 12).

Table 2.2: Button’s classification of policing

<table>
<thead>
<tr>
<th>Category</th>
<th>Mode of provision</th>
<th>Funding</th>
<th>Relationship</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Public police bodies</td>
<td>Public</td>
<td>Public</td>
<td>Public</td>
<td>Public</td>
</tr>
<tr>
<td>2. Hybrid Policing bodies:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Central and decentralised</td>
<td>Public</td>
<td>Public</td>
<td>Varies</td>
<td>Varies</td>
</tr>
<tr>
<td>public policing bodies</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Specialised police organisations</td>
<td>Varies</td>
<td>Varies</td>
<td>Varies</td>
<td>Public</td>
</tr>
<tr>
<td>Private policing (non-private</td>
<td>Private</td>
<td>Private</td>
<td>Varies</td>
<td>Private</td>
</tr>
<tr>
<td>security)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Voluntary policing</td>
<td>Private</td>
<td>n/a</td>
<td>Public</td>
<td>Private</td>
</tr>
<tr>
<td>4. Private security</td>
<td>Private</td>
<td>Private</td>
<td>Private</td>
<td>Private</td>
</tr>
</tbody>
</table>


Button (2002: 8-16) proposes a classification based on Jones and Newburn’s
(1998) factors that conceptualise the dichotomy: who provides the policing,
either the state or the market (mode of provision); sources of funding as either
taxation or fees; relationship between provider and client, whether the principle of service is a “right” of all or purchased (relationship); and the status of those who provide the policing, evidenced often by whether they hold special powers. Sarre and Prenzler (2005: 4) also offer a new definition to account for personnel and organisations excluded previously from definitions:

Private police are those who are employed or sponsored by a commercial enterprise on a contract or ‘in-house’ basis, using public or private funds, to engage in tasks (other than vigilante action) where the principal component is a security or regulatory function.9

This thesis considers primarily interactions between traditional, public police forces and private investigators working for financial institutions or investigation companies for whom policing e-crime is a commercial enterprise and who fit into Button’s private security category (see generally Johnston, L. 1999; Button, 2002). Generally, private investigators are considered part of the private security industry, because their broader purpose is loss prevention and security, even though they may focus upon policing (George and Button, 2000: 15). For the readers’ ease, public police may also be referred to as either police or law enforcement and private police as private investigators. Also considered are IT administrators for whom security is often not their primary role and policing is often a voluntary by-product of their ordinary occupations when their assistance is enlisted by police or private investigators.

---

9 This definition is superior to the one offered by Sarre (2005: 62) which would inadvertently have unsworn personnel of public police services, such as intelligence analysts, labelled as private police.
Policing involves surveillance, investigation and threat or actual punishment of offenders according to Reiner (1994: 722). For public law enforcement agencies policing e-crime means investigation based on reported incidents or proactive intelligence, often using digital evidence analysis, apprehension of suspects, prosecuting using the criminal law and court ordered sanctions including imprisonment. In the private sector, the more familiar processes might be monitoring of intrusion detection software and other security systems, IT auditing, formal or informal investigation optionally involving law enforcement and prosecution using either in-house regulations or civil law. In the private sector, investigations may be either litigious or non-litigious (Stucki, 2002). Although Gill and Hart’s (1997b: 557-58) study of British private investigation agencies found that defence work most often characterised their involvement in criminal investigations, investigations of fraud for private companies focused primarily on establishing causes of loss and enacted private justice.\textsuperscript{10} Sanctions might involve dismissal, demotion or civil penalties.

The Internet is renowned for “voluntary policing” of the activities of users (see also Wall, 1998: 205-6). On Internet Relay Chat (IRC) there are IRCops who have the power to banish users from the chat rooms (Rhapsody, 2003). Other examples include the infamous Gnutella “Wall of Shame” that lists the IP addresses of computers (and hence quite often the people using them), which have been used to search for child pornography (http://www.zeropaid.com/busted/), and Open Relay Black lists that list people who run insecure mail-servers and permit exploitation by spammers (Ozcableguy, 2002). “Private security” is provided by tech support personnel

\textsuperscript{10} Private justice refers to “the localized non-state systems of administering and sanctioning individuals accused of rule breaking or disputing within groups or organisations” (Henry, 1987: 45-6).
who monitor their company’s services, such as chat rooms, online bulletin boards, Massively Multiplayer Online Role Playing Games and the like. Most ISPs also have an “abuse” email address for users to report illegal or abusive behaviour by their clients. Other activities often carried out by the same private sector personnel, such as developing security policies and installing security measures like anti-virus software and firewalls, are not considered policing; instead these are crime prevention activities and not the focus of this thesis.\(^\text{11}\) However, some crime prevention initiatives blur the line between prevention and surveillance to detect offenders such as digital rights management software installed surreptitiously by the music industry that can “phone home” information about compact discs played in a user’s computer (see Russinovich, 31 Oct 2005, 4 Nov 2005).

**Police investigation of e-crime in Australia**

Australia comprises six states and two territories, including the Australian Capital Territory (ACT) location of the nation’s capital Canberra. Victoria is Australia’s second-smallest state in area, approximately the same size as Britain. In 2004, Victoria had an estimated population of 4,973,000 residents (ABS, 2005). Each state and territory has a police force and there is also the Australia Federal Police. In

\(^{11}\) Crime prevention is any measure that reduces the damage of harmful or criminal acts, other than the enforcement of the criminal law (Van Dijk and de Waard, 1991). Anti-virus and firewalls are crime prevention, because generally no attempt is made to identify or sanction an offender.
2004/05 there were 10446 sworn police officers in the state of Victoria, having grown from 9488 in 2000/01 and representing twenty-three percent of the total of 45,201 sworn police officers throughout Australia (Australian Government Productivity Commission, 2006: Table 5A.16). The number of detectives in Victoria Police is much less at 936 in 2006.

Early cases of e-crime in Australia were dealt with using property offences like larceny and reports do not focus on the investigation. For example, in *Kennison v. Daire* (1986) 160 CLR 129 the accused was charged and convicted of larceny when he “deceived” an offline automatic teller machine (ATM) into dispensing funds using the debit card for an account he had already closed (see also *R v Evenett* (1987) 2 Qd R 753; *R v Baxter* (1987) 84 ALR 537).

Similarly, no investigative details are given about the BBS operator known as Blue Thunder who pleaded guilty to credit card fraud in the Melbourne Magistrates court in 1988 (Dreyfus, 1997: 62). However, we know that in New York in 1987 a thief who forged ATM cards after “shoulder surfing” for PIN numbers was apprehended when the manufacturer programmed their bank network to recognise the flawed cards and alert security (Morrison, 1990: 8).

**Introduction of Computer Crime Investigation units**

In January 1989 the media reported allegations that Australian hackers were responsible for stealing US$500,000 electronically from Citibank (Dreyfus, 1997: 159-163). Ken Day, a former AFP detective sergeant, recalled:

> At that particular time, there was no law in Australia directly relating to computer crime. There was really very little the federal police could do other than take it on board as an intelligence probe to try and find out the facts and report to government that there was a problem with lack of legislation (Interview of Ken Day, *In the Realm of Hackers*, 2002).
The Victoria Police Computer Crime Section of the Fraud Squad was the first computer crime unit to be established in Australia in that month of January 1989, because most computer crime activity was originating from Victoria (Thompson, 1990: 28). At that time, globally, there were approximately eleven computer crime investigation units in the United States, one in Britain in the Metropolitan Police and one in the Royal Canadian Mounted Police (Thompson, 1990: 28). The US Federal Bureau of Investigation (FBI) had formed its Computer Analysis and Response Team (CART) in 1984, however this only became fully operational in 1991 (FBI, 2004). Even with the introduction of Australia’s first computer crime legislation in mid 1989, the Crimes Legislation Amendment Act 1989 (Cth), the priority given to computer crime investigation was low:

The AFP had a very low computer literacy at that point in time; we’re talking about people still using typewriters. It was still the carbon paper days. And so the unknown element of what computers were resulted in a very low opinion of people, to say, ‘Well, I don’t use computers. It’s not important’ (Interview of Ken Day, In the Realm of Hackers, 2002).

Computer crime was not a popular choice amongst police according to Ken Hunt, a former AFP detective superintendent: “Most of my colleagues, most of the other people at my level, thought it was a wank. And that I should be out there investigating ‘real crime’” (Interview of Ken Hunt, In the Realm of Hackers, 2002).

The investigation of electronic crime is highly technical and investigators struggled initially to build their capacity to investigate successfully. Any

---

12 A Victoria Police investigation later found the allegations that Australians hacked Citibank were unfounded (Dreyfus, 1997: 161).
Police officer can tell you the four points to be proven in a criminal investigation (Fairchild, 1994: 115):

- the identity of the offender;
- the crime;
- the nexus between the offender and the crime; and
- the whereabouts of the offender.

Specifically, the AFP had to work out how to record intercepted computer data to gather evidence of the above elements (In the Realm of Hackers, 2002).

From the investigators’ point of view, it was a very steep learning curve. Most of us had computers, our own computer. But we would not have known what would happen if we lifted up the bonnet and had a look inside. It was very difficult just trying to work out what all these brand new terms were. I had a difficulty early in the piece just understanding what is now I suppose the Internet. How did it work? Who paid for it? Why could you get over to the United States and it wouldn’t cost you a penny (Interview of Ken Hunt, In the Realm of Hackers, 2002)?

Resources were scarce in the early days of police computer crime investigations:

Initially we had to borrow computers. We borrowed computers from banks. Computers they didn’t need, older ones. We had to borrow quite a bit of equipment from anybody we could speak nicely to (Interview of Ken Hunt, In the Realm of Hackers, 2002).

Thompson (1989) described other difficulties faced by Australian law enforcement in the detection, investigation and prosecution of computer crimes at the inaugural Australian Computer Abuse conference. These included the low visibility of incidents hampering detection, the impact of
committing crimes across large distances and jurisdictional boundaries, the difficulty of discovering and understanding the methodology used, the volatile nature of digital evidence, difficulty obtaining physical evidence, the admissibility of evidence and explaining it to the court.

Early cases were lengthy and criticised for lenient sentences. On 2 April 1990, the Australian Federal Police raided the homes of three Victorian hackers known as the Realm Hackers. The Australian Federal Police Fraud and General Crime Computer Crime Section was formed subsequently in July 1990. Final charges were filed on 5 May 1992 and the Realm Hackers subsequently pleaded guilty to various charges of unauthorised access. On 3 June 1993, Electron was convicted and given a six months suspended sentence and community service. Later that year, Phoenix and Nom also escaped prison, sentenced to community service and good behaviour bonds (Dreyfus, 1997). Other early police operations, like the 1990 Operation Sundevil in the United States that targeted hackers using bulletin boards, were criticised for heavy-handedness and unfocused seizure of IT equipment (Hafner and Markoff, 1991; Sterling, 1993) or poor forensic practices (Campbell, D., 26 Nov 1997).

---

13 In 2000, the FBI demonstrated questionable legal tactics when they seized evidence from the computer tech.net.ru in Chelyabinsk, Russia without first obtaining a search warrant or permission and cooperation from Russian authorities. They had lured two Russian hackers, Gorshkov and Ivanov, to US soil with a job offer and asked them to demonstrate their hacking prowess (Cha, 19 May 2003). The unsuspecting hackers did so opening a conduit to their computers in Russia. The investigators then arrested them and retrieved evidence from the still open connection with which they convicted the pair. In response to the suspect search and seizure, the Russian Federal Security Service laid charges against FBI agent Michael Schuler for illegal hacking (Cha, 20 May 2003; Jahnke, 2005). US courts later upheld their police tactics.
In the early 1990s, law enforcement began coordinating large scale, international operations to police Internet child pornography distribution and child sex offences (Krone, 2005a). Australian police agencies have participated in many of these including operations Longarm (Krone, 2005a), Avalanche (USA Customs), E-Circles.com (FBI), Macron (USA), Mondo (German Police), Kinderschultz (German Police), Auckland (United Kingdom), Southside (US Customs) and Candyman (FBI) (ACC, 2003: 17). In 1998, Operation Cathedral coordinated law enforcement officials in 13 countries including Australia as they simultaneously conducted raids on suspected paedophiles in the Wønderland Club, which resulted in the arrests of dozens of suspects. Two Western Australian men were convicted.

The patchwork nature of the Internet means that the evidence trail may pass through innumerable hosts, requiring legal paperwork for each and gambling on evidence retention against business demands. The potential sources of digital evidence to be considered have also multiplied and are increasingly wireless and miniature (National Institute of Justice (US), 2001: 9-22) and cases often result in numerous leads and mountains of evidence (Krone, 2005a). Other impediments that have been documented in recent years in relation to transnational offending include identifying suspects, extradition, lack of or inconsistent legislation, deciding jurisdiction, encryption, mutual assistance and logistical issues such as navigating different global time zones and languages (Smith, 2004a).

Each of the other Australian state police services would eventually create dedicated computer crime investigation units (see Table 2.3). Prior to that, detectives working out of their local areas or fraud squads handled computer crime cases (Tasmania Police, 27 Feb 2006, personal communication; Queensland Police, 28 Feb 2006, personal communication). Thompson (1990:
28) noted that the role of these units included tasks outside the normal investigative role, including researching and reviewing legislation to recommend amendments and maintaining knowledge of current digital technologies. In the late 1990s, Victoria Police’s team was renamed the Computer Crime Investigation Squad.

In 2000, the Australian Police Minister’s Council decided that e-crime was to be one of the top three priorities for 2001 (COAG, 2002: 387). The Prime Minister and State and Territory leaders agreed to adopt model computer offences by the end of 2002 (NCA, 5 April 2002). The Cybercrime Act 2001 (Cth) gave police additional investigative powers and placed an onus upon companies to install technological security measures (MCCOC, 2000, 2001; Pearce, 23 October, 2002). Victoria was second to introduce the model legislation at the state level, behind New South Wales, through sections 247A-L of the Crimes (Property Damage and Computer Offences) (Vic) Act 2003 (see Appendix C: Victoria’s model computer offences legislation). The model legislation introduced offences for:14

247B - Unauthorised access, modification or impairment to commit a serious offence;
247C - Unauthorised modification of data to cause impairment;
247D - Unauthorised impairment of electronic communications;
247E - Possession of data with intent to commit computer offence;
247F - Produce, supply of data with intent to commit a computer offence;
247G - Unauthorised access to restricted data;

14 Western Australia drafted computer crime legislation in 2001 that would include the act of copying from a computer as “stealing information from a computer”, however this legislation was never passed (Victoria Police, 2003, personal communication; unpublished draft legislation).
247H - Unauthorised impairment of data held in a computer disk, credit card etc; and

247K and L - Damage or disruption of (or threat against) a public information system.

Most Australian state and territories have now introduced the model legislation.

Worldwide police have realised that the pervasiveness of digital technologies requires all law enforcement officers to develop skills as first responders to digital evidence (Casey, 2004: 27). From their original investigative focus, the Victoria Police Computer Crime Investigation Squad has evolved into a support service to assist other police members. The word “Investigation” was removed from the Victoria Police Computer Crime squad’s (CCS) title in 2002 to reflect that the squad normally no longer conducts its own investigations; although it can and still does occasionally. CCS remains part of the Major Fraud Investigation Division (MFID) of Victoria Police, which has approximately 135 members in CCS, an Initial Action Squad, three Investigation Squads and an Asset Recovery Squad. The most common support CCS provides is digital evidence analysis of seized computer

---

15 See Appendix B for CCS’s current charter that still reflects its original proactive investigation role.
Table 2.3: Australian police e-crime investigation units

<table>
<thead>
<tr>
<th>Australian police service</th>
<th>Name of current units</th>
<th>Date first unit established</th>
<th>Current staffing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Victoria Police</td>
<td>Computer Crime Squad &amp; Sexual Crimes Squad</td>
<td>January 1989</td>
<td>CCS: 9 sworn officers, 2 sworn analysts, 1 unsworn analyst</td>
</tr>
<tr>
<td>Australian Federal Police</td>
<td>Online Child Sex Exploitation Team &amp; Computer Forensic Teams†</td>
<td>July 1990*</td>
<td>OSCET: 53 members; CFT Melbourne: 5 members</td>
</tr>
<tr>
<td>Australian Federal Police (ACT policing)</td>
<td>Territory investigations group ‡ (incl. Fraud and Sexual Assault &amp; Child Abuse teams)</td>
<td>Not available</td>
<td>Not available</td>
</tr>
<tr>
<td>New South Wales</td>
<td>E-Crime unit &amp; Child Exploitation Internet Unit</td>
<td>Not available</td>
<td>Not available</td>
</tr>
<tr>
<td>Western Australia</td>
<td>Computer Crime Investigation Team</td>
<td>November 1997</td>
<td>9 sworn, 1 unsworn</td>
</tr>
<tr>
<td>Queensland Police</td>
<td>Computer Crime Investigation Unit, Forensic Computer Section, Child &amp; Sexual Assault Unit</td>
<td>Sept / Oct 2000</td>
<td>CCIU: 4 sworn officers and 1 forensic computer specialist</td>
</tr>
<tr>
<td>Northern Territory</td>
<td>Computer Crime unit</td>
<td>2001</td>
<td>3 sworn officers</td>
</tr>
<tr>
<td>South Australia Police</td>
<td>Electronic Crime Section (ECS)</td>
<td>March 2003</td>
<td>Not available</td>
</tr>
<tr>
<td>Tasmania Police</td>
<td>Fraud Investigation Services unit</td>
<td>March 2003</td>
<td>4 permanent members, 2 on-call forensic computer examiners</td>
</tr>
<tr>
<td>Australian High Tech Crime Centre</td>
<td>(includes Joint Banking and Finance Sectors Investigation Team)</td>
<td>July 2003</td>
<td>17 sworn &amp; unsworn AFP agents, 2 VicPol, 2 NSWPol, 1 from each other state police force, ABA, Customs, 5 from banks</td>
</tr>
</tbody>
</table>

Sources: AHTCC website, AFP Annual report 2004/05 and personal communications.
* Originally the Fraud and General Crime Computer Crime Section.
† CFT laboratories are located in Brisbane, Canberra, Melbourne, Sydney and Perth.
‡ Unit not dedicated to only e-crime.
equipment, including hard drives, mobile telephones, personal digital
organisers and various other storage media. CCS provides assistance with
brief preparation, interviews and taking statements involving digital evidence
and computer crime law. The squad has developed training materials on an
intranet for police members on investigative techniques, warrants and search
and seizure. CCS also provides liaison between Internet Service Providers and
police who need to obtain information from ISPs for their investigations. At
the time of writing, a Detective Inspector manages the Computer Crime
Squad with a Detective Senior Sergeant as Officer in Charge. The strength of
CCS increased from 11 staff to 13 staff in 2003. The squad also comprises two
detective sergeants, seven senior constables detectives, an analyst, a technical
intelligence officer and an unsworn Computer Systems Engineer / Analyst.
Ten CCS members undertake evidence analysis tasks.

It has long been argued that state police forces in Australia have a loosening
grip on what they term “high policing” or “elite policing” as other specialised
regulatory agencies assume responsibility for drug trafficking, organised
crime, money laundering, e-crime and the like (O’Malley and Palmer, 1996:
151-2). In addition to the police forces listed in Table 2.3, a plethora of other
Australian law enforcement and government agencies have been responsible
for investigating particular forms of e-crime. These have included the
Australian Broadcasting Authority (illegal online content), the Australian
Communication Authority (commercial spam),16 the Australian Tax Office
(tax fraud), Australian Competition and Consumer Commission (Internet
scams), the Australian Crime Commission (criminal intelligence on e-crime),
AUSTRAC (money laundering), Australian Customs Service (child
pornography), Centrelink (social security fraud) and the Australian Securities

16 On 1 July 2005, the ABA and ACA roles were taken over by the Australian Media and
Communication Authority.
and Investment Commission’s (ASIC) Electronic Enforcement Unit (online scams, financial fraud). The Defence Signals Directorate’s (DSD) Information Security Group also receives incident reports on computer security breaches (DSD, 2004). Forums for policy development include the Australasian Police Commissioners Electronic Crime Working Party, Action Group into the Law Enforcement Implications of E-commerce (AGEC), Hi Tech Crime Managers Group, Australasian Identity Crime Working Party, ACCF National Approach to Fraud Control Working Party, ACCF Working Party into Online Child Abuse, National Heads of Fraud, ACC National Fraud Help Desk, ACC E-Crime Help Desk, ACC Identity Fraud Register Pilot program, Trust and Information Sharing Network and GovCERT.au. Australian police e-crime investigators have also set up police-only Digital Evidence Groups where they can discuss investigation techniques. The list is staggering and yet not comprehensive and does not include numerous international forums in which Australia participates.

**Australian High Tech Crime Centre**

In March 2001, Australia’s police chiefs called for the establishment of a national centre to police electronic crime, stating that “It’s just not possible for every state and territory to have the capability to look at all of this (separately)” (Chulov, 2001). The Australian Federal Police proposed the creation of a national, centralised organisation for policing electronic crime to be called the *National Electronic Crime Centre* (NECC) (AFP, 2000). The proposal aimed to establish the NECC as “the primary means through which law enforcement and regulators are able to interact with the private sector and to coordinate response to threats to the National Information Infrastructure” (AFP, 2000: s.5.1.3). The NECC proposal focused upon bringing together law enforcement, intelligence and regulatory agencies;
defining the role of the private sector as simply an information resource. In July 2003, the Australian High Tech Crime Centre (AHTCC) was formed to provide this national capability. The AHTCC is the national agency responsible for serious, complex and multi-jurisdictional high tech crimes (AFP, 2004) having taken over responsibilities held formerly by the ACPR and various sub-committees. Its mission is to:

- provide a national coordinated approach to combating serious, complex and multi-jurisdictional high tech crimes, especially those beyond the capability of single jurisdictions;
- assist in improving the capacity of all jurisdictions to deal with high tech crime; and
- support efforts to protect the National Information Infrastructure (AFP, 2004).

The formation of AHTCC is part of Australia’s “capability model” for responding to e-crime (Electronic Crime Steering Committee, ACPR 2001: 4). Staffed by seconded officers from each of Australia’s police forces, it represents a joint force operation (JFO), which is an increasing trend in policing (LeBeuf, 2001). The AHTCC is hosted administratively by the AFP and governed by its own Board of Management comprising all Australian Police Commissioners and currently Chaired by the Commissioner of the South Australian Police. The Commissioner of New Zealand Police also observes board meetings. A Director who is an AFP Federal Agent heads the AHTCC. The core team at the Centre includes investigators, technical specialists, intelligence officers, policy advisors and support staff (AFP, 2004; see Table 2.3). The Centre coordinates high tech crime matters involving Australian law enforcement, federal government and international agencies. The Centre draws its legal powers from the Crimes Act 1914 (Cth). It provides intelligence services, liaison, alerts and advisories to government and the
community. The Australian High Tech Crime Centre has also cemented a research relationship with the Australian Institute of Criminology (Krone, 2004; Krone, 2005a,b,c) to assemble knowledge of high tech crime issues such as preventative measures, best practice investigative tools and techniques, expert advice, training and education (AFP, 2004: 2). The AHTCC provides an online reporting service for e-crime incidents. Contrary to the NECC proposal, AHTCC also formed the Joint Banking and Finance Sector Investigation Team that is a public-private partnership for policing phishing, which is discussed in detail in Chapter Seven.

**Operation Auxin**

The trend toward large scale, coordinated, multi-national policing operations continued with Operation Auxin in 2004, codenamed Operation Lodden in Victoria. The US Customs Service referred Operation Auxin to Australian police. Auxin led to charges against more than 200 people in Australia, including 68 Victorians (*The Courier Mail*, 4 October, 2004). Auxin received lots of news coverage as police in other states used video cameras to record the serving of warrants and arrests, images of which appeared in the media (Mitchell, 5 October, 2004: 19). In the wake of Operation Auxin, four men took their own lives and Victoria Police admitted they needed to review the handling of ‘at-risk’ suspects (*The Courier Mail*, 4 October, 2004). It is possible that the situations of these suspects was exacerbated by the intense media coverage of these coordinated raids and stigma attached to having been caught up in such a notorious child pornography investigation. The police minister at the time said it was important that these people did not face a “death penalty by default” (*The Courier Mail*, 4 October, 2004).¹⁷ At the end of

---

¹⁷ This recognition is important in light of comments by readers on the Herald Sun website: “Police shouldn’t be worried about the child porn suicides. Sure they weren’t found guilty in
2004, the AHTCC reverted responsibility for online child exploitation and child pornography cases to the AFP’s Online Child Sex Exploitation Team, so as to focus upon financial e-crimes.

Arguably, the Internet is an under-policed area, however there are initiatives forming to address this, such as the Virtual Global Taskforce. This initiative plans to introduce a 24/7 online presence and “patrolling” by public law enforcement (Virtual Global Taskforce, 2005). The idea is that police from Australia, Canada, the UK and the USA will rotate shifts at their computers, making their presence known in public chat rooms and other cyberspaces where cyberstalking, grooming of children or dissemination of child pornography have been known to occur. Introducing anti-“grooming” laws supported this initiative (Krone 2005b). Operation PIN is another Australian operation, whereby police set up fake “honeypot” child pornography sites to lure offenders. Besides investigation and prosecution, these operations aim to undermine notions of Internet anonymity (Krone, 2005a).

**Victorian Fraud Information Reporting Centre**

The Victorian Parliamentary committee inquiry into Fraud and E-Commerce held during 2004 found that information on the extent of electronic commerce-related crime and fraud in general could be improved greatly (DCPC, 2004: 86). The committee recommended the creation of a dedicated Victorian Fraud Information Reporting Centre (VFIRC) within Victoria Police (DCPC, 2004: 86-88). The purpose of the VFIRC would be to “coordinate and respond to all aspects of fraud reporting, prevention and the provision of

---

a court, but their suicides are in effect confessions of guilt made outside a court” (Herald Sun, 8 October, 2004).
information and statistics” (DCPC, 2004: 86). To fulfil that role the Centre would:

i. collect and disseminate information about the nature and extent of fraud occurring across Victoria;
ii. collect and publish statistics on fraud; and
iii. receive complaints of fraud from members of the public and public and private sector organisations for referral to appropriate agencies for investigation (DCPC, 2004: 88).

The Committee recommended location of the Centre within the portfolio of Specialist Operations—not in Operations or in the Major Fraud Investigation Division—as the proposed centre would not undertake any policing or intelligence function.

VFIRC would be staffed by civilian analysts with backgrounds in law, commerce, banking, statistics, and criminology, rather than sworn police officers. It would receive dedicated funding administered by Victoria Police and seek to attract partial funding from the private sector (DCPC, 2004: 86).

These analysts would follow the progress of incidents from reporting to finalisation, regardless of whether they were referred for investigation to Victoria Police or another agency (DCPC, 2004: 87). The centre would be facilitated by mandatory fraud reporting legislation. Public and private sector organisations becoming aware of fraud would have to report their incidents to the VFIRC within ten days (DCPC, 2004: xxi).

Private investigation of e-crime in Victoria

Little has been published about early commercial e-crime investigation and from the popular literature, such as Stoll’s (1989) Cuckoo’s Egg, one might
conclude that early private investigation of e-crime amounted to individual obsession as much as hacking is also portrayed (see Dreyfus, 1997). Stoll’s tale of investigating a hacker, triggered by a 75 cent accounting discrepancy, is one of sleepless nights and personal sacrifices, inventing his own intrusion detection systems and navigating various police brush-offs that it was not their “bailiwick”, eventuating in the arrest of five Germans in the employ of the Russian KGB, known as the Hanover hackers. However, despite the lack of public stories, investigation in the private sector certainly began with providers of telecommunications services. For example, in 1975 the surveillance chief for AT&T, one of the largest telecommunications carriers in the United States, revealed to Newsweek magazine that in 1964 AT&T monitored approximately 33 million toll calls over the period of seven years till 1970 to find phreakers. The company obtained two hundred convictions from this (Krebs, 14 Feb 2003).

Following early virus outbreaks, the private sector formed an international network of computer emergency response teams (CERTs). CERT Coordination Center was created in 1988 at the University of Carnegie Mellon following the Morris worm outbreak. The Forum of Incident Response and Security Teams (FIRST) was formed in 1990 in response to the lack of coordination between CERT teams following the WANK worm outbreak (see Dreyfus, 1997 for a description of the WANK worm). Australia’s CERT, AusCERT, was formed in 1993. AusCERT is an independent subscription-based, not-for-profit team of 20 security professionals, some of whom hold high-level security clearances, hosted in Brisbane at the University of Queensland (AusCERT, nd; Riley 2006). AusCERT provides incident management services and operates an email subscription alert service that warns readers about network threats and responses. It also provides an IT Incident Reporting Scheme. With Australia’s police forces, AusCERT

In the Australian context, development of commercial private security has been a relatively new phenomenon (Swanton, 1993) and a few firms dominate the industry (Prenzler and Sarre, 1998). While there has been a proliferation of local companies offering computer security services in Australia, most of these companies provide security services rather than policing services, as defined above. Most focus upon provision of anti-virus software, intrusion detection and other security technology. In terms of private policing of e-crime, there has been growth in small to mid-size firms offering forensic digital analysis services in Australia and the Australian forensic software industry is competitive internationally. Private fraud and digital forensic investigators are becoming more commonplace in the financial, IT, telecommunications, retail and government sectors. The “big four” accountancy firms have also created their own local forensic investigation arms: KPMG Investigation and Security, Deloitte Forensic, PriceWaterHouseCoopers Computer Forensics and Litigation Support and Ernst & Young Fraud Investigation and Dispute Services. Other large firms including the major Australian banks have established their own in-house investigation teams. Of the many different types of electronic crime, these investigators focus mainly upon those involving monetary loss to their employers, such as fraud and theft. To a lesser degree, they also police the morality of their companies, by investigating instances of employees downloading objectionable materials or wasting company resources.
Increasingly, incident investigation is a regulatory requirement of instruments such as the US Sarbanes-Oxley Act 2002 and ISO 17999 (Stephenson, 2004).

Emerging in Australia are private organisations in relation to e-crime that fit Button’s subcategory of private policing (non-private security). These organisations or individuals provide investigation services instead of security services. The best examples of this category in Australia are Music Industry Piracy Investigations (MIPI), which investigates and prosecutes piracy for the music industry and the Business Software Alliance of Australia (BSAA), which accepts reports from the public and investigates and litigates against software copyright infringements on behalf of its software vendor members. Both MIPI and the BSAA undertake raids of premises through the use of court sanctioned Anton Piller orders.

It is difficult to quantify exactly the size of the private e-crime investigation industry in Australia, which is a subset of all investigators. Investigator numbers are often aggregated in figures relating to the rest of the security industry. In Victoria, a (private) investigator is defined by section 3 of the Private Security Act 2004 (Vic) as:\(^{18}\)

\[\text{a person who on behalf of any other person is employed or retained:}\]
\[\begin{align*}
\text{- to obtain and furnish information as to the personal character or actions of any person or as to the character or nature of the business or occupation of any missing person; or} \\
\text{- to search for missing persons.}
\end{align*}\]

\(^{18}\) The Private Security Act 2004 came into effect on 1 July 2005, tightening licensing and training requirements in Victoria for private security personnel, including investigators, in the wake of the death of Australian test cricketer David Hookes following an altercation with a bouncer. See also Private Security Regulations 2005 Vic.
The most recent Victorian figures compiled in 2004 identified 1827 holders of inquiry agent (investigator) licenses accounting for approximately ten percent of the Victorian private security industry (Department of Justice, Victoria, 2005; see Table 2.4). Quantification is difficult due to inconsistent licensing schemes across Australia (Sarre and Prenzler, 2005: Ch 1). The figures do not include those not requiring licenses by virtue of working only for their employer. Counts of individuals working in the industry are also difficult as some may hold multiple licenses in different states or may work casually (Golsby, 1998: 121) and have been made even more difficult in Victoria by the abolition of combined security guard / crowd controller licenses in Victoria by the Private Agents Regulations 2003 (Vic) such that most (over twenty thousand) Victorian security personnel now hold two licenses.

Table 2.4: Comparison of Victorian investigator license holders to other security license holders, 1980-2004

<table>
<thead>
<tr>
<th>Year</th>
<th>Licensed investigators / Percent total</th>
<th>Other security license holders*</th>
<th>Victorian total</th>
</tr>
</thead>
<tbody>
<tr>
<td>1980</td>
<td>462 (11.1%)</td>
<td>3670</td>
<td>4132</td>
</tr>
<tr>
<td>1990</td>
<td>1227 (15.8%)</td>
<td>6554</td>
<td>7781</td>
</tr>
<tr>
<td>1992</td>
<td>1095 (9.4%)</td>
<td>10554</td>
<td>11649</td>
</tr>
<tr>
<td>1999</td>
<td>1287 (6.0%)</td>
<td>19993</td>
<td>21280</td>
</tr>
<tr>
<td>2000</td>
<td>1447 (6.3%)</td>
<td>21585</td>
<td>23032</td>
</tr>
<tr>
<td>2001</td>
<td>1657 (n/a)</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>2002</td>
<td>1801 (7.1%)</td>
<td>23497</td>
<td>25298</td>
</tr>
<tr>
<td>2004</td>
<td>1827 (3.7%)</td>
<td>47677†</td>
<td>49504†</td>
</tr>
</tbody>
</table>

Sources: 1980 & 1990 (Golsby, 1998); 2001 (Prenzler and King, 2002); all other years Department of Justice, Victoria (April 2005).

* Includes security firm, security guard, crowd controller and security guard/crowd controller licenses.

†This doubling of license holders reflects the abolition of dual security guard/crowd controller licenses in 2003.

In 2004, the ratio of licensed Victorian private investigators to sworn Victoria Police members was 1 to 17.5. The ratio of private investigators to Victoria Police detectives is 2:1.
Private investigators are represented in Victoria by several security industry
associations including the Association of Investigators and Security
Professionals (AISP), Victorian Security Institute (VSI), Australian Security
Industry Association Limited (ASIAL), International Association of Financial
Crimes Investigators (IAFCI) and the Australian Institute of Professional
Investigators (AIPI). ASIAL, Australia’s largest security industry association,
does not keep statistics on the number of investigators in their memberships,
stating, “we do not keep specific data on this category of security service”
(ASIAL, 8 March 2006, personal communication); their website indicates a
focus on security guards and installers. IAFCI’s Southern Region Chapter has
46 members from Victoria, Tasmania, South Australia and Western Australia,
including nine police officers (IAFCI, 20 April 2006, personal communication).

Table 2.5: Membership of the Australian Institute of Professional
Investigators, 2005

<table>
<thead>
<tr>
<th>Australian State or Territory</th>
<th>AIPI Members</th>
</tr>
</thead>
<tbody>
<tr>
<td>Victoria</td>
<td>83</td>
</tr>
<tr>
<td>New South Wales</td>
<td>51</td>
</tr>
<tr>
<td>Queensland</td>
<td>24</td>
</tr>
<tr>
<td>Western Australia</td>
<td>18</td>
</tr>
<tr>
<td>South Australia</td>
<td>17</td>
</tr>
<tr>
<td>Overseas</td>
<td>4</td>
</tr>
<tr>
<td>Australian Capital Territory</td>
<td>3</td>
</tr>
<tr>
<td>Tasmania</td>
<td>2</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>202</strong></td>
</tr>
</tbody>
</table>

Source: AIPI Victorian Secretary, 24 Feb 2005, personal communication.

Of these members approximately 38 are involved in e-crime investigation
roles. AISP represents 70 members, of which 49 are inquiry agents and only
one or two might conduct e-crime investigations (AISP, 2006; AISP, 9 March,
2006, personal communication).19 AIPI represents just over two hundred

---

19 VSI did not respond to requests for information on their investigator membership.
members nationally, eighty-three of who are located in Victoria (see Table 2.5).

In addition to numerous self-help texts written to protect Internet users (Petraitis and O’Connor, 1999; Bidwell, 2002; Queensland Police Service, 2005) a growing literature on forensic computer analysis has been written to educate investigators in the technical and procedural skills required increasingly to investigate e-crime (Icove, Seger and VonStorch, 1995; Stephenson, 2000; National Institute of Justice (US), 2001; Casey, 2002; Kruse and Heiser, 2002; Stucki, 2002; Vacca, 2002; Australian Centre for Policing Research, Feb 2003; Mandia, Prosise and Pepe, 2003; Casey, 2004; Ferraro and Casey, 2004). These texts focus variously on planning incident response; forming investigation teams; warrant preparation; crime scene and other forensic procedures and prosecution. Some titles, like the *Hacking Exposed* series, explain the methodologies employed by offenders to breach systems from the philosophy that it takes a thief to catch a thief (McClure, Scambray and Kurtz, 2003).

Since 2002, the *International Journal of Digital Evidence*, a dedicated professional journal, has published research on theoretical, practical, legal and policy issues. More recent offerings include *Digital Investigation: The International Journal of Digital Forensics & Incident Response* and the *Journal of Digital Forensic Practice*. Procedures for digital forensic analysis have increasingly become subject to national and international standards, such as *HB171-2003 Guidelines for the management of IT Evidence* (Standards Australia, 2003; see also National Institute of Justice (US), 2001; ACPO, 2002).
Partnership in e-crime policing strategy

“Partnership” has become a buzzword in relation to e-crime. Criminals are speaking the language of partnership, albeit often in broken-English: “I seek your partnership to accommodate the sum US$42M (Forty Two Million United State Dollars Only) for us” (scam email) and “Australian Finance Group invites you to cooperation” (scam email). Criminals, as in the past, draw together expertise to perpetrate their offences (Gaudin, 7 March 2005). One offender might supply stolen credit card numbers, another might harvest countless email addresses or lend access to a botnet to attack a network. Others will design the malware that exploits security vulnerabilities or point a fellow hacker to a convenient source of phishing email text (McDermott, 15 August, 2005).

In response to these and the numerous investigative challenges detailed above, public and private police have called for greater cross-sector cooperation to attend to e-crime (Cochrane, 2003). The US National Institute of Justice identified “cooperation with the hi-tech industry” as one of their Critical Ten needs to address e-crime:

Private industry can assist by reporting incidents of electronic crime committed against their systems, helping to sponsor training, joining task forces, and sharing equipment for examining electronic evidence. Crime solvers need industry’s full support and cooperation to control electronic crime (Stambaugh et al, 2001: x).

Police require cooperation because the private sector owns much of the critical infrastructure that is targeted by e-crime (Stambaugh et al, 2001: 22). The Crime Reduction Strategy of the National High-Tech Crime Unit (NHTCU) in the UK notes the importance of information sharing:
... probably the single most important factor in the entire Crime Reduction Programme and the aspect of industry outreach, which will determine its success will be the ability to encourage businesses and public sector departments in the UK to share information on hi-tech criminality with the NHTCU (NHTCU, 2004: 5).

The Council of Europe Convention on Cybercrime is also premised on recognition of the need for cooperation between States and private industry.

In Australia’s *Electronic Crime Strategy* partnership is one of the five focus areas that police need to address, including partnership with “private agencies” (ACPR, 2001: 11). The objective is to “maximise the effectiveness of electronic crime investigations and protection of critical infrastructure. A key outcome is to prevent the duplication of effort and maintain a cohesive spirit and integrated approach”. The strategy is guided by a principle of:

- private sector leadership and self regulation wherever possible, and practical regulation where necessary, complemented by effective and mutually beneficial partnerships with police (ACPR, 2001: 5).

Victoria Police in its *The Way Ahead* strategy for 2003-2008 recognises an “increasing array of providers of policing services”, proposing to:

- involve more people such as volunteers, in crime prevention and community safety activities;
- provide training and education in policing techniques and professional standards to other organisations and agencies providing policing services; and
- develop partnerships with private providers of policing services which includes the security and gaming industries (Victoria Police, 2003a: 17).
Likewise, the Victorian private investigation industry welcomes cooperative relations, as evidenced by the Australian Institute of Professional Investigators objectives to: “Develop, implement and facilitate compliance with the partnership arrangements with law enforcement and regulatory agencies” (Australian Institute of Professional Investigators, 2003). Partnership would present commercial opportunities for many investigators and additional, perhaps more effective, policing avenues for their clients.

Concerns arising from joint public-private investigation

However, as noted in Chapter One, concerns about police “partnership” with the private sector are not without precedent and form an important context for this thesis. For example, in 1989, a self-styled security expert Paul Dummett (aka Stuart Gill) misled Victoria Police claiming to have knowledge that Australian hackers had hacked Citibank, swapped credit card numbers and sold drugs on bulletin boards (“Hackwatch spokesman charged”, 2 October 1989; see also Dreyfus, 1997: Ch2 & 3). Dummett’s relationship with police was later characterised as inappropriate by the Ombudsman (Deputy Ombudsman (Police Complaints) Victoria, 1993). An ICAC report into improper information sharing by police noted that informal networks extend beyond police and their former colleagues to include ‘membership’ from banks, finance companies, retailer and estate agents (Roden, 1992: 154). Hoogenboom (1991) termed this “grey policing”. In 1995, Victoria Police was under the spotlight for the Window Shutters scandal, because members bypassed internal systems and made unauthorised referrals to shutter service operators when they attended at unsecured premises, such as following break-ins. In some instances this involved taking kickbacks from the shutter companies. Ironically, in the context of this thesis, the scandal was known in the media as “Windows 95” (The Ombudsman Victoria, 1998; Munro, 13 May
2003). Operation Bart, an investigation by the Ombudsman of Victoria, resulted in the disciplining of 550 members of Victoria Police, criminal charges against two members, and the creation of the Victoria Police Ethical Standards Department.

There has been ongoing controversy about unauthorised access to the information stored in the Victoria Police Law Enforcement Assistance Program (LEAP),\(^\text{20}\) which will impact on any attempts to formalise public-private investigative partnerships. Public concerns were raised during the 2002 state elections when comments by the then police minister, Andre Haermeyer, revealed knowledge of a Liberal candidate’s police file (The Age, 7 December 2004). On 10 October 2003, Victoria Police admitted in a media release that five members were disciplined after inappropriate access to the record of Kay Nesbit, who was a victim of violent crime and is now a victims’ rights campaigner (Victoria Police, 10 Oct 2003). The problems continued when up to 35 members accessed the criminal history of Zdravko Micevic inappropriately, the security guard later acquitted of the manslaughter of cricketer David Hookes (The Age, 13 February 2004). Later still, in July 2005, 20,000 Victoria Police files relating to over a thousand Victorians were mistakenly sent out to a corrections officer (Tomazin, 24 August 2005). These problems are exacerbated, because Victoria Police has 56 non-integrated intelligence databases on criminals, which had resulted in a lack of information sharing and fostered corruption (Silvester, 8 February 2005).

In another recent example, Kerry Milte, a former federal police officer, barrister, lecturer and consultant, claimed to have been working with Victoria

\(^\text{20}\) The LEAP database has been in use across Victoria Police since 1 March 1993 (Victoria Police, 2005c). It is the official database in which Victoria Police record information pertaining to incidents and from which official crime statistics are generated.
Police as a consultant on serious organised crime. In October 2005, Milte pleaded guilty to receiving and disclosing information improperly from the LEAP database via a federal agent (ABC Local Radio, 7 Oct 2005). The court was told that Milte received travel records and whereabouts of three people that he disclosed to a law firm. The Chief Commissioner of Police has now reportedly distanced herself from Milte and denies he was ever a consultant to Victoria Police (ABC Local Radio, 7 Oct 2005). George Brouwer, the Director of the Office of Police Integrity in Victoria recommended that Victoria Police officers who leak information without authority should receive up to 10 years imprisonment (Office of Police Integrity Victoria, 2005).

As noted in Chapter One, there are concerns about under-reporting of e-crime. Previous research has offered several reasons that companies do not report computer crime offences including negative publicity, loss of advantage to competitors, ignorance of the law and belief that internal action by the company is best policy (Power, 1999). Chan H.K.H. (2000) analysed the factors that lead to (non) reporting of hacking. He proposed that the process leading up to the reporting or non-reporting of hacking had four distinct phases. He termed this the DIER model consisting of discovery, investigation, escalation and revelation phases. He proposed five driving forces that propel an incident from one phase to another. These are technology (computer security), education (knowledge and skills), corporate policy (rules, regulations and procedures, resources and priority), ethical value (attitude, perception and assessment) and external factors (external agents). The problem evolves from a technical issue to a managerial issue (Chan, 2000: 298).

Chan (2000: 323) concluded that reported cases are associated closely with multiple stakeholders and IT users, whereas unreported cases are associated with single stakeholders and IT professionals (see Table 2.6). The modus
operandi of an incident, classified by Chan as either internal or external and the skill of the offender, either less skilled and opportunist or highly skilled, were not strong predictors of (non) reporting. However, additional factors might determine reporting behaviour, such as complexity of the incident, perceived seriousness and impact of incident, ownership of problems, perceptions of legislative or regulatory regimes and available sanctions, perceptions about outcomes of reporting, media reporting, previous experience with law enforcement, previous victimization, knowledge of reporting mechanisms or insurance.

Chan (2000: 299) described the situation following reporting as “a handover of power and control (transfer of ownership) of the ‘individual/corporate owned case’ to an external agency, the police”. Is this an entirely accurate picture where private investigators are involved in the ongoing investigation and prosecution with police under “partnership policing”? Incidentally, Chan (2000: 333) also called for “partnerships between governments and private companies who may be rivals and competitors” due to the interconnectedness and interdependency of company computer systems via the Internet.

Table 2.6: Factors that do and do not predict (non) reporting of hacking

<table>
<thead>
<tr>
<th>Predictive factors</th>
<th>More likely to report</th>
<th>Less likely to report</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stakeholders</td>
<td>Multiple stakeholders</td>
<td>Single stakeholder</td>
</tr>
<tr>
<td>IT knowledge</td>
<td>IT users</td>
<td>IT professionals</td>
</tr>
<tr>
<td>Motivation</td>
<td>Liability changed</td>
<td>Liability unchanged</td>
</tr>
<tr>
<td>Victim</td>
<td>Individual victim</td>
<td>Corporate victim</td>
</tr>
<tr>
<td>Modus operandi</td>
<td>Internal attack</td>
<td>External attack</td>
</tr>
<tr>
<td>Perpetrator skill</td>
<td>Opportunist</td>
<td>Skilled offender</td>
</tr>
</tbody>
</table>

Non-predictive factors | No clear directional influence on reporting

Source: Adapted from Chan (2000: 170; 322-324).

Other concerns about private investigation that might impact public policing efforts if combined, include misinterpretation of digital evidence (Casey, 2002b), incorrect information entered in police databases (Ladd, 1989: 224),
planting digital evidence, coerced confessions and plea bargaining, improper evidence collection techniques such as pretext calling, compromised investigations due to financial and fiduciary relationships (Gill and Hart, 1997b: 559; 560; 564), assaults, abuse of search and seizure and protection racquets. Marx (1987: 182) questioned whether former police find it easier to compromise police investigations and cover up illegal tactics, because they know how police operate. “Hacking back” an attacker as self-defence counterhacking has also found support (Jayawal, Yurcik and Doss, 2002). Nor has the IT security industry been shy about employing hackers, even convicted ones, as consultants. In 2002, 43% of Australian organisations were willing to hire ex-hackers knowingly, three times more than in the USA (AusCERT et al, 2002: 1). Conscripting private organisations to public policing could unintentionally compromise privacy and facilitate other forms of crime. For example identity theft was facilitated when the US government required airlines to collect and provide passenger information for the purpose of terrorism security screening, with no recompense for their assistance except avoidance of penalties. The companies minimised costs and did not

---

21 For example, email and some logs may be falsified easily (Casey, 2002b). Planted evidence would often require faking a history of computer usage and not simply placement of illicit material, because of how data is overwritten. Forensic computing offers means of detecting fabricated digital evidence, including dynamic time and date stamp analysis (Weil, 2002) and event time bounding (Gladyshev and Patel, 2005).

22 Although an analogy of self-defence and defence of property might be made, MCCOC (2000: 92-93; 2001: 109) decided not to institute a specific defence of counterattack against hacking in the Model Criminal Code, such that doing so under Australian law constitutes an offence.

23 For example Kevin Mitnick; Kevin Poulsen; Kim Schmitz; Mark Abene aka Phiber Optik hired by Ernst & Young in the 1990s (Wikipedia contributors, 2006); and Sven Jaschan, author of the Sasser virus (Best, 2004). Matthew Bevan aka Kuji avoided conviction but was also employed as an IT security consultant (Wall, 1998: 204).
adequately protect that information, which criminals could obtain easily from boarding pass stubs (Boggan, 3 May 2006).

Implementing public-private partnership for policing e-crime has met difficulties. A case in point relates to Internet Service Provider cooperation with Australian law enforcement.24 Police and the Internet Industry Association (IIA) attempted to negotiate a code of practice for the Internet industry to regulate and harmonise assistance:

The IIA is concerned that we reach a balance between the legitimate needs of law enforcement agencies to investigate and prosecute criminal offences perpetrated over the internet, versus the privacy of end users and the cost to industry (IIA, 2003).

However, failing to reach agreement on key provisions the code remains unratified after two years.25 Instead, from 1 March 2005 Internet Service Providers and Internet Content Hosts (ICHs) became required under the new section 474.25 the Criminal Code 1995 (Cth) to report to the Australian Federal Police any child pornography hosted on their services of which they are made aware or face fines of up to AUS$55,000 for companies and AUS$11,000 for individuals.26 This overturned their previous ‘innocent disseminator defence’ afforded to them by the precedent of Thompson v Australia Capital Television

24 Although “reasonably necessary” help is obligated under section 313(3) of the Telecommunications Act 1997 (Cth) this is not defined. See also the Telecommunications (Interception) Act 1979 (Cth).

25 In 2005, the draft code was updated to reflect amendments to the Interception Act by the Telecommunications (Interception) Amendment (Stored Communications) Act 2004 clarifying that stored communications, such as email, voicemail and SMS do not require a Telecommunications Interception Warrant.

The Federal Minister for Justice and Customs, Senator Chris Ellison, made it clear that “ISPs and ICHs should be aware that come March 1, they will be obligated to join the federal government’s frontline fight against abusers of children online” (ZDNet Australia, 23 February 2005). “Conscription” of cooperation through legislation remains the fallback position of governments (Grabosky, 1995), which Haines (1995: 269) considers necessary if interest groups cannot reach virtuous outcomes.

Chapter conclusions

The investigation of e-crime is a specialist pursuit in both law enforcement and the private sector, which has developed reactively to advances in electronic crime. Police argue that partnership has become exigent due to the commercial landscape and complexity of ICT technologies like the Internet, resource shortages and lack of exposure due to under-reporting. The private sector argues for partnership to protect or grow their commercial interests. LeBeuf (2001) argues that police do not need to become experts in particular IT systems as much as learn the processes of how to conduct e-crime investigations. “There is a large pool of experts in the field of technology; police officers simply have to learn to work with them.” However, high profile instances of improprieties and failures such as the draft Cybercrime Code of Practice and the ability and willingness of government to legislate “cooperation” suggest at least initially that policing of e-crime need not and perhaps should not rely on true partnership. Yet, partnership remains a high agenda item. Consequently, so does the question of how police should interact with private investigators? And how can this be achieved so as to protect public interests?

27 An Australian commercial television station defended charges of defamation successfully after it screened an interview with a child who alleged abuse at the hands of her father.
The next chapter examines the broader development of partnership policing as a law enforcement strategy; standards of policing and examines previous attempts to prescribe appropriate police interaction with the private security industry as they might guide this investigation of e-crime policing partnerships.
Chapter 3: Partnership policing in perspective

Chapter Two demonstrated that arguments for partnership policing of e-crime though widespread are not uncontroversial. Formal partnership between public and private police is far from common practice, difficult to implement and has been and continues to be vulnerable to a variety of improprieties. For this reason, it is important to understand the partnership policing strategy in the broader context of other developments in policing, how it might be used and to examine its implications. Thus the chapter first discusses partnership policing through an examination of its development as a policing strategy. Some practical considerations of forming successful partnerships taken from the business management and crime prevention literature are then tendered.

To judge the merits of the current push for greater inter-sectoral cooperation in e-crime investigation requires an understanding of the general legal, ethical and performance standards and accountability mechanisms to which public and private police are held officially, and consequent questioning of whether these are sufficient for investigative partnerships. Accordingly, the chapter next outlines those standards and mechanisms for consideration. Following this, previous attempts to prescribe appropriate relationships between public and private police are also examined, including Sarre and Prenzler’s (2000) Regulated Intersections model.

Distinguishing partnership policing

Partnership policing as a strategy of crime control grew out of community policing in the 1980s. In the 1960s and 1970s the predominant discourse of policing was community policing as a Keynesian welfare model (O’Malley
and Palmer, 1996). In Australia, this was characterised by initiatives focused on assisting non-criminals and counselling offenders that drew criticism for shaping police as welfare officers (O’Malley and Palmer, 1996: 138-9). Many of those initiatives appeared removed from problems of crime and community safety (O’Malley and Palmer, 1996: 139). The discourse changed in the 1980s, reflecting a neo-liberal retreat of state governments from this welfare model to one of recognising the community as competent (when trained) to form partnerships with police due to their knowledge of local conditions (O’Malley and Palmer, 1996: 145). Victoria’s Chief Commissioner of Police encapsulated the new relationship between police “professionals” and a “responsible” community with the words: “Together we are a partnership – police and the people of Victoria – partners against crime” (Vicsafe, nd, cited in O’Malley and Palmer, 1996: 144).28 The philosophy is underpinned by recognition that police cannot function independently to address crime (Greenberg, 2000: 318):

The police alone cannot win the fight against crime and disorder. It requires a coordinated response from the community as a whole. Local authorities, the private sector and others all have to work in partnership with the police to develop and implement local crime and disorder reduction strategies (Home Office, 2001: 84).

As seen in Chapter Two, arguments for partnership policing of e-crime focus jointly on this shared responsibility and inability to go it alone. In O’Malley and Palmer’s “post-Keynesian” state the focus is upon “steering” not “rowing” (Osborne and Gaebler, 1993 cited in Davids and Hancock, 1998; see also Abbey and Button, 1997). Hunt (1995: 54) provided an early description of partnership policing focusing on this leadership role—adopted by others as

28 This was certainly meant figuratively and not to mean the literal formation of a partnership, as a legal relationship, as defined by the Partnership Act 1958 Vic.
a definition (O’Malley and Palmer, 1996: 145; Oppler, 1997: ¶10)—as when police take:

a proactive and leadership role in bringing disparate community groups such as the public, elected officials, government and other agencies together to focus on crime and community disorder problems.

However, this definition does not sufficiently distinguish partnership policing from earlier forms of community policing.29 Nor does it capture recent developments that position partnership policing as potentially distinct to even post-Keynesian community policing. Partnership policing as it is emerging now reflects a desire by some police to withdraw from the community policing philosophy of necessarily taking all community concerns seriously, because police have found that community concerns sometimes represent “phantom menaces” (D’Ambra, 2002; see also Nixon (2002) in Chapter 1). For instance, partnerships might be based on the complaint du jour rather than serious problems; or involve partners “forced” to be there (due to corporate governance requirements or even “cause-related marketing”) who distract from police priorities rather than engender “truly benevolent partnering” (D’Ambra, 2002: 24).30 James Q. Wilson (1968) suggested thirty years previously that as most calls for police assistance involved non-criminal

29 Arguably, from the context of his statement, Hunt was not attempting to distinguish partnership policing from community policing, but used the term interchangeably. See Moore and Trojanowicz (1988) for a discussion of distinguishing corporate policing strategies.

30 An alternate response, termed ‘reassurance policing’, is premised on addressing ‘signal crimes’ that have a disproportionate affect on an individual’s perception of crime and community safety so as to address the gap between falling crime rates and fear of crime and increase public confidence in police (Leicestershire Constabulary (UK), 2004; see Innes et al, 2004).
matters governments would profit by turning such responsibility over to private concerns. Likewise, Davids and Hancock (1998: 54) observed wittily that the rhetoric of “the customer is always right” is nonsensical to police for whom offenders are a key “customer” base.

Noting Gordon’s infamous critique of community policing as “an attempt at surveillance and control of communities by the police, under the guise of police offering assistance” (Gordon, 1987: 141), one might argue that partnership policing is simply a less covert attempt by police to control communities and the anti-crime agenda. Under partnership policing, police forces decide with whom they will partner, under what conditions and for what priorities.

Flexibility of response is a stated cornerstone of partnership policing and as such there has been no single model for its implementation at the operational, local level (Oppler, 1997: ¶1). Partnership policing is often considered policing through networks, which is characterised generally by diplomacy, trust and reciprocity:

Trust is the central coordinating mechanism of networks in the same way commands and price competition are the key mechanisms for bureaucracies and markets respectively. Shared values and norms and an appreciation of divergent organisational cultures are the glue which holds the complex set of relationships together; trust is essential for cooperative behaviour, and, therefore, the existence of the network (Flemming and Rhodes, 2002: 195).

The policing partnerships in the UK and Holland examined by Oppler (1997) employed variously mixtures of crime prevention with reactive policing (joint patrols, arrests), proactive policing (intelligence operations, crime analysis),
problem-oriented policing\textsuperscript{31} (venue license revocations) and what might be termed post-Keynesian community policing (charter agreements, discussion forums, crime prevention training and leaflets) to reduce crime levels at the various problem sites.\textsuperscript{32} There was an emphasis on consultative processes, including needs assessment and planned policing responses involving both police and civilians (Oppler, 1997: ¶10).

However, arguably, police may still option either bureaucratic “command and control”, contracts or network relationships with their citizenry as it best suits their needs (Flemming and Rhodes, 2005), all the while calling this “partnership”. Flemming and Rhodes (2005: 200-203) argue that the application of any one or a mix of these policing models will depend upon choices about underlying, conflicting motivations: cooperation versus competition for resources, accountability versus efficiency, openness about capacity versus avoiding criticism or “tipping off” criminals as to incapacities and governability versus flexibility.

Partnership policing can take advantage of developments in business. Unlike the business sector in general, law enforcement agencies have always been restricted as to the form of strategic alliances they can enter. They cannot acquire or merge their private sector competitors, such as security or investigations firms, nor own shares in those companies as other businesses might. As flexible rafts of partnered organisations become the norm in business over mergers and acquisitions (Deering and Murphy, 2003), competing organisations become less problematic for police. Cooperation with business rivals has ceased to be the opposite of competition: “it is no longer a controversial idea that the main competitive agent in the future will


\textsuperscript{32} Hunt (1995: 56-58) for details the techniques employed by these styles of policing.
not be integration but networks of autonomous companies with complementary skills and resources pursuing shared objectives” (Deering and Murphy, 2003: ix). Bradenburger and Nalebuff (1996) describe this subtle change as “co-opetition”, where companies must cooperate and compete with each other simultaneously (cited in Geis and Geis, 2001: 18-9). The duality described by Bradenburger and Nalebuff (1996) is that the process of creating value is inherently cooperative, whereas capturing value is inherently competitive. “Co-opetition means cooperation to create a bigger business ‘pie’, while competing to divide it up” and policing partnerships benefit from co-opetition where this permits innovative alliances.

However, diplomacy might take shape as “third party policing”, especially if reciprocity is too costly (Beurger and Mazerolle, 1998: 301). This command and control strategy involves police persuading or coercing external agencies and groups to take responsibility for crime prevention or control (Mazerolle and Ransley, 2004). Coercion might involve threat of civil action or other regulation.

Given economic rationalism and managerialism, partnership policing might also mirror the contractualism of “public-private partnerships” (PPPs), which is the trend for partnered construction and maintenance of infrastructure projects, such as roads and bridges, characterised by private financing and competitive tendering for contracts. Webb and Pulle (2002: 2) define these public-private partnerships as:

partnerships between the public sector and the private sector for the purposes of designing, planning, financing, constructing and/or operating projects, which would be regarded traditionally as falling within the remit of the public sector.
Construction of the new Victorian County Court, new remand and correctional programs centres and the Mobile Data Network (a wireless communications network for police and ambulance) are examples of criminal justice PPPs in Victoria. In each, there is a single or a small consortium of private sector partners. PPPs generally involve only a single or small syndicate of private sector companies vying for the partnership contract. The possible use of one-to-one or small cluster relationships for delivery of policing infrastructure or services would be more typical of partnership in business (see generally, Lendrum, 2003: 28) than previous policing efforts aimed at whole communities.

However, contractualism in public policing might create false markets through imposed purchaser-provider splits, which in turn may hamper flexible response as police and governments become locked in (Davids and Hancock, 1998: 61). Crawford (2005) argues that contractual governance evades due process, marginalises legality and offers significant discretion to bureaucrats. Inherent in a contractual model of governance is the idea of the power of one party to restrain the other. Oppler (1997: ¶16) contends that in partnership policing “there should be an equitable distribution of power. A powerful agency should not impose its views, priorities and objectives upon others with less power”. One must then ask to what extent contractual governance is an imposition of values and to what extent is it indeed a voluntary negotiation of them (Crawford, 2005)? In terms of accountability, contracts are often individual and private and thus sheltered from open legal review. There is also the distinct possibility of “defining deviancy up” in contracts—to discourage, deter, forbid or outlaw behaviours that used to be overlooked or tolerated (Karmen, 1994)—without occasioning appropriate public debate. For example, regulating potential “partners” who might be expected, because of their societal position, to work closely with police but
who elected not to assist them for whatever reasons. Arguments for mandatory reporting of fraud (DCPC, 2004), as heard recently in Victoria, fall into this category of defining deviancy up, albeit via legislation.

MacNeil (1968) proposed seven ideal qualities of relational contracts, which offer useful signposts for evaluation of partnership policing efforts that take contractual formats:

1) distribution of responsibility and obligations in a concrete manner;
2) a degree of reciprocity and mutuality;
3) treating the parties as self-maximising rational choice actors;
4) a sense of choice in the decision to enter the contract (although the choice may not be real);
5) a conscious awareness of the future and a desire to control uncertainty by regulating excesses;
6) provocation of active instead of passive responses;
7) facilitation of a form of accountability through performance monitoring.

Crawford (2005) argues that we must aim to build procedural fairness into contractual models of governance.

The reform agenda of Victoria Police in the 1990s, mirroring trends seen internationally, included adoption of user pays, outsourcing of ‘non-core’ services, corporate sponsorship and introduction of performance targets and “professionalisation” of police (Davids and Hancock, 1998). Outsourcing ‘non-core’ services raises questions about what police functions constitute core tasks of the state and what services can be provided legitimately by the

---

33 See Davids and Hancock (1998) for a detailed discussion of the political influences on policing in Victoria.
private sector. However, contracting out has not supplanted bureaucratic models of organisation within policing that are still required to manage contracted services (Flemming and Rhodes, 2005: 194). The language of partnership as “working together” might assist divestment of policing function to the community without negative perceptions that they are abandoning their core functions.

Victoria Police’s *The Way Ahead Strategic Plan 2003–2008* distinguishes four key value areas: ‘intelligent policing’, ‘confident policing’, ‘community policing’ and lastly ‘partnership policing’. This dissection of policing strategies permits distillation of previous concepts of “partnership” policing, when the term was often used interchangeably with community policing, such that it opens up flexibility in the concept:

> Partnership policing: collaborates and works with other agencies and groups in the pursuit of common community safety outcomes through developing and strengthening community partnerships across the State (Victoria Police, 2003a: 7).

Distilling the building of police capability into intelligent policing, means partnership policing might not focus on building capacity in partners, who might be expected to source their own. Where community policing focuses “on local level service needs and delivery to achieve maximum impact on local priorities and safety outcomes” (Victoria Police, 2003a: 7) partnership policing might focus on police priorities. Locating the police leadership role in the concept of “confident policing” suggests that partnership policing might not require police leadership.34 The strategic plan refers also to “influencing

---

34 Recall “private sector leadership” in Australia’s e-crime strategy (ACPR, 2001: 5).
others’ behaviour” as partnership policing, which suggests incorporating “third party policing” (Victoria Police, July 2002: 10).

In addition to recognising new “providers of policing” (see pg. 48), under the partnership policing strategy Victoria Police proposes to:

- develop joint initiatives to target crime and fear of crime in the community;
- actively work towards whole-of-government initiatives by creating or supporting information and resource sharing mechanisms, referral networks and other crime prevention and safety strategies;
- form partnerships with research and training institutions to identify, adapt and develop best practice (Victoria Police, 2003a: 17).

The Victoria Police Manual (2005a), in the section devoted to donations and sponsorship, defines “partnership” as:

a well defined relationship between Victoria Police and an external organisation or individual which has as its purpose, cooperation between the parties in relation to the completion of a specific project, the achievement of a specific outcome and/or the delivery of a specific service (VPM Instruction 205-5: s3).

The next section examines some of the practical issues of partnerships. That is followed by an examination of the general legal, ethical and performance standards that apply to public and private police.
Policing partnerships as projects

Both the business management literature on partnerships and strategic alliances (Wilcox, 2000; Deering and Murphy, 2003; Lendrum, 2003; Gage, 2004; Reuer, 2004; EDuce Ltd and GFA Consulting, nd; Huxham and Vangen, 2005) and police-authored literature on crime prevention partnerships (Calhoun, 1998; Goode, 1998; Greenberg, 2000) more often than not focus upon practicalities of achieving successful outcomes over ethical considerations.

Huxham and Vangen’s (2005: 37) number one tip for collaborating is “don’t do it unless you have to”:

> Joint working with organizations is inherently difficult and resource consuming. Unless you can see THE POTENTIAL for real collaborative advantage (i.e. that you can achieve something really worthwhile that you couldn’t achieve otherwise) it’s most efficient to do it on your own (emphasis in original).

Greenberg (2000: 319-20) argues that policing partnerships only work when the mutual benefits for the parties involved are “well defined, understood and attainable”. He argues that many policing partnerships are ineffective, and even counter-productive to an alleviation of crime and fear of crime, citing that many partnerships have been entered into for short-term public relations benefits, to meet grant funding requirements or simply because they “seemed right”. Further, he argues that for many police officers “partnership” means occasional attendance at public forums and nothing more substantial, and that such attendance only serves to raise public expectations about police performance. Wilcox (2000) also warns that the term partnership “may be too widely applied to situations where one powerful organisation is doing no
more than consult with others, or mask fundamental differences of approach and objectives that will later lead to conflict”. Although in some contexts less participation is appropriate, this should not be termed partnership.

In the business literature, it is often noted that not all of an organisation’s relationships will or should move to partnering or alliance relationships (Lendrum, 2003: 30). Partnerships progress typically through five standard phases where they form, frustrate, function and of course may either fly or fail (EDuce Ltd and GFA Consulting, nd). Some partnerships will go from the second stage of frustration directly to failure for want of a sufficient common goal, change in people or failure to work at cooperation (see Figure 3.1).

Figure 3.1: The partnership life cycle

![Diagram of partnership life cycle]

Source: EDuce Ltd and GFA Consulting, nd.

Partnerships can be described according to combinations of the ambitions for partnering and partners’ views of and reactions to difference (Deering and Murphy (2003: 18-19; see Table 3.1). Expectations, perceptions and assumptions about these are as important as facts to the success or failure of
partnership efforts and should be considered carefully in partnering dialogues (Deering and Murphy, 2003: 133).

Wilcox (2000) summarised characteristics of successful and failed partnerships (see Table 3.2). A lack of success characteristics would also

<table>
<thead>
<tr>
<th>View of difference</th>
<th>Avoid difference</th>
<th>Tolerate difference</th>
<th>Value difference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command and control</td>
<td>• Strategies to minimise visible differences (formal operations, processes, behaviours) • Negotiated contractual agreements and procedures • Pre-planning to last detail</td>
<td>• Distant relationships with some suspicion • Uniformity by external controls &amp; structures • Acceptance of different objectives and behaviours, but low trust • Clear communication and strict checks on understanding</td>
<td>• Outside forces (regulation, market) constrain partners to reduce negative • Face saving causes lack of momentum • Power struggles cause risk aversion</td>
</tr>
<tr>
<td>Hearts and minds</td>
<td>• Strive for same basic culture (thoughts and feelings) • Shared visions and commitment to common aims • Difference is invisible • Harmony will produce creative outcomes</td>
<td>• Strong process orientation • Changing, complex objectives and constant review • Focus on learning and continuous improvement</td>
<td>• Differences explored for maximum benefit • Work in radically new ways • Build shared picture, not shared vision • Multiple stakeholders • Challenge through dialogue</td>
</tr>
<tr>
<td>Reason for partnering</td>
<td>Promote positive</td>
<td>Radically new</td>
<td></td>
</tr>
</tbody>
</table>

Table 3.1: Partnering grid

Source: Deering and Murphy (2003: 141).
Table 3.2: Characteristics of successful and failed partnerships

<table>
<thead>
<tr>
<th>Success characteristics</th>
<th>Failure characteristics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agreement that partnership is necessary</td>
<td>History of conflict between key partners</td>
</tr>
<tr>
<td>Respect and trust between partners</td>
<td>One partner manipulates or dominates</td>
</tr>
<tr>
<td>Leadership by respected individual(s)</td>
<td>Lack of clear purpose</td>
</tr>
<tr>
<td>Commitment developed through a clear and</td>
<td>Unrealistic goals</td>
</tr>
<tr>
<td>open process</td>
<td></td>
</tr>
<tr>
<td>Development of shared vision of goals</td>
<td>Key stakeholders missing from partnership</td>
</tr>
<tr>
<td>Time to build partnership</td>
<td>Financial and time commitments</td>
</tr>
<tr>
<td></td>
<td>outweigh the potential benefits</td>
</tr>
<tr>
<td>Shared mandates or agendas</td>
<td>Unequal and unacceptable balance of power and control</td>
</tr>
<tr>
<td>Development of compatible and flexible</td>
<td>Differences of philosophy and ways of working</td>
</tr>
<tr>
<td>ways of working</td>
<td></td>
</tr>
<tr>
<td>Good communication, even if aided by</td>
<td>Lack of communication</td>
</tr>
<tr>
<td>facilitator</td>
<td></td>
</tr>
<tr>
<td>Collaborative decision making</td>
<td>Hidden agendas</td>
</tr>
<tr>
<td>Effective organisational management</td>
<td></td>
</tr>
</tbody>
</table>


indicate problems within a partnership. Problematic power-relations are central to dysfunctional policing partnerships (Oppler, 1997). Deering and Murphy (2003: 132) make a strong case that marginalisation and the attendant lack of communication, more than conflict, is what prevents partnerships from succeeding. Conflict brings to the fore issues that need resolution and so should be dealt with rather than smoothed over (Deering and Murphy, 2003: 132). Lack of information sharing is a common complaint within police that might impact investigative partnerships. Writing about information sharing between Canadian police, LeBeuf (2001: ¶29) identified four main factors that impede information sharing between police: lack of trust, legalities, investigation philosophies and methods that entrain secrecy and work conditions that limit physically the recording of information. Agreements between policing agencies (MOUs) were listed as also impeding information sharing (LeBeuf, 2001: s3.3.1). He argued that these impediments to
information sharing aim “to protect the information, the investigators, the information sources, and the investigation itself”.

Experience from crime prevention partnerships warns that partnerships should be organised by issue, not sector (Calhoun, 1998: 8). Goode (1998: 7) also argues “partnerships should spend as much time developing the capacity of their partner, and co-ordinating strategy as they do in industry”.

Greenberg (2000: 320) offers key questions to ask before forging policing partnerships:

- What is the purpose of the partnership and what are the projected outcomes?
- Who are the key players in the partnership?
- What is the experience of the key players in working with partners?
- What do the partners stand to gain or lose by participating?
- Are both partners worthy of participating in the partnership?
- Are the right players involved in the partnership?
- Are officers comfortable with their position and authority to make the decisions necessary and support the outcomes of the partnership?
- Are the outcomes of the partnership well stated?
- How will the success of the partnership be measured?
- Are employees trained and well versed in the nature of partnerships?
- How much time will be allowed before assessment occurs and a determination is made to continue or disband the partnership?

Tools such as these emphasise constructing policing partnerships as “quality” projects. Underlying questions of “success” are considerations of ethics and legality and performance standards to which we now turn.
Standards of public and private policing

Broadly speaking public police are held officially to legal, ethical and performance standards. Legal standards may be considered the low bar of “minimally accepted behaviour” or duty and ethical standards as the high bar of aspiration to ideal virtues (Cohen and Feldberg, 1991: 42-3). Acceptance of the role of the public police officer dictates a modification of general rights and duties, often imposing higher standards than expected of other citizens (Miller, Blackler and Alexandra, 1997: 9-10; Davies, 2000; Delattre, 2002).

The basis for police authority and the powers afforded them is often premised on social contract theory (Kleinig, 1996a). From the idea of the social contract, Cohen and Feldberg (1991: 39) identified five core ethical standards of public policing. Police must:

1) Provide fair access to their services;
2) Insure that their power is held and used as a public trust, and will not be abused;
3) Put the primacy of safety and security of citizens before the unreflective enforcement of law;
4) Acknowledge the coordination of governance with other officials in the system (teamwork); and
5) Maintain an attitude of non-partisan objectivity in carrying out their functions.

Behaviour that achieves these standards should be applauded as good and that which falls short should be criticised or condemned (Cohen and Feldberg, 1991: 39).\(^{35}\) Cohen and Feldberg (1991: 57) base the moral imperative

---

\(^{35}\) This thesis takes the view that moral standards are objective and cooperation is a virtue as Cohen and Feldberg propose; contra Benedict (1989) who cites a tribe in Melanesia that views
of teamwork on its requirement to achieve successful policing: “because the success of the police function depends on teamwork, police behaviour that tends to undermine other officers or other actors in the system cannot measure up to moral standards”. Thus “teamwork” is not an end in itself, but a means to fighting crime effectively and efficiently, which must be balanced against the other ethical requirements, such as institutional independence of police organisations. Cohen and Feldberg (1991: 56) identify the tests of teamwork as coordination, communication and cooperation.

The Partnerships Victoria policy for public-private infrastructure projects (exceeding AUS$10 million) stipulates additional public interest criteria that are applicable in the context of this thesis: effectiveness, accountability and transparency, providing for affected individuals and communities through consultation and appeals, consumer rights, security and privacy (Department of Treasury and Finance, Victoria, 2002: 8).36 The Virtual Global Taskforce requires that corporate partners must evidence five principles including “a proven track record of co-operation with, and a public commitment to, law enforcement” (Virtual Global Taskforce, 2006).

Increasingly, many ethical standards for policing have been codified as legal standards, thus raising the low bar. Public police powers and legal standards for their use are set out explicitly in statute law and common law precedents. Police powers include amongst others authorities to enter, search and seize, cooperation as a vice. Cohen and Feldberg (1991: 145) also argue that, “widespread practice, entrenched custom or the dictates of police culture do not, by themselves, establish a moral standard.” Moral principles are objective: “If a moral principle is correct, it is correct even though people rarely, if ever, live up to it”.

36 Although, Partnerships Victoria explicitly excludes police services from consideration under the policy, as core government services, and because “it is in the public interest that government retains direct control” (Department of Treasury and Finance, Victoria, 2001: 4).
conduct surveillance, interrogate and use force to arrest (see Edwards, 2005: 19-23). In Victoria, state police powers are enshrined primarily in the *Crimes Act 1958* (Vic) as amended frequently. Police can only enforce the current law; not the law as they or others think it should be and they can only so do using powers granted under the law. Contrary to Cohen and Feldberg’s criteria about unreflective enforcement, Edwards argues police have a duty to enforce the criminal law and not ignore unpalatable incidents (Edwards, 2005: 18).³⁷ Police collection of evidence must meet a standard for criminal prosecution.

In Australia, laws relating to private investigation are not found as easily, often deriving from common law considerations of other professions, such as journalists in the case of privacy (Sarre and Prenzler, 2005: 6). Private investigators derive their policing powers from criminal, property, employment, contract and common laws (Sarre and Prenzler, 2005: 68). They are held generally to different if not lower legal standards than police and many principles of law said to attend to them have not been tried in court (see especially, Sarre and Prenzler, 2005). As examples, they can choose not to enforce the law and might only need to collate evidence to a civil standard depending on circumstances. Use of data surveillance devices by public police is regulated in Victoria by the *Surveillance Devices Act 1999* (Vic). However the Act does not regulate at all use of such devices by private investigators who would be free to use technologies for keyword searching and blocking of email, surveillance of Internet usage and keylogging (see also, Sarre and Prenzler, 2005: 143-168). In relation to partnered investigations this point is moot as persons assisting law enforcement are permitted specifically to employ such techniques of surveillance under the Act.³⁸ Increasingly,

---

³⁷ Police discretion to enforce the law has been subject to much debate (see eg, Kleinig, 1996b).

³⁸ See Smith, Grabosky and Urbas (2004: 71) for a discussion of when the involvement of private third parties is considered action by the State.
cooperation with law enforcement is legislated (see for example, Crime and Disorder Reduction Partnerships mandated by the UK *Crime and Disorder Act 1998* as amended by the UK *Police Reform Act 2002*).\footnote{See also note 24.}

The ethical standards of Victoria Police are stated concisely in the Code of Ethics motto, “I uphold the right in my role within the Victoria Police Force by acting impartially, with integrity and by providing service excellence to everyone” (Victoria Police, 2002a). As a step towards their own visible professionalism, industry associations for private investigators increasingly employ codes of ethics for their members. As an example, the AIPI Code of Professional Ethics states:

1) The Institute shall be non-political and non-sectarian.
2) The integrity and reliability of members must be beyond reproach.
3) A member shall not negligently, maliciously or willingly injure directly or indirectly the reputation, prospects or business of another member of the Institute / investigation profession.
4) All inquiries and investigations undertaken by members must be conducted within the relevant laws of the states and Commonwealth of Australia and the AIPI Code of Ethics.
5) Members shall not disclose information obtained by them in the course of their profession unless authorised by law and with the consent of their principal / employer / client.
6) Members shall conduct themselves in a manner that does not damage the good standing of the Institute (AIPI, 2003).

Professions are generally characterised by provision of a public service, possession of a code of professional ethics, specialist knowledge and expertise, higher education, autonomy and discretionary authority and self-
regulation (see Kleinig, 1996b: 31-41; Johnston, D.G., 2001: 59-61). Jennings, Callahan and Wolf (1987: 5) argue that not only is ethical behaviour intrinsic to professions, but that this justifies applying higher moral standards to its members:

In ethical terms, to be a professional is to be dedicated to a distinctive set of ideals and standards of conduct. It is to lead a certain kind of life defined by special virtues and norms of character… Higher standards of moral responsibility can and should continue to be applied to the professions.

As policing often requires on-the-spot judgments, the Victoria Police Code of Conduct utilises the SELF Test mnemonic, which stands for “Scrutiny, Ensure compliance, Lawful and Fair” (Victoria Police, 2005a: 201-1: s1). The Code implements these standards by posing four simple questions for members: “Will your decision withstand scrutiny?”, “Is your decision ethical?”, “Is your decision legal?”, and “Is your decision fair?”

Public police are also held to performance measures of effectiveness and efficiency indicated variously by crime and clearance rates and even recently customer satisfaction (Dadds and Schiede, 2000; Edwards, 2005: 240-244). Demands for more efficient and effective policing have driven police reform in Australia for the past 30 years (Flemming and Rhodes, 2005: 192). Police and private investigators are subject to similar performance measures, such as controlling costs of investigations and profit margin, customer satisfaction, reputation and avoidance of penalties. In both policing and business the iron triangle of cost, quality and timeliness often rules. “Growth of the business” as a performance measure of private investigators is where they differ. Two kinds of competence are required: skill to provide the services investigators

__________________________

40 See also Kallman and Grillo (1996) for questions that can guide decision-making through the various ethical philosophies.
advertise and resource management to make sensible business decisions (Gill and Hart, 1997a: 128).

Measures of “effectiveness” and “efficiency” in policing have generally been poor indicators of police activity; but programmes designed to improve police efficiency have also been flawed (Froyland and Bell, 1996). How will the successes of partnership policing be measured? The most basic definition of success is “to set out to do something and to succeed in doing it” (de Bono, 1985: 9). The main aim of the Australian e-crime strategy is to “reduce the incidence and effects of electronic crime” (Electronic Crime Steering Committee, ACPR, 2001). The goal of Victoria Police is a general crime rate reduction of five percent by 2008 (Victoria Police, 2003a: 4). As a hybrid of previous policing models, partnership policing may be seen as a hybrid short-term and long-term strategy. As a short-term strategy, partnership policing is likely to focus upon measures traditional to reactive policing, such as number of prosecutions. This may be a poor indicator in terms of e-crime, due to the relatively few prosecutions in the related area of fraud (Levi, 1987: 118) and traditionally lenient sentences. Regulation of these issues may also be delegated to regulatory bodies (Levi, 1987: 118). Yet, how can maximising a performance indicator such as number of prosecutions reconcile with the simultaneous aim of reducing levels of crime (Flemming and Rhodes, 2005: 194)?

Abbey and Butten (1997: 39) argue that community safety measures must focus on outcomes as “the results of what is done”. They argued that outcomes should be stated in absolute terms, such as the incidence of a type of crime and changes over time. These are distinguished from inputs (resources) and

---

41 The crime rate is calculated from “the total number of crimes reported and recorded by police per 100,000 population in any particular period” (Victoria Police, 2004b: 6).
outputs (processes) of agencies, programs or partnerships. Victoria Police has already signalled it has discontinued the ‘count’ of policing partnerships as a performance measure, when it failed to meet its projected target by almost 50% in 2004/05 and the lack of value in such an indicator became clear (Victoria Police, 2005d: 13). Production of a more proactive policing strategy requires needs assessment about how efficiently and effectively police perform to outcome measures (Abbey and Butten, 1997: 149). The results of long-term strategies, such as proactive policing, are not easily measured in performance indicators and contracts (Flemming and Rhodes, 2005: 195). Prevention of crime per se might be preferable to the private sector but is difficult to measure. Where partnerships can be instituted and documented between police and private entities, lack of crime in or against the individual workplace over time might become a measure of partnership policing success. However such a measure might lack validity due to innumerable intervening factors.

At least four formal watchdog mechanisms provide oversight of the above standards for Victoria Police: the courts, the Office of Police Integrity (OPI),42 the Victoria Police Ethical Standards Division and the Privacy Commissioner. Requirements to publish annual reports and crime statistics are additional accountability mechanisms. Different public accountability mechanisms are mainstays for private police including licensing and training requirements, criminal records checks, industry self-regulation and civil43 and criminal liability (Sarre, 1998; Sarre and Prenzler, 2005). Customer and shareholder considerations also govern them (Stenning, 1989: 182). The application and effectiveness of these mechanisms is considered haphazard: licensing in

42 Replaced the Police Ombudsman in 2004.

Australia is considered piecemeal, civil suit is unlikely due to costs, criminal prosecution unlikely due to low visibility of the industry and “illegal or morally reprehensible yet effective” practices might actually be sought in the marketplace (Sarre, 1998: 101).

Following the introduction of the *Private Security Act 2004* (Vic), which came into effect on 1 July 2005, the Chief Commissioner of Victoria Police has direct responsibility for licensing and registration of private investigators in Victoria; those powers are delegated to the Licensing Services Division (LSD) of Victoria Police. To improve professionalism, regulation under the Act includes training requirements and probity checks including initial and ongoing monitoring of criminal history during the life of a license.44

Arguments for mutual benefit in partnership arrangements often stem from pragmatism of engaging and retaining support of private partners, rather than moral principle (see for example, MacNeil, 1968 above). In terms of partnership policing, this is complicated by at least three sets of interests (Figure 3.2). Public interests do not always coincide with the interests of police organisations. Likewise, what is considered the public good has the potential to change. Figure 3.2 illustrates that public-private partnership is most beneficial when all three spheres of interest intersect. If private interests do not accord with those of the public good, should not the public good supersede those interests? Where public interests coincide with private interests, but not with current police interests might that not suggest that these should become public police interests?

---

44 Investigators were required to complete a generalist Certificate Level III in Investigative Services by 1 March 2006 (or have completed equivalent or higher certification previously).
Given the usually different legal and ethical standards for public and private police outlined above, how does this affect standards for partnership policing? Does private sector partnership with public police, especially cooperation that is formalised, require private investigators to adhere to higher legal or ethical standards than they might otherwise be held to during their separate private practice? Are current standards and accountability mechanisms for private investigators sufficient for the proposed partnerships? Or, because public police accept higher standards as part of the police role, is it sufficient that public police are the bastions of public interests during investigative partnerships? The next section examines previous attempts to recommend appropriate relationships between public and private police.

**Prescribing relationships between public and private police**

There have been several attempts in the criminological literature to describe the relationships between public and private police (Shearing, Stenning and Addario, 1985; Marx, 1987; Stenning, 1989; Shearing, 1992; McManus, 1995;
Morley and Fong, 1995; Gill and Hart, 1997b; Golsby, 1998; Jones and Newburn, 1998; Nalla and Hummer, 1999; Johnston, L. 1999; Sarre and Prenzler, 2000; Bayley and Shearing, 2001). Normative theorising about what ought to be the state of affairs for any particular justice issue has been central to criminology since the Classicists. However, few attempts have been made to prescribe ethical public-private police relationships (Marx, 1987; Stenning, 1989; Loader, 1997; Golsby, 1998; Sarre and Prenzler, 2000) and these rarely include detailed recommendations. Loader (1997: 378) notes a normative impoverishment and lack of imagination in the discourse on private security.

Marx (1987) highlighted the need to address joint public-private investigations; each sector hiring the other or delegating authority to private police; organisational forms that blur public and private and the circulation of personnel between the policing sectors. He argued that a hydraulic principle might govern relationships between police and private investigators requiring new (unspecified) forms of accountability:

Restrict the conditions under which the police can carry out searches and seizures and undercover activities, coercive interrogation after arrest, or collect data on those who are not specific suspects, and police may make increased use of private detectives and informants who are less accountable and not as subject to such limitations (Marx, 1987: 186).

Stenning (1989: 173-179) offered a five-stage sequence to describe the interactions and level of cooperation between police and private security personnel. Until the 1970s, interactions could be described as “denial” or a “refusal to acknowledge that private policing was a legitimate topic”. The second stage in the early 1970s was a “grudging recognition” accompanied by “denigration”. Public police distinguished the work of private police from “real policing”; an attitude persisting through the 1990s (Nalla and Hummer,
1999). The third stage was characterised by “competition” and “open hostility” as private policing threatened the so-called public police monopoly, based coincidentally on recognition of fiscal crises within public policing, private police effectiveness and criticisms of corruption from the “old boys network” (Stenning, 1989: 175). The resulting fourth stage involved “calls for more controls” over private providers who were then seen as a necessary evil. In the 1980s, police moved to calls for “active partnership” as described generally above. This would involve formal protocols and liaison with police as “senior partners” and private providers assisting the public agenda (Stenning, 1989: 180). Stenning (1989: 177) noted that recognition and cooperation was conditioned on establishing and maintaining standards of ethics and training that Canadian police had themselves yet to establish.

Arising from his observations, Stenning (1989: 179-86) proposed a normative sixth stage of interaction, which he termed “equal partnership” in which police should abandon the “senior partner” role:

I strongly believe that if the public police approach their relationship with private policing organizations as an EQUAL PARTNERSHIP in this way, in which each partner is equally committed to discovering and implementing the most effective conceptions and practices through which to do policing, the quality of policing services which we receive as citizens could be greatly enhanced (Stenning, 1989: 185-86, emphasis in original).

Police should strive to better understand private policing and Stenning even imagined that public police might inventory all policing resources, public and private, and negotiate a master plan to deploy those resources that constituted the “best policing service”. However, Stenning (1989: 180-181) argued equal partnership is hampered because private police benefit from the myth that they do not do “real policing”, which lets them avoid public
scrutiny and certain accountability mechanisms.\footnote{Haines (1995: 260) confirmed that businesses in general “in response to threat, aim to reduce their vulnerability to scrutiny, and so too liability”.
} Button (2002) argues there are still few examples of police treating private counterparts as equals.

Gill and Hart (1997b: 564) suggest there are no practical reasons, only ethical concerns, that public police investigative work might not be contracted out as are guarding and patrolling duties. Loader (1997: 382) reasons that policing entails elements of compulsion that simply cannot be contracted out. He further argues that security is an indivisible public good and to promote policing as a user pays, two-tiered provision of security, undercuts social cohesion and even “the most stringently controlled private security industry might still serve to cement and exacerbate social inequalities” (Loader, 1997: 385).

It is often argued that public policing is becoming a service for the poor and less privileged as private policing is sold to the wealthy (Reynolds and Wilson, 1996). E-crime has the potential to widen this gap. As discussed in Chapter Two, e-crime investigations are often technically complex and hence expensive and it is conceivable that public police might turn away certain e-crime victims as they attempt to cope with fiscal crises and segmentation of policing functions (see generally, Reynolds and Wilson, 1996: 223).

Loader (1997: 388) concludes that all forms of security provision, including policing, should be “located within some kind of framework of democratic deliberation and decision making” and to think beyond “legal regulation” to considerations of sustaining justice and legitimacy. By this he meant (quoting Habermas (1996: n.77, 408) cited in Loader, 1997: 387) “build interactions as moral transactions, not only as market exchanges” and that public discussion
should replace market forces. Golsby (1998) also called for equal partnership in relation to cooperative crime prevention in Australia and suggested a liaison committee and a public complaints system similar to those for police. However, the number and disparate views of private security representative bodies pose communication problems for police (Golsby, 1998: 124). Golsby suggested a private security federation should be formed to address this.

**Sarre and Prenzler’s Regulated Intersections model**

Rick Sarre and Tim Prenzler (2000) have offered the most comprehensive attempt thus far to stipulate an appropriate relationship between public and private police. They call their normative—in their words “prescriptive”—model the *Regulated Intersections* model. The model draws upon the best qualities of seven descriptive models that they also offer to account for observed interrelationships. The descriptive models can be summarised in terms of the distinctive characteristics that they emphasise about where policing takes place and how, when and why the parties interact (see Table 3.3). The *Property* model focuses upon where policing takes place, either on public or private property and the boundaries this creates; the *Division of

---

46 Equally problematic is the fragmented representation of the ICT industry. For example the Australian Industry Group (Ai Group), Australian Computer Society (ACS), Australian Electrical and Electronic Manufacturers’ Association (AEEMA), Australian Information Industry Association (AIIA), Australian Information Security Association (ASIA), Internet Industry Association (IIA) and System Administrators Guild of Australia (SAGE-AU) are but a few of many Australia organisations.

47 Sarre and Prenzler (2000) do not delineate private policing from private security. As their respective roles and issues about their interaction with public police may be very different, thus requiring differentiated responses this thesis differentiates the two.

48 Property boundaries exist even in cyberspace. Although the computer networks that developed into the modern day Internet began in public universities in the United States, it is
Labour model focuses upon how each sector addresses crime control through different measures. The Competing Forces model focuses upon conflict between the sectors, ostensibly considered a competition for “market share”. The Supplementary Service model describes interaction in terms of different policing powers. The Ad Hoc Partnership model suggests police and private sectors cooperate temporarily in response to crisis events. The Combined Forces model argues that permanent, synergistic cooperation can be developed at both executive and operational levels. The Unholy Alliances model is the

<table>
<thead>
<tr>
<th>Model</th>
<th>Characteristics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property</td>
<td>Common objectives, sectors use similar means of patrol and investigation, differing mainly in terms of the location and boundaries of that activity on either public or private property</td>
</tr>
<tr>
<td>Division of Labor</td>
<td>Common goals, different methods; police focus on deterrence through investigation &amp; prosecution, private police focus upon crime prevention</td>
</tr>
<tr>
<td>Competing Forces</td>
<td>Compete for “market share”; assumed to have similar capacities to respond to crime</td>
</tr>
<tr>
<td>Supplementary Service</td>
<td>Public police have precedence due to legislated powers, superior training and equipment; security industry is regulated by police</td>
</tr>
<tr>
<td>Ad Hoc Partnership</td>
<td>Sectors combine temporarily if and when needed for particular crises or events, based on mutual need for each other</td>
</tr>
<tr>
<td>Combined Forces</td>
<td>Sectors combine permanently and symbiotically at executive and operational levels</td>
</tr>
<tr>
<td>Unholy Alliance</td>
<td>Corrupt relationships between public and private police (eg. moonlighting police and improper information sharing)</td>
</tr>
<tr>
<td>Regulated Intersections</td>
<td>Normative model; partnerships are necessary but cooperation needs to be limited and regulated closely to ensure maximum public benefit</td>
</tr>
</tbody>
</table>

Source: Adapted from Sarre and Prenzler (2000).

Increasingly true that the ICT networks and associated infrastructure are owned and operated by private sector commercial entities.
model to be avoided; arguing that corruption derives from relations between police and private security.

Sarre and Prenzler (2000: 92-3) argued that much of the previous research focused upon the problems posed by having multiple sources of policing, rather than building descriptive or normative models for relationships between those sources. The Regulated Intersections model as a pragmatic compromise between the hazards and potential benefits of cooperation is premised on the mission statement that the:

distinctly different principles of service between the two sectors mean that cooperation needs to be, for the most part, limited and closely regulated. At the same time, ad hoc and established partnerships are necessary responses to the inevitable interaction and conflicts due to overlapping responsibilities. Procedures are required to establish standards and to ensure maximum public benefit (Sarre and Prenzler, 2000: 97).

Some of the differing principles to which they refer are police and private investigators having different ‘masters’, training disparities, conflicts over ownership of successes and failures, differing abilities to assist victims and frustrations with responding to false alarms (Sarre and Prenzler, 2000: 107). “Regulated” implies assessing and controlling interaction against public interest provisions of the police mission (Sarre and Prenzler, 2000: 106). “Limited” interaction might imply “maintaining a respectable distance” (Sarre and Prenzler, 2000: 106). Such a model, they argue, should ensure maximum public benefit and a “level playing field” for security operators, while carrying the expectation that they have a social obligation to assist the public beyond commercial interpretations of their contracts (Sarre and Prenzler, 2000: 106). However, they also urge “caution should temper any push towards a totally symbiotic cooperation between the public and private
policing”, weighting avoidance of corruption as preferable to crime reduction accompanied by corrupt relations.

That unholy alliances should be avoided is self-evident. The challenge is to devise relationships that avoid corruption and at the same time achieve crime control. “What works” is an oft-rued question in criminology and interventions are often plagued by unintended consequences. Sarre and Prenzler (2000) make five suggestions for “regulating cooperation” between police and private security:

- maintain “a respectable distance”;
- have regular meetings;
- cooperative opportunities should remain a standing agenda item;
- establish an executive level standing committee involving police, senior private figures and an ombudsman; and
- licensing of private security should move away from police, because they argue that currently undermines perceptions of equality.

The relationship between police and private security in Spain has been described as a “regulated intersections” model, where the relationship has been defined clearly through legislation since 1992 as complementary forces (Gimenez-salinas, 2004: 160, 162). In Spain, “mixed commissions of coordination” establish collaboration and coordination of efforts and a “coordination room” established in 2000 coordinates information sharing.

Sarre and Prenzler’s model suggests underlying adherence to philosophies of post-Keynesian policing that it be consultative, the community has a “social obligation to assist” and support for the continued predominance of state sponsored police forces. Their model supports more equal status between the sectors, as did Stenning (1989) and Golsby (1998). It depicts Deering and
Murphy’s (2003: 28-30) “arm’s length” partnership by tolerating difference and reducing negatives, navigating between filling competence gaps and the need for instant independence.

However, what constitutes appropriate regulation and how to enact this remain central debates within criminology (Grabosky and Braithwaite, 1986; Braithwaite, 1989; Ayres and Braithwaite, 1992; Braithwaite, 1993; Grabosky, 1995; Haines, 1995, 1997, 2002, 2003, 2005; Cherney, 1997; Haines and Sutton, 2003; Crawford, 2005). It is unlikely there is a single, simple solution to these problems. One must avoid juridification⁴⁹ that attempts to use technocratic solutions to address political problems (Haines and Sutton, 2003: 18). Thus the general trend in regulation is from coercive to co-operative regulation (Crawford, 2005). Assessment of regulatory reform requires consideration of regulatory contexts as well as regulatory techniques, as these interact (Haines, 2003). The interaction between individuals, social norms and formal laws has been termed regulatory character (Haines, 2003: 469). Consideration of regulatory character involves mapping the tensions that underlie implementation of particular reforms and how they fit or mismatch existing character of “how things are done around here” (Haines, 1997; see Figure 3.3). Benefit lies in the ability to explain both local and global influences and the unique and familiar in contexts (Haines, 2003: 469). Sarre and Prenzler’s model is a proposal for a particular regulatory character, more so than prescription of any particular regulatory technique (see Figure 3.4).

---

⁴⁹ Juridification is “increased reliance on detailed instructions, rather than on less formal modes of authority to ensure compliance with state requirements” that tend to overwhelm regulated organisations and individuals through conflicting requirements (Haines and Sutton, 2003: 3).
Ironically, although this thesis is concerned with partnerships for investigating crime, underlying this normative model for relationships between these potential policing partners is prevention of misconduct and waste as its fundamental requirements. This suggests that theories and
techniques of crime prevention might apply to the problem. Sarre and Prenzler’s focus upon regulating intersections suggests relevance in Cohen and Felson’s (1979) ‘routine activity approach’ to crime analysis to analyse the intersections between public and private police personnel. Their approach examines the circumstances necessary to produce crime and how social settings and institutions act to either create or deflect those circumstances (Cohen and Felson, 1979: 594). Exploitative, predatory crimes are said to rely upon the physical convergence of three elements, known today as ‘Felson’s triangle’: a likely offender, a suitable target and the absence of a capable guardian (Cohen and Felson, 1979: 589). Felson (1998: 67-71) examined the chemistry of vice crime in terms of “quick dash” transactions between sellers and buyers in the absence of place managers who might prevent these.


By their own admission, these models are an “abstraction from empirical chaos” and are inevitably “limited, nebulous and involve overlaps or different applications in different circumstances” (Sarre and Prenzler, 2000: 94). The challenge is whether these models can be applied usefully to real policing problems and it is in that vein the models will be assessed in this thesis. How well do Sarre and Prenzler’s descriptive models explain the interactions

50 The number of techniques was later extended to twenty-five by Cornish and Clarke (2003) in response to Wortley’s (2001) critiques relating to ‘situational precipitators’ of motivation to commit crime.
between public police and private investigators in the realm of e-crime investigation? More importantly, how beneficial is the normative model they propose to future cooperation between public police and private investigators for e-crime investigation?

A regulated intersections model requires knowledge of intersections. When do police and private investigators interact in relation to e-crime investigation? When, where and how might they interact that requires additional or new forms of regulation? What regulation or limitations are needed to institutionalise positive, appropriate interaction? Are current accountability mechanisms sufficient or do they require reform? What “key entry points” exist for regulation of investigative partnerships (Haines, 1995: 271)? Does the Regulated Intersections model fit with existing regulatory character? Might partnership policing, if implemented wisely, act as a corrective to the undercutting of public policing by private security of which Loader (1997) warned? As police are forced through fiscal crises and practicality to ally with private providers of policing might they achieve equitable distribution of policing? And more specifically, what role might situational prevention techniques play in preventing corruption in partnered public-private investigations?

**Chapter conclusions**

Recent developments in policing suggest that partnership policing should be distinguished clearly from community policing. First, partnership policing underscores collaboration between “professionalised” police services and “responsible” communities, unlike early welfare models of community policing. Second, learning from the unintended consequences of community policing, partnership policing seeks to place less emphasis on the
community’s reported crime and community safety needs so police regain control of the agenda. Third, the broad language of “partnership” permits flexibility of response and improvised initiatives such that it might entail policing through networks, contractualism or even third party policing.

The preceding discussion of standards that apply separately to public and private policing personnel demonstrates that although in general the two groups must consider many of the same principles, such as integrity, privacy and success, they are generally held to these by different measures. Arguably, when considered in tandem, these mechanisms might regulate effectively public and private police working in partnership. Previous attempts to prescribe normative relationships between public and private police have generally taken one of two directions: either promoting virtuous behaviours (equal partnership) or counselling avoidance of non-virtuous ones (corruption). These are not irreconcilable positions, but reflect concern with either aspiration to ethical virtues or preserving the minimum standards of duty under law. It is important not to ignore either one when considering a normative position; as to do so might either stunt potential benefits or have the carpet pulled unexpectedly from under one’s feet.

Sarre and Prenzler consider cooperation and partnership central elements for police and private security interactions as pronounced in their Regulated Intersections model, whilst avoiding the temptations of corrupt relationships. However, they admit that the precise mechanisms and limits of their model need further analysis and clarification (Sarre and Prenzler, 2000: 106). The next chapter outlines an empirical study to examine issues of partnership policing further in the context of this model, the above general policing standards and the proposals for greater inter-sectoral cooperation in e-crime investigation to establish appropriate principles and procedures.
Chapter 4: Research design and methods

The preceding chapters highlighted the tensions between potential benefits and costs of partnered policing of e-crime. Benefits might include new effectiveness and efficiencies in investigations, which might serve multiple stakeholder interests. Misgivings about closer cooperation between public and private police extend generally from previous examples of impropriety. Many questions about the hybridisation of policing and appropriate relationships between public and private personnel are yet to be answered. Bayley and Shearing (2001: vii) note that most of their explanations of changes to policing are largely academic hypotheses, yet to be tested or confirmed empirically. Likewise, Sarre and Prenzler (2000: 106) admit that the precise mechanisms and limits of police and private security interaction in their normative theory require further examination and theorising.

This chapter outlines the design of a program of research to undertake a critical examination of the questions and issues raised by partnership policing of e-crime, from which normative guidelines for implementation might be proposed. First, the key research questions and hypotheses to be studied are refined from the many issues raised already. The next section discusses an appropriate methodological stance for framing this normative research. The final section examines the choice of appropriate research methods and describes how these procedures were implemented.

Research questions and hypotheses

The central aim of this thesis is to examine critically the conditions under which partnership policing of electronic crime at the state police level can be
mutually beneficial to law enforcement and the private sectors, while maintaining public interests.

In writing their law enforcement strategies, law enforcement agencies have hypothesised already that partnership policing is an answer to e-crime. What impact, if any, does partnership with the private sector have on the successful policing of e-crime? Is partnership policing beneficial especially for particular types of e-crime or is it a measure required across the board? What contexts exist that either facilitate or hinder partnered investigative efforts? Sarre and Prenzler (2000) have suggested that interaction between public police and private security should be limited and regulated closely to avoid corrupt relationships. How useful is their normative model? Can investigative partnerships be developed between police and private investigators that are mutually beneficial while preserving public interests? What contexts are needed for this and are these present in Victoria? What, if any, are the implications of corporations and private investigators not partnering with law enforcement? What if they chose to not to “be partners” and do not assist law enforcement actively and wholeheartedly?

Fundamental to this analysis, because the policing of e-crime is a newly emergent phenomenon, several conceptual building blocks need closer examination. Academia has articulated several definitions and broad typologies to describe electronic crime, which have been variously adopted within law enforcement circles. Does the ambiguous definition of “electronic crime” assist or hinder public and private policing of these types of incidents? If the definition hinders effective policing, how does this then contribute to a more appropriate definition of “electronic crime”? Grabosky, Smith and Dempsey (2001: 204) suggest the literature lacks descriptions of the organisational forms through which law enforcement interact with non-
government actors in relation to electronic crime. Grabosky et al (2001: 205) also note that knowing which legislative reforms work and which do not aids those jurisdictions yet to enact legislation and where unsuccessful allows for jurisdictional reform. How do those who are asked to take action in reply to incidents of e-crime respond, whether that is separately or with their counterparts?

If partnerships are found to be an important factor in the successful policing of electronic crime, it will then be incumbent to suggest an appropriate model and mechanisms by which these partnerships should be guided. Such partnerships should aim to be mutually beneficial to law enforcement and the private sector, while maintaining the public interests enunciated in Chapter Three. Such norms may be expressed in the form of prescriptions, preferences, permissions or proscriptions (see generally, Merton, 1982: 5).

**Methodology**

Justifying one’s choice amongst the competing paradigms that guide inquiry, especially qualitative inquiry, has been an almost bloody battle between researchers in the social and natural sciences (see especially, Guba and Lincoln, 1994; Pawson and Tilley, 1997). In this research, it is the aim of the research that guides that choice foremost, seconded by the preference of the researcher. This thesis aims to learn from current practice at the coalface so as to guide future policy and practice. The point of such applied research is to inform policy makers, practitioners, participants and the public in addition to a contribution to academic knowledge.

“Doing criminology” according to Anthony Bottoms necessitates engagement with normative issues (Bottoms, 2000: 48). As “crime” itself is a normative category defined by societies through social censure this is inescapable
By extension, the study of policing must also engage with norms. Normative theory and analysis is primarily about seeking principled answers to questions of what ‘ought’ to be. As Bottoms points out, this form of theorising differs subtly from explanatory research, in that the aim is not to use theory and data simply to find true explanations of social phenomena.

Normative analysis is not engaged in a search for truth in quite the same way: rather it attempts a rational and principled exploration of moral/political justifications for a given course of action (Bottoms, 2000: 48).

However, normative analysis is also not simply armchair theorising as early positivists argued (Bottoms, 2000: 50). Empirical research can illuminate the philosophical analysis of norms. The normative theorist considers what criteria justify a particular normative proposition. Without intending to exhaust the list, these criteria may be legal, moral or ethical principles or evidence supporting ‘best’ or ‘recommended’ practice as outlined in Chapter Three (eg, MacNeil, 1968; Cohen and Feldberg, 1991; Greenberg, 2000). The purpose of an ethical analysis is to seek reasons rather than authority to justify principles (Pojman, 1989; 4). Then the normative theorist considers whether the reality of the situation meets the criteria to support adopting a proposed position. In this way, empirical research advances a normative debate, however it has done so differently to explanatory research (Bottoms, 2000: 49). Given the novelty, in many senses, of the investigation of electronic crime, it is crucial to also provide explanatory accounts of current practice.

Accordingly, the ontology or worldview accepted in this research accords with the assumptions underlying Pawson and Tilley’s treatise for realistic evaluation. The e-crime problem is real. Attempts to address the problem and the attendant successes and failures of those attempts are also real.
Constructivist paradigms are fraught with casuistry and solipsism that do not lend them to applied research.

To be realistic, it is necessary to look beyond and beneath the political rhetoric and legal discourse that surrounds the key players. It is necessary to attend to the reality stratified in individuals and institutions, their structure and agency. Social programs, like the partnerships envisaged in partnership policing, create interplays of disagreement, power-play and interdependencies that often resolve into real-world customs and practices, which Pawson and Tilley (1997: xiii) argue are often not quite what people want them to be. These are the phenomena of realist inquiry and this research. Further, this research adopts a hypothetico-deductive approach (Kellehear, 1993), which attends such a postpositivist paradigm (Guba and Lincoln, 1994: 110). Bottoms (2000) argues that Pawson and Tilley’s focus upon explanation in evaluation studies is a useful corrective to its neglect by some experimental/quasi-experimental researchers.

The logic of a realist evaluation follows Wallace’s ‘wheel of science’ (Wallace cited in Pawson and Tilley, 1997: 85). Figure 4.1 illustrates this cycle from a realist viewpoint, which is the approach taken in this study. Pawson and

---

51 The term postpositivist refers to efforts in the last few decades to respond to the critiques against positivism, while maintaining the basic critical realist ontology (Cook and Campbell, 1979). Such critiques include “context stripping”, excluding situated “meaning”, relying on an “etic” (outsider) viewpoint and exclusion of “discovery” from inquiry by reliance on a priori hypotheses among others (Guba and Lincoln, 1994: 106-7). The postpositivist methodology emphasises “critical multiplism” (essentially triangulation) as a way of falsifying (rather than verifying) hypotheses. This methodology reintroduces “discovery” as an element of inquiry, soliciting emic (insider) viewpoints to assist determining meanings and purposes, and to contribute to “grounded theory” (Glaser and Strauss, 1967). Replicated findings are probably true, but subject to falsification (Guba and Lincoln, 1994: 110).
Tilley (1997: 75) argue for the conceptual clarity of restating theories in terms of how mechanisms for change are ‘fired’ by programs in particular contexts to produce outcomes. “Outcomes follow from mechanisms acting in contexts” (Pawson and Tilley, 1997: xv).\(^\text{52}\)

\[ \text{Mechanism (M) \times Context (C)} \rightarrow \text{Outcome (O)} \]

Often this is the case, Pawson and Tilley would argue, of an introduced mechanism overcoming another ‘blocking’ mechanism that led to the original problem. Restated in the milieu of this thesis, it is that “cooperation” between police and the private sectors is the mechanism that will effect some change in the existing social processes, which led to the problem of e-crime policing difficulties. It is hypothesised that partnership policing will trigger cooperation and community responsibility for crime and effect desired outcomes in crime rates. In more traditional scientific language, cooperation is the independent variable, supposed to be effected by a program of partnership, and which works also on the independent variable of e-crime, hopefully reducing offending. It is also hypothesised that limiting and regulating interaction between public and private police is necessary to do this without corruption.

\(^{52}\) Pawson and Tilley’s (1997: xv) original notation uses an addition sign, however Bottoms (2000) suggests the multiplication sign more accurately depicts their argument. This consideration of CMO configurations underlies Haines’ (2003) analysis of regulatory character.
The task from a realist perspective is to therefore to ask “what works for whom in a set of given circumstances” and make empirical observations tailored carefully to the hypotheses to test these circumstances (Pawson and Tilley, 1997: 86). In normative studies, it is important to state clearly the points of view from which such an evaluation is pursued (Ruttio, 2005a). This study examines key stakeholders: investigators working in Victoria Police, private sector financial institutions and government agency investigators in their current circumstances and those of the proposed partnerships. Victims of e-crime are also considered as those for whom law enforcement acts. Ruttio (2005b) argues that in normative research the preferences of those people who are going to encounter the result of a project or use it should guide the research. That seems a potentially relativistic stance, given the objective
criteria against which police are judged formally. Where the standards are silent, stakeholder preferences will be considered.

The difference of the realist evaluation cycle from much positivist research is that instead of moving from observations to unqualified or unconditional generalisations realist evaluation aims for program ‘specification’ (Pawson and Tilley, 1997: 86). This means focusing upon the circumstances in which change may occur, cognisant that these circumstances, or ‘outcome patterns’ as Pawson and Tilley term them, may only be temporary given the irresistible forces of social change. Finally, the knowledge learned from observation is refined and fed back into theoretical development to effect cumulation of knowledge; in this case addressing this theoretical development from the normative angle.

Research methods and case studies

In his broader study of police undercover work (Marx, 1988), which revealed joint investigations with private investigators (Marx, 1987), Marx conducted interviews with police and private investigators, case studies and document analysis of court records, policy guidelines and media accounts (Marx, 1988: xxi-xxiii). Marx observed and even participated in police training sessions, although active investigations were off-limits. Recent attempts to research the private security industry and private investigators have most often utilised self-administered surveys (Morley and Fong, 1995; Prenzler, 1995; Gill and Hart, 1997a; Golsby, 1998; Nalla and Hummer, 1999). These studies have often focused upon opinions elicited by police and private security personnel. Some studies have noted investigators’ poor response to postal surveys (Gill and Hart, 1997a: 119; Prenzler and King, 2002). Subsequently, Gill and Hart

53 Although Golsby (1998) achieved a 55% response rate in his survey.
(1997a: 119) employed interviews (also of clients) and observed operations in their study of private investigation agencies. Prenzler and King (2002) contacted regulatory agencies to determine size of the industry and conducted interviews with investigators in the Australian states of NSW and Queensland. Others reviewed individual court cases in light of inaccurate media reporting (Broucek, Frings and Turner P., 2003), performed legal research and analysis of laws and accountability mechanisms (Sarre, 1998; Sarre and Prenzler, 2005). Chan’s (2000) examination of 207 reported and unreported hacking cases in Hong Kong was facilitated by virtue of his status as a high-ranking Hong Kong police officer.

Each method of inquiry has delivered a different form of insight into private policing and, when researched, its relationship to public police. Sarre (2005: 59) suggests the main difficulty in researching the phenomenon of private policing is “determining what exactly is ‘private policing’” and where to research it given the uneven application of the label “private police” and difficulties gaining access to the private domains involved, due to the general lower visibility, variety and constant change of such domains.

A realistic approach to research always begins with an attempt at a sociological understanding of resources and choices available to participants involved in addressing a problem (Pawson and Tilley, 1997: xiii). At the beginning of the project, meetings were held with representatives from the Victorian Department of Justice, Multimedia Victoria and the Major Fraud Investigation Division of Victoria Police to discuss the project and identify their needs on this topic that the research might address and identify investigative partnerships that could be examined.

Ideally, case studies of police and private investigators working in partnership to investigate e-crime incidents jointly could be observed
extensively. This would permit a firsthand routine activity analysis of intersections to address potential corruption (Cohen and Felson, 1979; Felson, 1998: 148). From these either successful or unsuccessful attempts could be built theoretical models of successful partnership policing of e-crime (Eisenhardt, 2002). However, at the beginning of this project, due to the ad hoc nature of investigative cooperation between the sectors, there was a lack of existing electronic crime investigative “partnerships” to observe in Victoria. This also excluded the possibility of cost-benefit analyses.54 Instead, the research was designed to examine the precursor circumstances to the formation of cross-sector investigative partnership in this area. To answer the research questions, the following design and methods were proposed:

An exploratory pilot survey would help identify community stakeholder issues. Victoria Police was interested in learning more about victims’ needs. A self-administered survey was considered appropriate to access the wider community, as this would permit anonymous responses and hopefully encourage discussion of the issues by those who might otherwise not engage with law enforcement. A survey questionnaire, disseminated widely, would also attempt to address issues of small, select sample sizes in the AusCERT Computer Crime and Security surveys.55 Survey responses could be followed up with interviews where necessary.

Analysis of closed e-crime cases investigated by Victoria Police would explore the nature of e-crime in Victoria and local factors affecting the successful

---

54 Cost-benefit analysis, cost-savings analysis, cost-effectiveness analysis and cost analysis are appropriate measures of program costs and benefits (AIC, 2003).

55 AusCERT did not reply to requests for access to the questionnaire sent to their respondents in the AusCERT Computer Crime and Security Survey, so as to facilitate comparable data in this study. This was disappointing, as a lack of comparable statistics is one of the hurdles facing both law enforcement and the private sectors.
investigation of e-crime and whether “partnerships” is one of those factors. A previous report from Victoria Police suggested the number of “computer-related offences” was low, numbering only 281 over a ten-year period from 1993 (DCPC, 2002: 203) and it was unknown how many e-crime offences would be discovered.

The Department of Justice was interested in the impact of new model computer offences legislation to be introduced in Victoria in May 2003 (see pg. 32 and Appendix C). It was neither ethical nor possible to assign persons randomly to experimental and control groups to test the legislation’s impact. Therefore, it was considered that a "switching replications" design (Cook and Campbell, 1979; Trochim, 2002) might be used to compare case dispositions in Victoria with matched offences in New South Wales (NSW). NSW had already enacted the model computer offences, as section 308 of the Crimes Act 1900 (NSW) over a year before Victoria. However, NSW had apparently at that time not yet prosecuted anyone under the new legislation (NSW Bureau of Crime Statistics, 29 Oct 2002, personal communication). Similarly, during this project, only a handful of incidents were prosecuted in Victoria using the model computers offences, ruling out meaningful statistical analysis. Instead the impact of the legislation was explored through interviews and incident records.

E-crime investigators would be key informants to this research. Private sector investigators and members of Victoria Police would be interviewed as members of an expert population, those having practitioner knowledge of investigating e-crime. Interviews with police and private sector investigators would examine the different sectoral responses to e-crime and examine proposals for public-private partnerships in detail. These interviews were used as a means of confirming or disconfirming themes that had emerged
from documentary data, such as the closed cases analysis and elaboration of findings from the official records and other interviewees.

On 20 May 2004, midway through this research, the Australian commonwealth government announced the formation of the Joint Banking and Finance Sector Investigation Team (JBFSIT) at the Australian High Tech Crime Centre in Canberra (Minister for Justice and Customs, 20 May 2004). The JBFSIT provides for secondment of investigators from the major Australian banks and state police forces to the AHTCC (see Table 2.3), where they work together on a daily basis to investigate high-tech e-crime, especially phishing incidents (ZDNet Australia, 20 May 2004). Other major institutions such as MasterCard International, Visa International and the Credit Union Services Corporation Australia Limited (CUSCAL) also support the team. The JBFSIT works closely with AusCERT to respond to incidents of online ID theft reported to AusCERT and the AHTCC (AusCERT et al, 2005). It represents the clearest example available of ongoing partnership policing of e-crime in Australia. While this is a federal initiative and located in the nation’s capital Canberra, the team interacts with and impacts upon policing of e-crime in the state of Victoria. As a model of public-private partnership in practice, the JBFSIT has had to address issues of secondment, information sharing and security and private sponsorship of policing among others. Once the team had been in operation for six months, a two-day field trip to Canberra in February 2005 was negotiated with the AHTCC to interview members of the JBFSIT to capitalise on this development and provide a limited case study of investigative partnership. Six interviews were conducted over the two days. Could and should this initiative be replicated at the state level?

---

56 AusCERT did not respond to requests for interviews of its staff to explore its relationship with law enforcement.
It was also late in 2004 that another initiative formed, which provides a second case study. This initiative grew from the *Graduate Certificate in Electronic Crime Investigation* at Melbourne University Private. The course is a cross-sectoral melting pot, taught by university lecturers and detectives from Victoria Police to students from various corporations and government agencies, including Victoria Police. Included in the curriculum I taught was the topic of partnership policing of e-crime. Having completed the course some alumni who held a common vision for “creating partnerships and awareness”, including members of Victoria Police and private sector investigators, decided to form an industry association to address their perceived need for standards within the Australian forensic computing industry and development of cross-sector partnerships with law enforcement, both locally and internationally. The Electronic Crime and Forensic Technology Association of Australia (EFTA) was formed as a not-for-profit incorporated association.\(^57\) EFTA aimed to be an investigative partnership by facilitating work experience for forensic computer investigators in different settings, either police or industry. I was invited to hold a position on the steering committee and attended committee meetings at which the intentions and aims of EFTA were discussed and formulated.

Although an as yet unsuccessful attempt to establish an industry association in Australia for forensic computer specialists and e-crime investigators, EFTA highlighted numerous issues attendant to one-to-many configurations of investigative partnership (for example police-to-industry), especially through industry bodies.

In the middle months of 2005, a commercial investigation firm approached the Computer Crime Squad of Victoria Police to initiate discussions about a

\(^{57}\) Exempting EFTA from the *Partnership Act 1958 Vic*, according to section 2.
partnership for policing of e-crime. The researcher was invited by both Victoria Police and the firm to attend the subsequent meetings as an observer. Two meetings were held in the final months of data collection where a one-to-one commercial partnership was considered and issues related to such a partnership were discussed. No partnership was agreed after these meetings, however it was too early to preclude that from eventuating. The discussions indicated important issues that would influence this and other potential partnerships of a commercial nature.

During this study, respondents did not identify any examples of formal, ongoing police-private sector investigative partnership relating to e-crime in Victoria nor any framework for forming such partnerships. However, an initiative called the Victoria Police Security Industry Partnership Committee (POLSEC) had developed a broad framework for implementing investigative partnerships between Victoria Police and private investigators in Victoria (see generally, Thompson T., 2004; Appendix D: POLSEC partnership documents). On 4 July 2003, POLSEC was formed to develop partnerships between police and the security industry. POLSEC consists of a main, statewide committee and local liaison committees. POLSEC’s credo is “Partners in Policing”. While considered still in its infancy, POLSEC has developed a Partnership Charter and liaison committees in the districts of Yarra, Stonnington, Melbourne and Geelong.

Originally chaired by Assistant Commissioner Trevor Thompson, POLSEC’s main committee is now chaired by a Superintendent following Thompson’s retirement from the police. Inspectors chair the liaison committees within local police districts. The main committee oversees improving communication

---

58 POLSEC has a low profile: Victoria Police POLSEC webpages have been removed, but remain cached online, which is how it came to the attention of this research.
and sharing of information between the sectors, capitalising on private security as “eyes and ears” (POLSEC, 7 Mar 2006, personal communication). The Yarra District POLSEC established protocols for formal information sharing and trialed manual information sharing via faxes. For security it has since opted for and developed a secure server for data sharing that is considered transferable to other partnerships (POLSEC, 7 March 2006, personal communication). Local committees scan the local security industry and form representative committees based on local needs. POLSEC’s focus has been drug dealing at hotels and nightclubs and working with security guards and crowd controllers and has not considered e-crime (Dowling, 15 August 2004; POLSEC, 7 March 2006, personal communication). For example, in Stonnington, only the Crowd Controllers Association of Australia sits on their steering committee. Stonnington learned from the Yarra district to avoid having too many industry stakeholders, who had their own ‘phantom menace’ agendas. This steering committee meets only very briefly to decide the topic of their monthly forum, which is their main focus. Four police officers and fifty to sixty crowd controllers attend these forums each month, which focus on training and setting expectations for cooperation. For example, a recent forum taught crowd controllers how to take proper notes about assaults to assist police (differing from the shorthand techniques they are taught in Certificate IV courses that often prove unreliable later) (POLSEC, 7 Mar 2006, personal communication).

POLSEC has also held an inaugural Leadership Program (VSI, 2005) and POLSEC awards (Licensing Services Division, Victoria Police, March 2005). The Association of Investigators and Security Professionals (AISP) was involved originally, however their participation dropped off due to the above focus (POLSEC, 7 March 2006, personal communication). That no participant in this research identified POLSEC highlights the fragmented nature of the
security industry and police initiatives for partnership. Late identification of POLSEC precluded closer examination of this initiative and it is yet to be evaluated formally (POLSEC, 7 March 2006, personal communication); however the POLSEC framework is considered here for partnership policing of e-crime.

**Ethics clearances**

Obtaining ethics clearance and authority to conduct this research was of particular importance, given ongoing controversies about the Victoria Police Law Enforcement Assistance Program (LEAP) outlined in Chapter Two. The research undertaken in this thesis study was vetted and approved by the Department Human Ethics Advisory Group (DHEAG) of the Department of Criminology and the central Human Research Ethics Committee (HREC No. 020601) of the University of Melbourne. The Research Coordinating Committee of Victoria Police (RCC No. 380) and the Department of Justice Research Ethics Committee (EC/04/14) also approved it (see Appendix E: *Letters of ethics clearance*). The Chief Commissioner of Victoria Police, Christine Nixon, endorsed the research as beneficial to Victoria Police (see Appendix F: *Letter of support from Victoria Police*). The Victorian Department of Justice is committed to “evidence-based strategic planning” (Ward, T. 2003) and with Multimedia Victoria provided a scholarship to undertake the research.\(^59\) The

\(^{59}\) Where their research is governed by a third party contract, such as the contract between the University, Justice and MMV for the studentship, PhD candidates at the University of Melbourne are required usually to assign their intellectual property rights to the University. However, with the support of the sponsors, this researcher argued successfully against that requirement, as neither government department wanted intellectual property rights from the research, nor was this research undertaken in the context of a pre-existing study at the University involving other researchers (as is often the case in medicine or other sciences).
chosen methods complement research undertaken by the Australian Centre for Policing Research\(^\text{60}\) (NPRU, 1998). Participation of federal agents and seconded personnel to the Australian High Tech Crime Centre was authorised and arranged by the Director of the AHTCC. Access to the members was conditional on not interfering with their workload, and some interviews were halted while these matters were attended.

**Ethical issues and risk management procedures**

People who are the subject of Victoria Police incident files examined in this study were not participants in the research. Regardless, their privacy under the *Information Privacy Act 2000* (Vic) has been respected and protected. The *Information Privacy Act 2000* (Vic) provides exemptions for “research in the public interest”. Where it is impracticable for an organisation to contact persons to gain their consent, organisations can disclose sensitive personal information to researchers (Schedule 1, section 2(1)(c)).

In the process of receiving approval from Victoria Police, the researcher consulted Privacy Victoria in relation to this exemption. It was noted that the Victorian Privacy Commissioner does not have the power to make determinations of public interest, unlike his federal counterpart. It was recommended that Public Interest Determination No. 5, issued by the federal Privacy Commissioner in 1991, provided a useful guide to “research in the public interest” (Office of the Privacy Commissioner, 1991). That determination was in relation to the Australian Federal Police disclosing information to researchers from the Australian Institute of Criminology for homicide research. It was advised that the conditions imposed in that determination would be good practice for this research (Director, Policy &

\(^\text{60}\) Formerly the National Police Research Unit.
Compliance, Privacy Victoria, 1 March, 2004, personal communication). Public Interest Determination No. 8 is another example permitting similar research into the nature and extent of serious fraud (Office of the Privacy Commissioner, 2002). That determination notes that de-identification of records “would be unreasonably resource intensive and would likely impede the objects of the research” (Office of the Privacy Commissioner, 2002). Based on this advice, the following conditions of access applied to this research:

1) That the information disclosed only be used for the purposes of the research.
2) That the information disclosed only relate to witnesses, suspects and offenders.
3) That the names of witnesses, suspects and offenders not be recorded by the researcher.
4) That access to relevant information be provided on Victoria Police premises, under Victoria Police supervision.
5) That the researcher responsible for inspecting the information held by Victoria Police be authorised personally to undertake the research by the University of Melbourne.
6) That the results of the case analyses be published in aggregate form to prevent the identification of individuals or individual cases.

Further, police members are restricted in what they can comment upon to the public. Section 127A(1) of the Police Regulation Act 1958 (Vic) states:

Any member of the police force who publishes or communicates, except to some person to whom he is authorised to publish or communicate it, any fact or document which comes to his knowledge or into his possession by virtue of this office and which it is his duty not to disclose shall be guilty of an offence against this Act.
Section 95 of the *Constitution Act 1975* (Vic) provides that officers in the public service must not:

a. publicly comment upon the administration of any department of the State of Victoria.

b. use except in or for the discharge of his official duties, any information gained by or conveyed to him through connection with the public service; or

c. directly or indirectly use or attempt to use any influence with respect to the remuneration or position of himself or of any person in the public service.

The Research Coordinating Committee approved the semi-structured interview schedule and police interviewees were apprised of these restrictions at the commencement of their interviews.

It was considered that Victoria Police personnel may have believed that this research was an evaluation of their job performance. However, that was not the intent of the research. Prospective participants were informed in the letters of invitation and at the beginning of interviews that participation or otherwise in the study would have no affect upon their employment (see letters in *Appendices H* and *I*). Participants were given the opportunity to ask questions about the research, prior, during and after their interviews. All participants had the option to withdraw any unanalysed data, through provision of a unique participant code number, which could be quoted to the researchers or ethics committees; however none did (see consent forms in *Appendices J* and *K*). The records and data relating to this study have been stored in the Department of Criminology at the University of Melbourne in compliance with the university’s Ethics Storage Policy and Procedures.
Online, pilot survey

For the pilot survey, an online, self-administered questionnaire was created by writing a semi-generic script in the PERL programming language for authoring and presenting online surveys. The online survey was part of the research study website hosted by the Department of Criminology (http://www.criminology.unimelb.edu.au/research/ecrime/). The survey permitted encrypted transmission of survey responses using a secure socket layer and digital certificate. A paper-based version of the survey was also produced, which included provision of reply paid envelopes for return of completed surveys.

Two questionnaire items were constructed to compare public and police perceptions of the priorities given by police to different types of electronic crime, based on the format of a survey conducted by the National Police Research Unit (Boni and Packer, 1998). According to Boni and Packer (1998), little research has involved comparing the public and police views of the role of police. The NPRU study examined perceptions of police roles and focused on perceptions about current priority and what priorities ought to be.

To improve the comparability of results from this study, demographic items from Boni and Packer’s (1998) survey were used in the questionnaire. Industry sectors are classified according to the Australian and New Zealand Standard Industrial Classification (ANZSIC) (ABS, 1993). Although the Australian Standard Offences Classification (ASOC) is based primarily upon the behavioural and victim characteristics of offences (ABS, 1997), and e-crime is also defined by behavioural characteristics, the ASOC does not include any category of “computer-related offences” or e-crime offences. Consequently, it was not of use for the creation of offence related items. These items were based on Grabosky and Smith’s (1998; 2003) taxonomies of digital
crime (see Table 2.1), using terminology considered to be familiar to respondents based on its media usage. These items were pre-tested by a senior member of Victoria Police for appropriateness to the concept of “e-crime” and for how understandable they were. The full questionnaire is available in Appendix G: Private sector survey.

The survey was advertised on the Department of Criminology homepage. With assistance of Multimedia Victoria, the survey was advertised on several prominent government websites, including Business in Victoria and the Business Channel (www.business.vic.gov.au). The information was replicated by several local organisations. The research was also advertised through the Victorian Information Technology Teachers Association (VITTA) magazine Infonet in the form of an article discussing electronic crime in the digital classroom (McKenzie, 2004).

The Australian Communications Authority (ACA) confirmed that inviting people to participate in the survey via email would not breach the newly introduced Spam Act 2004 (Cth) (ACA, 29 June 2005, personal communication). Thirty-four Internet Service Providers providing services in Victoria, selected randomly from a local telephone directory listing, were invited via email to complete the survey or be interviewed. Only one Internet Service Provider responded and answered questions via email. The lack of response from Internet Service Providers in general provides further context to this thesis (see generally, Sutton R.I., 1989). The survey was also advertised on the LINK mailing list, a forum that discusses the impact of technology.

61 The benefit of this became dubious later, when some online survey responses had to be culled as ‘non-responsive’, because students had submitted nonsensical answers, perhaps as part of a classroom exercise.
Analysis of closed incident records

To explore the nature of electronic crime incidents in Victoria and success factors in e-crime investigation, official Victoria Police LEAP records for closed electronic crimes cases were analysed. The data collection took place at the offices of the State Intelligence Service and the Major Fraud Investigation Division of Victoria Police. The Victoria Police Pilot Intelligence Database downloads data from LEAP and is part of the Intelligence Framework Project at the State Intelligence Service. It was use of this subsidiary database that permitted keyword and Boolean logic searching of LEAP incident records using Structured Query Language (SQL) queries to identify and extract electronic crime incidents.

Sample LEAP data for this study relates to cleared incidents reported to Victoria Police during the five financial years of 1 July 1999 through 30 June 2004. Cleared cases were those flagged as other than “unsolved”, including “offender processed”, “no offence disclosed”, “complaint withdrawn” and “other”. Incidents that have not been resolved remain “unsolved” and active investigations, at least officially, and so were not available for examination in this study. To account for this limitation, unsuccessful investigations were discussed specifically with interviewees.

“E-crime” is not one of the 27 offence categories used by Victoria Police (see generally, Victoria Police, 2005c). Incidents were identified on the basis of characteristics in the definition of “e-crime”. An incident needed to involve some digital technology as either the tool in the commission of an offence, the target of an offence or the storage medium for illicit data or information. As an

62 While the raw data was physically secure in, and never left the MFID premises, PGP 128 bit encryption was used to further secure it to prevent unauthorised police access.
example, incidents classified as e-crime for the offence “Possess Unclassified Computer Game to Sell” related to digital piracy and illegal data storage and not the fact of the unclassified item was a computer game. Cases were excluded if the involvement of the technology was only as ‘bait’ in a fraud, such as offering to sell a computer to a person, and this transaction did not take place via an ICT, such as email or an Internet auction website. Some cases were included which interviewees have argued are not electronic crime. For example, incidents involving use of a computer and printer to print forged cheques were included, when investigators often exclude cheque fraud. Similarly, simple theft of computers was excluded, yet perhaps should have been included, because police argued that they often needed to conduct digital evidence analysis in these cases to determine ownership.

An initial pilot sample of e-crime incidents was examined to develop a coding sheet for incident characteristics. Subsequent incidents were coded by completing entries in an SPSS database file. The database file includes only de-identified information about the incidents. The LEAP data was then sampled in three stages. First, to identify as many e-crime incidents as possible. Secondly, a stratified, random sample amounting to 10% of the initial sample was coded. This sample was stratified proportionally according to the LEAP Offence code. Incidents which had extremely short narratives recorded in LEAP (such as those which were only three lines long) were discarded from the random sample and replaced with incidents that provided more of the required information. Third, all closed incidents of “pure” e-crime offences within the timeframe were coded separately. This last sample was coded, because it is these types of offences that are most often considered “computer crime” by the lay person, and as such merit special attention in comparison to the wider category of e-crimes.
Like all empirical research, this inquiry had practical limitations and imperfections. The original research design called for examination of court records relating to the closed e-crime incidents that had proceeded to court. However, it became apparent upon access to the LEAP data that this was not feasible. To access court outcomes via the Court Services section of the Victorian Department of Justice, the unique brief identifier or “BriefID” was required and arrangements were made to do so. However, it was found that Victoria Police does not record BriefIDs centrally or systematically in LEAP. BriefIDs were only available for a total of 6 incidents identified as e-crime by this study, where they were noted in incident narratives by investigating members. Further, to access court outcomes in records held by the Office of Public Prosecutions would require recording identifying details, contrary to the conditions of access required by Victoria Police and so was not pursued.

Following the extraction of the study data, the media raised concerns related to the accuracy of some data in the LEAP database. The claims, based on a leaked email to Central Data Entry Bureau (CDEB) staff, were that police had asked CDEB to manipulate entries to artificially reduce crime rates by downgrading multiple sub-incidents to single incidents (Hughes and Shiel, 13 December 2004). This study avoids concerns relating to this claim by analysing the LEAP data on the basis of incidents, instead of sub-incidents.

LEAP incident narratives provided a rich source of qualitative data about the types of incidents reported to Victoria Police. Other LEAP fields provided quantitative data about these incidents. Unfortunately, incident narratives do not follow any consistent pattern. Some include lots of details about the incident and investigation, while others record almost no detail. The Computer Crime Squad provided data from its Jobs Database to more accurately reflect its involvement in e-crime investigations. Also, the LEAP
data exhibited numerous and serious deficiencies in terms of accurate data entry, which required time-consuming verification and cleaning where possible to permit data analysis. Examples included inaccurate application of LEAP Offence codes, mismatches of LEAP Offence Group to the LEAP Offence Code, nonsensical date entries for when incidents were committed and for both offenders’ and victims’ dates of birth, and entries stating the date reported to police that were well after the dates offenders were described as having been processed in the incident narratives. As an example, incidents of stalking, charged under section 21A of the *Crimes Act* (Vic), which has the LEAP Offence Code of 199AB, were listed variously as belonging to the categories of Deception (n=51), Harassment (n=58), Sex (Non Rape) (n=9) and Other (n=1), when only the Harassment category is correct.\(^63\)

In December 2004, the new Police Integrity Ombudsman announced an inquiry into systemic abuses of the LEAP system (The Age, 7 December 2004). His March 2005 report recommended replacement of LEAP and introduction of a specific regulatory offence for unauthorised access to police information (OPI, March 2005).

**Interviews with investigators and victims**

Private investigators were not sampled via a regulatory agency, as was the method in Prenzler and King (2002), because the researcher was informed that Victoria Police did not distinguish e-crime investigators in their records and accessing contact details would be onerous (Licensing Services Branch, Victoria Police, 5 May 2003, personal communication). The study website

\(^63\) The Victoria Police Crime Statistics 2002/03 also exhibited this problem for at least one offence: 321B Obtain Property by Deception was listed in both the Deception and Handle Stolen Goods categories.
provided information about the research to prospective interviewees. Flyers advertising the research were distributed to delegates of the 2004 International Association of Financial Crime Investigators (IAFCI) conference held at Melbourne University Private. A brief presentation was also given to the Australian Institute of Professional Investigators (AIPI) outlining the aims of the research and asking for interview participants and AIPI sent emails to the members of the Victorian Chapter.

Invitations to be interviewed confidentially were distributed to all members of the squads of the Major Fraud Investigation Division, including the Computer Crime Squad. Individual members indicated their willingness to participate in an interview by returning a slip by reply paid post, whereupon the researcher contacted them to arrange confidential interviews.

With assistance from the University of Melbourne Media Liaison Unit,64 a media release was distributed, advertising the research to the public. The media release generated considerable interest from the local media and resulted in two radio interviews to further advertise the research: on the local 774 ABC Melbourne radio Breakfast program with Red Symons and ABC News Radio. An interview was also conducted for an article in the local broadsheet newspaper, The Age (Turner, 14 September 2004). Several telephone calls were also fielded from individuals requesting to participate in the research, having been victims of e-crime.

Semi-structured standardised interviews were conducted as this aids with focus and comparative analysis (Patton, 2002: 344-347; see Appendices L and

64 The University of Melbourne Media Liaison Unit provides assistance in contacting the media about research. They helped draft and disseminate a media release announcing the online survey.
Nevertheless, interviewees were free to discuss other issues of interest to them, within the legal and ethical constraints discussed above. This style of interview also permitted triangulation of views, whilst maintaining confidentiality by raising information and points of view provided by other interviewees and seeking comment. Handouts detailing a definition of e-crime, suggested partnership activities and the new model computer offences were provided to interviewees at various points in the interview to stimulate their responses (see Appendix N: Handouts used during police & private sector interviews). Interviewees were also asked to comment on Sarre and Prenzler’s (2000) descriptive and normative models of police-private security interaction.

Interviews lasted between an hour and two hours, resulting in approximately a thousand pages of transcript. Once a transcript was completed and checked for accuracy, the original recording was destroyed. It is common knowledge among those with forensic knowledge of computers that Windows operating systems do not really delete files when they are deleted from the Recycle bin (Casey, 2004: 205). What happens instead is that the pointer to the file in the file allocation table (think of this as the card catalogue in a library) is deleted. The actual file remains where it was originally stored until it is overwritten by the data from a subsequent file. To account for this, PGP Wipe was used to destroy interview audio recordings securely after transcription as this overwrites the data and removes any traces of the file (PGP, 2001: 110). PGP Wipe was set for 32 passes to prevent any recovery using forensic tools and protect the confidentiality of participants. This exceeded the latest standards required by the Australia Defence Signals Directorate (DSD) for sanitisation of magnetic media classified as “In-Confidence” in the Australian Government.

---

65 Similarly, formatting a hard disk drive (except low level formatting) does not make data unrecoverable (Casey, 2004: 203).
Due to the sensitive nature of the topics under discussion, it was not always possible to negotiate ideal interview situations, nor always ask the most probing questions (see Marx, 1988: xxiii). Interviews with lower ranking officers at Victoria Police became infeasible. Approval was secured for invitations to be sent directly to individual officers identified from the closed case analyses as having worked e-crime cases at local CIUs or other squads. It was expected these officers would be located all across Victoria. LEAP records in general do not contain the name of investigating officers, instead identifying them by their badge number and unit. These would provide a contact list for interviews invitations. The Victoria Police Research Coordinating Committee indicated they would identify the officers from the list of badge numbers and arrange permission from local senior officers for these members to take part in interviews, whereupon they could be invited to participate by letter.

However, a subsequent conversation with a junior police member indicated a heightened level of concern about confidentiality, because of the requirement for seeking individual permission and thus providing to the Victoria Police chain of command a means of identifying interviewees. Subsequently, and due to the lengthy process obtaining the original approvals, these additional interviews were dropped from the research design. It would be beneficial to research the lived experiences of investigating e-crime and partnership policing at the local station and CIU level, however to do so requires a method of recruitment more sensitive to member needs.

At the AHTCC, the six interviewees were ‘chosen’ for the researcher and there is the possibility this was done to present “the right perspective”
(Haines, 1995: 71). On two occasions, interviewees refused audio recording, ostensibly lest it identify them or their employer. However, on both occasions, it was almost as if this was done to test the mettle of the researcher. Despite these restrictions the interviews permitted an insider or “emic” view of their organisations, their responses to e-crime and the reasoning guiding those responses.

It became very clear in the course of this study that there is a reasonably small circle of professionals within police and in the Victorian community, who know and interact with each other on a semi-regular basis. This has required additional disguising of some interviewees and incidents that were discussed to prevent inadvertent recognition of interviewees by readers of this thesis.

In all, 37 interviews were conducted with 41 people, at which point it became clear that the point of saturation had been reached (Eisenhardt, 2002: 7).

**Dissemination of the research findings**

A summary of the findings of this study was published on the research website, <http://www.criminology.unimelb.edu.au/research/e-crime/>, available for access by the research participants, stakeholders and the public.

The following three chapters report in full the findings of this exploratory research.
Results

Chapter 5: The nature of reported e-crime and police e-crime investigations in Victoria

Much of what has been learned so far about the nature of electronic crime originated from anecdotal and media reports of individual incidents, judicial proceedings (see for example, Grabosky and Smith, 1998) or victim surveys such as the AusCERT Computer Crime and Security survey. Little has come from official crime statistics. Police in Australia do not report statistics on electronic crime. It is not one of the standard categories of crime, such as homicide or deception. As discussed in Chapter Two, to describe an incident as ‘electronic crime’ relates more to describing the means of committing an offence rather than the offence itself. The involvement of information technology in the commission of an offence will often be more important in terms of how the incident is investigated.

Given this paucity in official crime statistics, what is the nature of electronic crime that is reported to and investigated routinely by police? How successful are the police in their investigations of e-crime, and does success rely upon partnership with the private sectors?

This chapter presents the results of an analysis of e-crime incidents to illustrate the nature of reported e-crime in Victoria. The chapter describes characteristics of the incidents and the investigations undertaken by Victoria Police as derived from incident data and their narratives. Commentary from interview participants provides additional insight on the nature of e-crime that they encounter in Victoria. But first, the chapter reports the demographics of the respondents participating in the study and the samples of e-crime incidents extracted from the LEAP database.
Respondent demographics

Table 5.1 displays the breakdown between law enforcement personnel and other members of the community who took part in this study. Table 5.2 shows the means by which respondents took part. Most private sector respondents participated in the survey only, although some were also interviewed to expand on their survey responses. Most private sector investigators were interviewed. All law enforcement personnel were interviewed.

Table 5.1: Respondents by sector

<table>
<thead>
<tr>
<th>Sector</th>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Police</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MFID</td>
<td>8</td>
<td>11.9</td>
</tr>
<tr>
<td>CCS</td>
<td>6</td>
<td>9.0</td>
</tr>
<tr>
<td>AHTCC</td>
<td>6</td>
<td>9.0</td>
</tr>
<tr>
<td>Other Govt Investigator</td>
<td>1</td>
<td>1.5</td>
</tr>
<tr>
<td><strong>Sub-total</strong></td>
<td>21</td>
<td>31.3</td>
</tr>
<tr>
<td><strong>Private Sectors</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Investigators</td>
<td>14</td>
<td>20.9</td>
</tr>
<tr>
<td>Managers</td>
<td>10</td>
<td>14.9</td>
</tr>
<tr>
<td>IT Admin</td>
<td>10</td>
<td>14.9</td>
</tr>
<tr>
<td>Other</td>
<td>12</td>
<td>17.9</td>
</tr>
<tr>
<td><strong>Sub-total</strong></td>
<td>46</td>
<td>68.7</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>67</td>
<td>100.0</td>
</tr>
</tbody>
</table>


* Respondents classified as ‘9631 Police services’ in the ANZSIC (ABS, 1993).

Each of the law enforcement officers interviewed represents an expert public policing practitioner. Their views expressed in this study do not necessarily represent the policy of the Australian or state governments or their employing agencies.
Table 5.2: Respondents by methods of participation

<table>
<thead>
<tr>
<th>Response Method</th>
<th>Survey</th>
<th>Interview</th>
<th>Both</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Police</td>
<td>MFID</td>
<td>0</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td></td>
<td>CCS</td>
<td>0</td>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>AHTCC</td>
<td>0</td>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td>Other Govt</td>
<td>Investigator</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Sub-totals</td>
<td>0 (0%)</td>
<td>21 (100%)</td>
<td>0 (0%)</td>
<td>21 (31.3%)</td>
</tr>
<tr>
<td>Private Sectors</td>
<td>Investigators</td>
<td>2</td>
<td>11</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Managers</td>
<td>8</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>IT Admin</td>
<td>7</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Other</td>
<td>9</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>Subtotals</td>
<td>26 (56.5%)</td>
<td>15 (32.6%)</td>
<td>5 (10.9%)</td>
<td>46 (68.7%)</td>
</tr>
<tr>
<td>Totals</td>
<td>26 (38.8%)</td>
<td>36 (53.7%)</td>
<td>5 (7.5%)</td>
<td>67 (100%)</td>
</tr>
</tbody>
</table>


The majority of respondents were aged between 35 and 44 years (Figure 5.1). Most respondents were male (n= 53; 79.1%). Twelve women took part in the study, making up the other 17.9% of the sample (see Table 5.3).

Figure 5.1: Age of respondents

![Age Distribution](image)


Only two women in this sample held investigator roles, one in law enforcement and one with a transnational corporation. Two survey respondents recorded neither their age nor sex.
Table 5.3: Sex of respondents

<table>
<thead>
<tr>
<th>Response Method</th>
<th>Male</th>
<th>Female</th>
<th>Missing</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Survey</td>
<td>17</td>
<td>7</td>
<td>2</td>
<td>26</td>
</tr>
<tr>
<td>Interview</td>
<td>31</td>
<td>5</td>
<td>0</td>
<td>36</td>
</tr>
<tr>
<td>Both</td>
<td>5</td>
<td>0</td>
<td>0</td>
<td>5</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>53 (79.1%)</td>
<td>12 (17.9%)</td>
<td>2 (3%)</td>
<td>67 (100%)</td>
</tr>
</tbody>
</table>


All fourteen Victoria Police respondents were sworn detectives. Nine of the Victoria Police respondents also held the rank of senior constable (64.3%). Five were ranked Sergeant or above (35.7%). The average length of service with Victoria Police by these police respondents was 17 years. On average they had been in their present positions for four years.

The Australian High Tech Crime Centre does not use ranks. Five AHTCC respondents were sworn members of law enforcement agencies. Two of these were on secondment from state police forces. The sixth AHTCC respondent was an unsworn member on secondment from a major Australian bank as part of the Joint Banking and Finance Sector Investigation Team. As the AHTCC had only been in existence for 18 months at the time of those interviews, the average tenure of those interviewees in their present positions was one year. However, on average, these participants had sixteen years experience in state or federal police forces.

Of the private sector respondents, ten reported serving previously in a law enforcement agency. All but two of these people reported having served with Victoria Police, the others having served with government regulators. Seven were now working as investigators, two were in management positions and one held an IT administration position, which entailed investigation of

---

66 Includes two acting Sergeants and one Inspector.

67 Excludes the bank investigator seconded to the Joint Banking and Finance Sector Investigation team as an unsworn member.
incidents. Although these private sector investigators worked in various industry sectors, it would be fair to characterise that most focused upon the investigation and prevention of fraud-related offences. Some by virtue of working for educational institutions include a focus upon child Internet safety. Respondents represented each of Gill and Hart’s (1997b: 138-139) typologies of private investigator, from ‘home-based’ to ‘prestige’.

Table 5.4: Highest level of education attained by respondents

<table>
<thead>
<tr>
<th></th>
<th>Private Sector</th>
<th>Law Enforcement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Degree+</td>
<td>26 (56.5%)</td>
<td>9</td>
</tr>
<tr>
<td>Diploma / Trade certificate or equivalent</td>
<td>8 (17.4%)</td>
<td>2</td>
</tr>
<tr>
<td>Completed Year 12</td>
<td>3 (6.5%)</td>
<td>3</td>
</tr>
<tr>
<td>Some high school</td>
<td>4 (8.7%)</td>
<td>0</td>
</tr>
<tr>
<td>No response</td>
<td>5 (10.9%)</td>
<td>7</td>
</tr>
<tr>
<td>Totals</td>
<td>46 (100%)</td>
<td>21 (100%)</td>
</tr>
</tbody>
</table>


Table 5.4 shows that the majority of private sector respondents had attained a university degree or higher. Police respondents were not asked specifically their highest level of education. They were asked if they had received any specialist training for the investigation of e-crime. Police members reported training such as Certificate IV in IT, and the Graduate Certificate in E-Crime Investigation. Three reported having no formal qualifications relating to e-crime investigation beyond standard detective training.

Of the private sector investigators, some had undertaken a modified version of the Victoria Police Detective Training School course. That course is no longer offered outside Victoria Police. Others had diplomas in fraud prevention or investigation or had undertaken a Certified Fraud Investigator’s Course or the Graduate Certificate in E-Crime Investigation.

The researcher also spoke with several people over the telephone, who called in response to the interviews on local radio. One man and two women who
contacted the researcher were interviewed in person. Their comments about their experiences as victims of e-crime are interspersed through the results chapters to highlight issues of police and private sector responses to e-crime. One recounted a theft from an Internet banking account and another a theft from an ATM. The third was a case of identity theft and cyber-stalking, involving a hijacked email account. To differing degrees in each incident, the respondents reported having difficulty getting positive investigative responses.

**Data sample demographics**

Sample LEAP data for this study relates to incidents reported to Victoria Police during the five financial years of 1 July 1999 through 30 June 2004.\(^{68}\) Victoria Police generates its statistics based on the financial calendar year, and so this thesis also uses the financial calendar year to permit comparison (Victoria Police, 2002b). From 7369 separate offences under Victorian and Commonwealth legislation listed in LEAP at the time, 573 offences representing 27616 closed incidents were identified initially as potential sources of electronic crime incidents.

Following the process described in Chapter Four, 3529 incidents were identified as e-crime.\(^{69}\) This reduced to 70 the number of offences for which e-crime incidents were included (see Table App O.1 in *Appendix O: LEAP sample demographics*). Keyword searching and manual verification identified 1738

---

\(^{68}\) Incident data is reported in aggregate form only as a condition of access and ethics. As this analysis is concerned mainly with investigation of e-crime, the sample was not restricted to offences committed between the 1999-2003 fiscal years and includes historical offences, reported to Victoria Police between 1 July 1999 and 30 June 2004.

\(^{69}\) An additional fourteen cases, which would have been classified as e-crime due to Modus Operandi entries, were excluded due to missing narratives.
incidents (49.3%) as electronic crime. To be classified as an e-crime incident the incident had to conform to the definition of e-crime provided in Chapter Two. Another 1793 incidents (50.7%) across four offences were included in the overall sample as electronic crime incidents on the basis of their Modus Operandi entries or the nature of the offence, although time constraints prevented manual verification of each of these incidents. Of these, 965 incidents of Obtain Property by Deception and 163 incidents of Obtain Financial Advantage by Deception were included, because the Modus Operandi recorded by police for these incidents was either “ATM / EFTPOS INVOLVED” or “CREDIT CARD INVOLVED”. Axiomatically, all closed incidents for the offences “Use Telecommunications Service to Menace” and “Use Telecommunication Service to Harass” were classified as e-crime.

Some offences included in Table App O.1 might not appear relevant to the definition of e-crime. However, for example, incidents included in the sample where a defendant was charged with “Sexual Penetration of a Child Under 16” involved using chat rooms or showing pornographic videos to groom the child victims (see A Stranger in Our Home, 2000). Equally, some offences, for which it might be assumed that all such incidents would be classified as e-crime, were not in fact all e-crime. As an example, the illegal use of binoculars as a “surveillance device” was not counted as e-crime.

The second sample, a stratified, random sample consisted of approximately 10% (n=365 incidents) from the full sample of 3529 e-crime incidents. Proportional strata for this sample were calculated based on the number of incidents identified and with a minimum of one incident coded per type of offence as reported in Appendix O: LEAP sample demographics.

The third sample contains all the incidents for offences that can be considered “new” or “pure” e-crime (see Table App O.2). These are the offences that
could not be committed without the involvement of information technology, such as a computer, or did not exist in another form prior to the information technology in question (see pg. 18). Included in this sample were the original Victorian computer crime offences under section 9A of the *Summary Offences Act 1966* (Vic). Also included were their replacement offences introduced to the *Crimes Act 1958* (Vic) by the *Crimes (Property Damage and Computer Offences) Act 2003* (Vic). Commonwealth offences relating to telecommunications offences, which appeared in the LEAP offence code list, were included in this sample framework. However, very few incidents for these offences were located (N=43).

The raw LEAP data included some errors relating to offences charged. As an example, three incidents had 137H listed, which relates to section 50(1) of the *Crimes Act 1958* (Vic) for the offence “Gross Indecency with a child under 16 years”. However this offence was repealed on 5 August 1991 by section 3 of the *Crimes (Sexual Offences) Act 1991* (Vic) at least eight years prior to the incidents for which it was entered. It would appear that some codes for repealed legislation have not been removed correctly from the system and are still used by members. Where this was the case, these offence codes have been ignored in this analysis. Three incidents relating to the new computer offences were recorded in LEAP under incorrect offence codes due to a lack, at the time, of an appropriate LEAP Code; however the narrative noted the actual charge.\(^\text{70}\)

\[^{70}\text{Two were coded as the federal offence 321MQ (Unauth interfere with computer) and another as 321K (False statement-destroy/Damage property). Miscoding as 321K is understandable, as the statutory reference “s.247B” could be confused easily with “s.247(b)”, especially when written as “247B” and “247.B” respectively in LEAP. See generally, Carcach and Makkai (2002) for an error audit study of LEAP conducted by the AIC.}\]
E-crime incident and investigation characteristics

Incidence and classification of incidents

From July 1999 through June 2002 there was a steady increase in the number of e-crime incidents reported to Victoria Police, peaking at 1092 incidents in the 2001/02 financial year. From July 2002, the number falls significantly.

In LEAP, incidents are classified by the offences charged, which fall into 27 offences groups. The e-crime incidents identified in the main sample belonged to only five of the 27 offence categories used by Victoria Police. These were Deception, Harassment, Other, Regulated Public Order and Sex (Non Rape). Table App O.3 of Appendix O displays the breakdown of the incidents by offence and offence category over the five-year sample period. As seen in Table 5.5 most e-crime involved deception or harassment offences.

Table 5.5: E-crime incidents by offence group

<table>
<thead>
<tr>
<th>Offence Group</th>
<th>Corrected Frequency*</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deception</td>
<td>2293</td>
<td>58.0%</td>
</tr>
<tr>
<td>Harassment</td>
<td>988</td>
<td>25.0%</td>
</tr>
<tr>
<td>Regulated public order</td>
<td>327</td>
<td>8.3%</td>
</tr>
<tr>
<td>Other</td>
<td>281</td>
<td>7.1%</td>
</tr>
<tr>
<td>Sex (non rape)</td>
<td>66</td>
<td>1.7%</td>
</tr>
<tr>
<td>Total</td>
<td>3955†</td>
<td>100%</td>
</tr>
</tbody>
</table>

* 399 incidents across 16 offences that had incorrect Offence Group codes assigned in LEAP were corrected based on groupings in Appendix A of Victoria Police Crime Statistics, 1999/00-2003/04.
† Total exceeds number of incidents (N=3529), as 19.2% of incidents involved multiple offences.

The maximum number of different offences charged against a single offender for any incident was seven, in a case of an offender procuring a child to create

---

71 Offence grouping required correction in 399 incidents across 16 offences, for example where deception offences had been coded as Sex (Non Rape).
child pornography using his computer. The mean and mode of different offences charged per incident were both one, accounting for 80.8% of the sample. Only one in five incidents had more than a single offence type recorded for an incident.

As the incidents sampled in this study only include cleared incidents, they can only be compared accurately against official statistics for cleared incidents, not against totals of recorded crime. Table 5.6 provides a comparison of the number of cleared e-crime incidents identified in this study with the overall number of incidents cleared by Victoria Police in these categories. Taken in the context of the overall number of incidents cleared each year by Victoria Police, it is apparent that e-crime incidents are but a very small portion of the crime with which this state police force deals. This table also reveals that, although there were more e-crime incidents involving deception, there was a higher proportion of e-crime incidents in the category of harassment—consistently above 8%—than in any other category. In 2003/04, e-crime clearances in the harassment category fell to a proportional level (2%).

On average two sub-incidents were recorded by police for each e-crime incident in the main sample (n=3529; \( \bar{X}=2.03, \sigma=4.79 \)). The maximum number of sub-incidents was 118. The same incident had the maximum number of charges laid for an incident, which was 742.\(^{72}\) The average number of charges

\(^{72}\) This figure was not entered into the LEAP database in the Offence Counts field, which recorded only 2 counts for this incident. The figure was stated in an incident narrative, which detailed a complex fraud involving multiple offenders committed against multiple financial institutions. The maximum number of Offence Counts recorded in the numerical data was 521.
laid per incident based on the numerical data was 2.89, with a standard deviation of 14.05.

As shown in Table App O.1, Obtain Property by Deception (OPBD) was charged more often than any other offence for incidents identified as e-crime (n=1634, 50.1%). In some cases the offences charged are broad, such as OPBD or Obtain Financial Advantage by Deception (OFABD), and were charged for many different types of illegal activity. To gain a greater appreciation of the actual types of e-crime that Victoria Police have reported to them, the stratified sample incidents were classified further to describe the particular e-crime incident by the activities involved, such as “online auction fraud” and “phishing scam”. These have been further grouped according to Grabosky and Smith’s (2003) typology. Activities that would be categorised by Grabosky and Smith (1998; 2003) as “Telecommunications in furtherance of Criminal Conspiracies” were not present in any of the sampled incidents in this study. The purpose of Tables 5.7 to 5.12 is to illustrate more fully the incidents recorded in LEAP and not to suggest a new classification scheme.

In the Deception category, a quarter of e-crime reported to police involved credit card fraud. The next most common activity was false accounting by issuing false refunds for non-existent returned goods or modifying computer records (see Table 5.7). A private investigator described such an incident committed that was investigated successfully and passed to police:

What she did was to get on to the online banking system, and she realised that whatever she put in to the online banking system would come back in the bank statements as being the destination of the money. This is what a lot of people don’t realise. The principals of the business were saying “Okay, I can see our account statements here, and I see we’ve paid Telstra, and I see we’ve paid Australia Post, and I see we’ve paid insurance company, couriers,
whatever it might be.” Naturally, if that name is there, the account number that goes next to it must match that name, because we assume that the banking system has this thing where it matches account numbers, not realising that the information that’s recorded there is just the garbage that’s been keyed in by the client. And so they think they’re paying all these people and actually they’re paying her, because that’s her account. And she was able to whiz off $158,000 there (PS#4).

Computers were often used to forge medical prescriptions or create false documents used for identification purposes, such as utility bills. Theft of Internet services by accessing other people’s ISP accounts without authorisation was also quite common between 1999/00 and 2002/03. Online auction site fraud, where goods were not delivered after receipt of payment was common also. Denial of service attacks (DoS) were not common among cleared cases; nor were the two incidents classified as DoS particularly sophisticated, one involving simply turning off a computer to commit a fraud at an EFTPOS terminal. No incidents involved the authoring of computer viruses. Although only a single incident was identifiable as a phishing scam in this sample, phishing is the current, major concern in the financial services sector:

Those fake jobs sites are everywhere. We’ve got a guy in Perth who got a link from a friend in the US, who sent him it, said “you should apply for this, you might make some money”. I mean that’s everywhere. We would suspect that there is far more customer information being held than there are enough mules to actually take the money out (Private sector investigator, PS#11).
Table 5.6: Comparative distribution of e-crime incidents to total cleared incidents by offence group and year*

<table>
<thead>
<tr>
<th>Offence Group</th>
<th>Cleared in 1999/00</th>
<th></th>
<th>Cleared in 2000/01</th>
<th></th>
<th>Cleared in 2001/02</th>
<th></th>
<th>Cleared in 2002/03</th>
<th></th>
<th>Cleared in 2003/04</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>E-crime</td>
<td>Total</td>
<td>E-crime</td>
<td>Total</td>
<td>E-crime</td>
<td>Total</td>
<td>E-crime</td>
<td>Total</td>
<td>E-crime</td>
<td>Total</td>
</tr>
<tr>
<td>Deception</td>
<td>170</td>
<td>31347</td>
<td>394</td>
<td>24739</td>
<td>651</td>
<td>23954</td>
<td>568</td>
<td>23845</td>
<td>510</td>
<td>25086</td>
</tr>
<tr>
<td>(52.8%)†</td>
<td>(70.1%)†</td>
<td>(52.8%)†</td>
<td>(66.1%)</td>
<td>(62.5%)</td>
<td>(60.0%)</td>
<td>(60.6%)</td>
<td>(70.1%)</td>
<td>(64.6%)</td>
<td>(516%)</td>
<td>(46.6%)</td>
</tr>
<tr>
<td></td>
<td>(0.5%)‡</td>
<td>(0.5%)‡</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Harassment</td>
<td>110</td>
<td>1384</td>
<td>338</td>
<td>1288</td>
<td>280</td>
<td>1815</td>
<td>223</td>
<td>1572</td>
<td>37</td>
<td>1855</td>
</tr>
<tr>
<td>(34.2%)</td>
<td>(31%)</td>
<td>(3.1%)</td>
<td>(39.4%)</td>
<td>(3.4%)</td>
<td>(25.4%)</td>
<td>(4.7%)</td>
<td>(23.6%)</td>
<td>(4.0%)</td>
<td>(5.1%)</td>
<td>(4.8%)</td>
</tr>
<tr>
<td></td>
<td>(8%)</td>
<td>(26.2%)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td>23</td>
<td>5294</td>
<td>79</td>
<td>5117</td>
<td>71</td>
<td>6285</td>
<td>57</td>
<td>7676</td>
<td>51</td>
<td>5487</td>
</tr>
<tr>
<td>(7.1%)</td>
<td>(11.8%)</td>
<td>(9.2%)</td>
<td>(13.7%)</td>
<td>(6.5%)</td>
<td>(16.4%)</td>
<td>(6.0%)</td>
<td>(19.5%)</td>
<td>(7.0%)</td>
<td>(14.1%)</td>
<td>(14.1%)</td>
</tr>
<tr>
<td></td>
<td>(0.4%)</td>
<td>(1.5%)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Regulated Public Order</td>
<td>14</td>
<td>1898</td>
<td>38</td>
<td>1649</td>
<td>81</td>
<td>1858</td>
<td>79</td>
<td>2104</td>
<td>115</td>
<td>2052</td>
</tr>
<tr>
<td>(4.3%)</td>
<td>(4.2%)</td>
<td>(4.4%)</td>
<td>(4.4%)</td>
<td>(7.4%)</td>
<td>(4.9%)</td>
<td>(8.3%)</td>
<td>(5.4%)</td>
<td>(15.8%)</td>
<td>(5.3%)</td>
<td>(5.3%)</td>
</tr>
<tr>
<td></td>
<td>(0.7%)</td>
<td>(2.3%)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sex (Non rape)</td>
<td>5</td>
<td>4789</td>
<td>8</td>
<td>4624</td>
<td>18</td>
<td>4412</td>
<td>20</td>
<td>4151</td>
<td>15</td>
<td>4370</td>
</tr>
<tr>
<td>(1.6%)</td>
<td>(10.7%)</td>
<td>(1%)</td>
<td>(12.4%)</td>
<td>(1.6%)</td>
<td>(11.5%)</td>
<td>(2.1%)</td>
<td>(10.5%)</td>
<td>(2.0%)</td>
<td>(11.2%)</td>
<td>(11.2%)</td>
</tr>
<tr>
<td></td>
<td>(0.1%)</td>
<td>(0.2%)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sub-total</td>
<td>322</td>
<td>44712</td>
<td>857</td>
<td>37417</td>
<td>1101</td>
<td>38324</td>
<td>947</td>
<td>39348</td>
<td>728</td>
<td>38850</td>
</tr>
<tr>
<td>(100%)</td>
<td>(26.5%)§</td>
<td>(100%)</td>
<td>(23.0%)</td>
<td>(100%)</td>
<td>(22.9%)</td>
<td>(100%)</td>
<td>(23.0%)</td>
<td>(100%)</td>
<td>(22.6%)</td>
<td>(100%)</td>
</tr>
<tr>
<td>All Offence Groups</td>
<td>168501</td>
<td>162737</td>
<td>167424</td>
<td>171781</td>
<td>171764</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(100%)</td>
<td>(100%)</td>
<td>(100%)</td>
<td>(100%)</td>
<td>(100%)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>


* Total of sample incidents exceeds number of unique sample incidents (N=3259), as 19.2% involved more than one offence charged.
† Percentage of total e-crime cleared in the year (E-crime / Sub-total).
‡ E-crime cleared as a proportion of Total cleared for the offence category (E-crime / Total).
§ Percentage of total cleared incidents (Sub-total / All Offence Groups).
Table 5.7: Breakdown of deception incidents by e-crime activity

<table>
<thead>
<tr>
<th>Category/Description</th>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Electronic Funds Transfer Crime</strong>*</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Credit card fraud</td>
<td>43</td>
<td>17.9%</td>
</tr>
<tr>
<td>False accounting</td>
<td>30</td>
<td>12.5%</td>
</tr>
<tr>
<td>Credit card fraud against Internet merchant</td>
<td>25</td>
<td>10.4%</td>
</tr>
<tr>
<td>EFT fraud</td>
<td>20</td>
<td>8.3%</td>
</tr>
<tr>
<td>Internet Banking Fraud</td>
<td>12</td>
<td>5.0%</td>
</tr>
<tr>
<td>Use of Credit card skimmer</td>
<td>11</td>
<td>4.6%</td>
</tr>
<tr>
<td>Other electronic theft of funds</td>
<td>4</td>
<td>1.7%</td>
</tr>
<tr>
<td>Obtain Credit card numbers online</td>
<td>2</td>
<td>0.8%</td>
</tr>
<tr>
<td>Phishing scam</td>
<td>1</td>
<td>0.4%</td>
</tr>
</tbody>
</table>

| **Electronic Money Laundering and Tax Evasion**          |           |         |
| Money laundering using EFT                               | 1         | 0.4%    |

| **Electronic Sales and Investment Fraud**                |           |         |
| Online auction site fraud (fail to deliver goods)       | 16        | 6.7%    |
| Fraudulent loan applications via Internet                | 9         | 3.8%    |
| Other Internet sales fraud (fail to deliver / pay for goods) | 8       | 3.3%    |
| Sales fraud via telephone (fail to pay for goods)       | 2         | 0.8%    |
| Fraudulent insurance claims via computer                | 2         | 0.8%    |
| Sell stolen goods online                                | 2         | 0.8%    |

| **Identity related crime**                               |           |         |
| Identity fraud (monetary motive)                         | 5         | 2.1%    |
| Identity theft (monetary motive)                         | 3         | 1.3%    |

| **Electronic Vandalism and Terrorism**                   |           |         |
| Denial of service attack                                 | 2         | 0.8%    |

| **Information Piracy**                                   |           |         |
| Pirate computer games                                    | 1         | 0.4%    |
| Pirate clothing using computer                           | 1         | 0.4%    |

| **Theft of Telecommunications Services**                 |           |         |
| Unauthorised access to an ISP account                    | 17        | 7.1%    |

| **Other**                                                |           |         |
| Create false document using computer                     | 17        | 7.1%    |
| Altered cheque using computer                            | 4         | 1.7%    |
| Forge currency using computer                            | 2         | 0.8%    |

| **Total**                                                | 240       | 100.0%  |

* Categories of e-crime from Grabosky and Smith (2003).
† Total exceeds number of Deception incidents examined (N=202), as some incidents involved more than a single e-crime activity.
And the interviewees indicated that increasingly, phishing is linked to identity theft:

When you think about all these mules that have been providing their details to the crooks – they’re actually giving their account numbers, their drivers licence numbers, their home addresses, their phone numbers as part of their job applications. So the crooks have a store of information there where they could then move to identity theft. Likewise, if I compromise a computer to steal funds, I can actually take whatever I want off that computer. And most people have a lot of personal details. One of the things we’re trying to do is get our customers to understand that it’s their privacy that’s actually been breached, because they may have photos of their kids, which end up on a paedophile site, they may have business accounts, their tax – so people get

<table>
<thead>
<tr>
<th>Table 5.8: Breakdown of harassment incidents by e-crime activity</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Category/Description</strong></td>
</tr>
<tr>
<td><strong>Cyber stalking</strong></td>
</tr>
<tr>
<td>Use telephone to offend, menace or harass</td>
</tr>
<tr>
<td>Use SMS to offend, menace or harass</td>
</tr>
<tr>
<td>Stalk via Telephone</td>
</tr>
<tr>
<td>Use email to offend, menace or harass</td>
</tr>
<tr>
<td>Stalk via Email</td>
</tr>
<tr>
<td>Surveillance of victim (telephone intercept, video camera etc)</td>
</tr>
<tr>
<td>Stalk via SMS</td>
</tr>
<tr>
<td>Stalk via Internet</td>
</tr>
<tr>
<td>Use Internet to offend, menace or harass</td>
</tr>
<tr>
<td><strong>Dissemination of offensive content</strong></td>
</tr>
<tr>
<td>Defamatory website</td>
</tr>
<tr>
<td><strong>Identity-related crime</strong></td>
</tr>
<tr>
<td>Identity theft (defamation as motive)</td>
</tr>
<tr>
<td>Identity theft (stalking as motive)</td>
</tr>
<tr>
<td><strong>Total</strong></td>
</tr>
</tbody>
</table>


* Categories of e-crime from Grabosky and Smith (2003).
† Total exceeds number of sampled Harassment incidents (N=97) as some incidents involved more than one e-crime activity.
tax file numbers, they get income, they get addresses – all that sort of stuff, which you can take off a computer (PS#11).

As seen in Table 5.8 most e-crime harassment incidents involved telephones instead of computers, although some harassment and stalking took place via email or defamatory websites.

Incidents in the Regulated Public Order category consisted mainly of possession of digital child pornographic images, and much less the

<table>
<thead>
<tr>
<th>Table 5.9: Breakdown of regulated public order incidents by e-crime activity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category/Description</td>
</tr>
<tr>
<td><strong>Dissemination of Offensive Content</strong></td>
</tr>
<tr>
<td>Possess digital child pornography</td>
</tr>
<tr>
<td>Show pornography to minor via computer</td>
</tr>
<tr>
<td>Make child pornography (eg digital camera or printer)</td>
</tr>
<tr>
<td>Show minor pornographic video</td>
</tr>
<tr>
<td>Distribute child pornography online</td>
</tr>
<tr>
<td><strong>Electronic Funds Transfer Crime</strong></td>
</tr>
<tr>
<td>Credit betting via computer</td>
</tr>
<tr>
<td>Credit card fraud</td>
</tr>
<tr>
<td><strong>Information Piracy</strong></td>
</tr>
<tr>
<td>Pirate DVDs</td>
</tr>
<tr>
<td>Pirate computer games</td>
</tr>
<tr>
<td><strong>Theft of Telecommunications Services</strong></td>
</tr>
<tr>
<td>Unauthorised access to an ISP account</td>
</tr>
<tr>
<td><strong>Other</strong></td>
</tr>
<tr>
<td>Groom child via chat room</td>
</tr>
<tr>
<td>Groom child via telephone</td>
</tr>
<tr>
<td><strong>Total</strong></td>
</tr>
</tbody>
</table>

* Categories of e-crime from Grabosky and Smith (2003).
† Total exceeds number of sampled Regulated Public Order incidents (N=39) as some incidents involved more than one e-crime activity.
distribution of such materials. The credit card fraud and unauthorised access to an ISP account referred to in Table 5.9 relates to incidents of obtaining child pornography online. Credit betting incidents involved punters distracting staff and entering bets into betting agency computer systems without payment.

In most cases, the blackmail incidents noted in Table 5.10 involved demands for payment of a “reward” for the return of a lost mobile phone,

<table>
<thead>
<tr>
<th>Category/Description</th>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cyber stalking</strong>*</td>
<td>2</td>
<td>6.7%</td>
</tr>
<tr>
<td>Surveillance of victim (video camera)</td>
<td>2</td>
<td>6.7%</td>
</tr>
<tr>
<td><strong>Digital Extortion</strong></td>
<td>4</td>
<td>13.3%</td>
</tr>
<tr>
<td>Blackmail via telephone</td>
<td>4</td>
<td>13.3%</td>
</tr>
<tr>
<td>Blackmail via SMS</td>
<td>2</td>
<td>6.7%</td>
</tr>
<tr>
<td><strong>Dissemination of Offensive Content</strong></td>
<td>1</td>
<td>3.3%</td>
</tr>
<tr>
<td>Make child pornography (digital camera)</td>
<td>1</td>
<td>3.3%</td>
</tr>
<tr>
<td><strong>Electronic Sales and Investment Fraud</strong></td>
<td>1</td>
<td>3.3%</td>
</tr>
<tr>
<td>Fraudulent loan applications via Internet</td>
<td>1</td>
<td>3.3%</td>
</tr>
<tr>
<td><strong>Electronic Vandalism and Terrorism</strong></td>
<td>13</td>
<td>43.3%</td>
</tr>
<tr>
<td>Bomb Hoaxes via Telephone</td>
<td>13</td>
<td>43.3%</td>
</tr>
<tr>
<td>Bomb Hoaxes via Internet</td>
<td>1</td>
<td>3.3%</td>
</tr>
<tr>
<td>Domain Name Service hijacking</td>
<td>1</td>
<td>3.3%</td>
</tr>
<tr>
<td>Unauthorised access to &amp; modify data in company computer</td>
<td>1</td>
<td>3.3%</td>
</tr>
<tr>
<td><strong>Identity related Crime</strong></td>
<td>1</td>
<td>3.3%</td>
</tr>
<tr>
<td>Identity fraud (monetary motive)</td>
<td>1</td>
<td>3.3%</td>
</tr>
<tr>
<td>Identity theft (monetary motive)</td>
<td>1</td>
<td>3.3%</td>
</tr>
<tr>
<td><strong>Information Piracy</strong></td>
<td>1</td>
<td>3.3%</td>
</tr>
<tr>
<td>Pirate video cassettes</td>
<td>1</td>
<td>3.3%</td>
</tr>
<tr>
<td>Pirate CDs</td>
<td>1</td>
<td>3.3%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>30</td>
<td>100.0%</td>
</tr>
</tbody>
</table>

* Categories of e-crime from Grabosky and Smith (2003).
communicated to the victim via their own mobile phone. For software companies, digital extortion can involve hackers demanding money to reveal vulnerabilities in software. “So, that’s a tough situation, they [hackers] want us to pay for exploits of our own software” (PS#9).

In the incidents that involved charges of Sex (Non rape) offences, the e-crime activity was generally preparatory to the charged sexual offence (see Table 5.11).

Seven “pure” e-crime offences were represented in the sample data (see Table App.O.2). Table 5.12 shows the activities that were involved that warranted charges under these offences for the total 43 incidents sampled. Most incidents involved unauthorised access to computers, exactly as described by the offences. In a quarter of cases, offences like OPBD or OFABD were charged and the “pure” e-crime offence was a secondary or even tertiary charge (n=10).

Table 5.11: Breakdown of sex (non rape) incidents by e-crime activity

<table>
<thead>
<tr>
<th>Category/Description of activity</th>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dissemination of Offensive Content*</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Possess digital child pornography</td>
<td>3</td>
<td>27.3%</td>
</tr>
<tr>
<td>Make child pornography with digital camera</td>
<td>2</td>
<td>18.2%</td>
</tr>
<tr>
<td>Show pornography to minor via computer</td>
<td>1</td>
<td>9.1%</td>
</tr>
<tr>
<td>Show minor pornographic video</td>
<td>1</td>
<td>9.1%</td>
</tr>
<tr>
<td>Digital Extortion</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Blackmail for sex via SMS</td>
<td>1</td>
<td>9.1%</td>
</tr>
<tr>
<td>Other</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Groom child via chat room</td>
<td>3</td>
<td>27.3%</td>
</tr>
<tr>
<td>Total</td>
<td>11</td>
<td>100.0%</td>
</tr>
</tbody>
</table>

* Categories of e-crime from Grabosky and Smith (2003).
Modus operandi

The modi operandi (MO) for committing e-crime are constantly evolving. One interviewee police officer described the constant change in reference to contacting interstate police for assistance:

You’ll ring them up and say something like “Oh look there’s a group of scammers running identity factories and generating false licences and cheques, and they’re Lebanese or whatever” and they’ll say “Oh yeah and which mob are you talking about this week?” So it’s either that group or it just morphs itself and creates splinter groups of itself and they break away groups and they think, “Oh this is how you make good money: we’ll break away and do it ourselves”. And they break away from the main group and you sort of get that multiplier effect or the main group may change its MO and, you know, it might be looking at cards, cheques or whatever one month and then it might head off and do some sort of loan scam the next and it might reinvent itself and go and target some retailers the next time and they will all be bringing in false cards from overseas and... you know it’s constant (VP#10).

The Victoria Police forms on which police reports are made include checkboxes for various modus operandi descriptors of the incident; multiple boxes may be checked. A location type is considered mandatory on these forms. One hundred and five different modus operandi labels were evident in the LEAP data. However, very few of the 3529 LEAP records in this study had more than one modus operandi entry (n=113, 3.2%), even fewer recording three (n=9, 0.3%). Only two incidents recorded four different modus operandi entries. This likely reflects distaste for paperwork more than an inability to

---

73 A few labels were repetitive, such as “ATM / EFTPOS” and “ATM / EFTPOS INVOLVED”.
Table 5.12: Breakdown of “pure” e-crime offences by e-crime activity

<table>
<thead>
<tr>
<th>LEAP Offence Code /Description of activity</th>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>321MQ: UNAUTH INTERFERE WITH COMPUTER</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unauthorised access to an ISP account</td>
<td>3</td>
<td>6.3%</td>
</tr>
<tr>
<td>Identity theft (defamation as motive)</td>
<td>1</td>
<td>2.1%</td>
</tr>
<tr>
<td>Unauthorised access to info in a computer</td>
<td>1</td>
<td>2.1%</td>
</tr>
<tr>
<td><strong>321PJ: KNOWINGLY CAUSE UNAUTH COMPUTER FUNCTION</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identity theft (monetary motive)</td>
<td>1</td>
<td>2.1%</td>
</tr>
<tr>
<td>Denial of Service (changed banking password)</td>
<td>1</td>
<td>2.1%</td>
</tr>
<tr>
<td><strong>593M: ENTER COMPUTER SYSTEM - NO AUTHORITY</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Delete / Modify Info in Computer</td>
<td>4</td>
<td>8.3%</td>
</tr>
<tr>
<td>Unauthorised access to a company computer</td>
<td>3</td>
<td>6.3%</td>
</tr>
<tr>
<td>Unauthorised access to an ISP account</td>
<td>3</td>
<td>6.3%</td>
</tr>
<tr>
<td>Unauthorised access to info in a computer</td>
<td>3</td>
<td>6.3%</td>
</tr>
<tr>
<td>Denial of Service (change accounts)</td>
<td>2</td>
<td>4.2%</td>
</tr>
<tr>
<td>Identity theft (defamation as motive)</td>
<td>2</td>
<td>4.2%</td>
</tr>
<tr>
<td>Deface website (defamation as motive)</td>
<td>1</td>
<td>2.1%</td>
</tr>
<tr>
<td>Modify website (money as motive)</td>
<td>1</td>
<td>2.1%</td>
</tr>
<tr>
<td>Unauthorised access to a home computer</td>
<td>1</td>
<td>2.1%</td>
</tr>
<tr>
<td>Credit card and identity fraud against Internet merchant</td>
<td>1</td>
<td>2.1%</td>
</tr>
<tr>
<td>Use email to offend, menace or harass</td>
<td>1</td>
<td>2.1%</td>
</tr>
<tr>
<td><strong>593N: GAIN ACCESS TO COMPUTER - NO AUTHORITY</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unauthorised access to an ISP account</td>
<td>5</td>
<td>10.4%</td>
</tr>
<tr>
<td>Denial of Service attack (crashed company computers)</td>
<td>1</td>
<td>2.1%</td>
</tr>
<tr>
<td>Deface company website (defamation as motive)</td>
<td>1</td>
<td>2.1%</td>
</tr>
<tr>
<td>Delete / Modify Info in Computer</td>
<td>1</td>
<td>2.1%</td>
</tr>
<tr>
<td>Disable security system</td>
<td>1</td>
<td>2.1%</td>
</tr>
<tr>
<td>No narrative recorded</td>
<td>1</td>
<td>2.1%</td>
</tr>
<tr>
<td>Identity theft (defamation as motive)</td>
<td>1</td>
<td>2.1%</td>
</tr>
<tr>
<td>Create defamatory website</td>
<td>1</td>
<td>2.1%</td>
</tr>
<tr>
<td><strong>832AS: USE/POSSESS/SELL PHONE INTERCEPT DEVICE</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tapped telephone line</td>
<td>2</td>
<td>4.2%</td>
</tr>
<tr>
<td>Possess other listening device</td>
<td>1</td>
<td>2.1%</td>
</tr>
<tr>
<td><strong>832AZ: INTERCEPT A COMMUNICATION</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tapped telephone line</td>
<td>1</td>
<td>2.1%</td>
</tr>
<tr>
<td>Use video camera and recorder for surveillance</td>
<td>1</td>
<td>2.1%</td>
</tr>
<tr>
<td>Use other listening device</td>
<td>1</td>
<td>2.1%</td>
</tr>
<tr>
<td><em><em>N/A</em>: “UNAUTH MODIFICATN OF DATA TO CAUSE IMPAIRMENT”</em>*</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Domain Name Service hijacking</td>
<td>1</td>
<td>2.1%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>48†</td>
<td>100.0%</td>
</tr>
</tbody>
</table>


* No offence code or description existed in LEAP at the time of sampling in Sept-Oct 2004 for s.247C of the Crimes Act (Vic); recorded under 321MQ.
† Some incidents involved multiple e-crime activities, thus exceeding total incidents (N=43).
record multiple descriptors. Almost one in ten incidents of the sample recorded no modus operandi data (n=312, 8.8%).

As seen in Table 5.13 most incidents of e-crime involved credit cards. Interestingly, “House”, which might not be considered very descriptive, was the second most oft recorded descriptor of these e-crime incidents. MO recorded computer involvement in only 4.7% of the incidents, although examination of incident narratives revealed this to be under-representative.

The labels ‘Totally computer based’, ‘Intangible property involved’ and

<table>
<thead>
<tr>
<th>Rank</th>
<th>Modus Operandi entry</th>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>CREDIT CARD INVOLVED</td>
<td>680</td>
<td>20.4%</td>
</tr>
<tr>
<td>2.</td>
<td>HOUSE</td>
<td>601</td>
<td>18.0%</td>
</tr>
<tr>
<td>3.</td>
<td>ATM / EFTPOS INVOLVED</td>
<td>304</td>
<td>9.1%</td>
</tr>
<tr>
<td>4.</td>
<td>ATM / EFTPOS</td>
<td>252</td>
<td>7.5%</td>
</tr>
<tr>
<td>5.</td>
<td>UNSPECIFIED / UNKNOWN LOCATION</td>
<td>170</td>
<td>5.1%</td>
</tr>
<tr>
<td>6.</td>
<td>COMPUTER USED</td>
<td>157</td>
<td>4.7%</td>
</tr>
<tr>
<td>7.</td>
<td>BUSINESS OFFICE</td>
<td>122</td>
<td>3.7%</td>
</tr>
<tr>
<td>8.</td>
<td>BANK</td>
<td>108</td>
<td>3.2%</td>
</tr>
<tr>
<td>9.</td>
<td>ACQUAINTANCE</td>
<td>84</td>
<td>2.5%</td>
</tr>
<tr>
<td>10.</td>
<td>FLAT / UNIT / APARTMENT</td>
<td>81</td>
<td>2.4%</td>
</tr>
<tr>
<td>11.</td>
<td>OTHER RETAIL</td>
<td>68</td>
<td>2.0%</td>
</tr>
<tr>
<td>12.</td>
<td>CIVILIAN / OTHER</td>
<td>53</td>
<td>1.6%</td>
</tr>
<tr>
<td>13.</td>
<td>SCHOOL</td>
<td>48</td>
<td>1.4%</td>
</tr>
<tr>
<td>14.</td>
<td>STREET / LANE / FOOTPATH</td>
<td>45</td>
<td>1.3%</td>
</tr>
<tr>
<td>15.</td>
<td>CASH STOLEN</td>
<td>38</td>
<td>1.1%</td>
</tr>
<tr>
<td>16.</td>
<td>OTHER LOCATION (NOT ELSEWHERE)</td>
<td>30</td>
<td>0.9%</td>
</tr>
<tr>
<td>17.</td>
<td>ALCOHOL / DRUG AFFECTED</td>
<td>26</td>
<td>0.8%</td>
</tr>
<tr>
<td>18.</td>
<td>CHILD INVOLVED</td>
<td>24</td>
<td>0.7%</td>
</tr>
<tr>
<td>19.</td>
<td>NO RELATIONSHIP</td>
<td>22</td>
<td>0.7%</td>
</tr>
<tr>
<td>20.</td>
<td>DEPARTMENT STORE</td>
<td>19</td>
<td>0.6%</td>
</tr>
<tr>
<td>20.</td>
<td>FORMER SPOUSE OR DEFACTO</td>
<td>19</td>
<td>0.6%</td>
</tr>
<tr>
<td>20.</td>
<td>OTHER EDUCATIONAL</td>
<td>19</td>
<td>0.6%</td>
</tr>
<tr>
<td>20.</td>
<td>SUPERMARKET</td>
<td>19</td>
<td>0.6%</td>
</tr>
</tbody>
</table>

‘Extra-territorial link’, which might be thought common to e-crime were each used only once.

As a practical application of the definition of e-crime discussed in Chapter Two, the stratified sample incidents were coded according to the definition, as involving digital technologies used as tools, targets or storage media. In 100% of incidents (n=365) digital technology was used as a tool in the commission of the offence. Digital technology was the target of the crime in 12.6% (n=46) of incidents. In 27.7% of incidents (n=101) the digital technology was used as a storage medium for illegal data.

**Cost of e-crime**

LEAP includes a field called “Total Value Lost”, however this field was consistently empty in the sample data extracted for this study. Instead, some narratives included a statement of the total value lost in an incident or listed the values lost in sub-incidents. However, this was by no means recorded consistently. Only 117 incidents of the 365 coded recorded a dollar value loss. The average loss recorded was AUS$46,499.31. The maximum value lost in a single incident was AUS$1.7 million. In total, AUS$5,440,419 was recorded lost for the 117 sample incidents.

**How incidents came to police attention**

In almost all cases, e-crime incidents were reported to police (see Table 5.14). This reflects what we know in general about the involvement of the police in detection of crime (see especially, Felson, 1998: 9). Very few incidents involved the police “detecting” e-crime in the process of policing. It is worth noting that no incidents in this study came to police attention through online police patrolling or undercover operations. Operations focused on credit card
“skimming” accounted for the majority of incidents detected by police. In three incidents offenders were so dim-witted as to telephone bomb threats directly to police! Who ever said criminals were smart (*contra*, Felson, 1998: 14-16)?

Table 5.14: How e-crime incidents came to police attention

<table>
<thead>
<tr>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reported</td>
<td>326</td>
</tr>
<tr>
<td>Police operation</td>
<td>8</td>
</tr>
<tr>
<td>Patrol</td>
<td>4</td>
</tr>
<tr>
<td>Referred from other police force</td>
<td>3</td>
</tr>
<tr>
<td>Detected while investigating other incident</td>
<td>3</td>
</tr>
<tr>
<td>Offender rang police</td>
<td>3</td>
</tr>
<tr>
<td>Traffic stop</td>
<td>2</td>
</tr>
<tr>
<td>Forensic computer analysis</td>
<td>1</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>350</strong></td>
</tr>
</tbody>
</table>


**Who reported e-crime?**

The majority of e-crime incidents examined in this study were reported to Victoria Police by individual complainants (n=193, 52.9%, see Figure 5.2). This confirms Chan’s (2000) finding that individuals are more likely to report e-crime than corporations. Companies were the next most common category of complainants (n=62, 16.9%). Only one incident listed an investigations service company as the complainant on behalf of their client. In several cases computer repair companies discovered illegal materials on computers they were repairing, whereupon they involved police.

ISPs only reported a small number of incidents involving unauthorised access to an ISP account, again confirming Chan’s findings that those with more IT knowledge are less likely to report. It is interesting to note that for the period in review, no Internet Service Provider reported illegal downloading of child pornography to Victoria Police. Hopefully, this situation will improve in the
future. In the context of changes to federal law in March 2005 (see Chapter Two) it should.

**Figure 5.2: Who reported e-crime to Victoria Police, 1999/00-2003/04**

![Bar chart showing the distribution of e-crime reports by source.](chart.png)


Banks were recorded as the complainants in only five percent of e-crime incidents in this study. Bank investigators spoken to for this research indicated that e-crime has only been a concern for them in the twelve months preceding the study.

Essentially, twelve months ago we didn’t really have an issue. And now we do. In fact, in [this bank’s] case, we didn’t have an issue up until probably April (PS#11).

The industry sector of complainants, according to the ANZ Standard Industry Classification, was only discernible in a third of these incidents. Figure 5.3
shows that break down. IT companies are included in the Communications Services industry, as per the standard.

Figure 5.3: E-crime complainants by industry sector

![Bar chart showing counts of e-crime complainants by industry sector.]

Source: McKenzie 2005, E-Crime Investigation Study [computer file], N=141 incidents, 244 missing.

**Age and sex of alleged e-crime offenders**

Two e-crime incidents had the maximum number of seven alleged offenders. In one, all seven defendants were male. In the other, three were male and four were female. Most incidents recorded only one offender. Overall, the e-crime data recorded the sex of 1010 alleged offenders across 893 incidents and this data was missing from the 2636 others. Men were more than twice as often represented as alleged offenders of e-crime than women (see Table 5.15).
Table 5.15: Sex of alleged e-crime offenders in sampled incidents, 1999/00-2003/04

<table>
<thead>
<tr>
<th>Sex of Alleged Offender</th>
<th>Frequency</th>
<th>Percent</th>
<th>Valid Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Male</td>
<td>737</td>
<td>20.2%</td>
<td>73.0%</td>
</tr>
<tr>
<td>Female</td>
<td>273</td>
<td>7.5%</td>
<td>27.0%</td>
</tr>
<tr>
<td>Not recorded for incident</td>
<td>2636</td>
<td>72.3%</td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td>3646*</td>
<td>100%</td>
<td>100%</td>
</tr>
</tbody>
</table>


* Total exceeds number of incidents (N=3529), as some incidents recorded more than one alleged offender.

Unlike images of Matthew Broderick as the teenage hacker in War Games (1983), most alleged e-crime offenders in these incidents were adults. Date of birth information was available for only 862 alleged offenders.74 The average age of offenders was calculated from the date of birth and date entered as the commencement of the incident. The average age of alleged offenders at commencement of their incidents was 29 years with a standard deviation of ten years (n=862; $\bar{X}=29.4$, $\sigma=10.0$). The oldest offender recorded was 64 and the youngest 11 years old.75 Victoria Police classifies persons under the age of 17 as juveniles (Victoria Police, 2003b: 7). Only 53 incidents recorded juvenile offenders.

Age and sex of e-crime victims

The sex of e-crime victims was often not recorded in the LEAP field VICTIMSEX; however in many cases this was evident in the narratives. Information was compiled for 769 incidents on 808 victims. Table 5.16 indicates that the majority of e-crime victims were women. Age information

---

74 Excludes one entry giving date of birth years in the future and another four where data did not match narrative; offenders would be too young to commit the alleged sexual offences.

75 In Victoria children under 10 years cannot be charged with an offence and between 10 and 14 there is a *doli incapax* presumption that the child is “incapable of crime” (AIC, 2005).
was available for only 465 victims.\textsuperscript{76} The average age of victims at the time the incident was first committed was 37 years (n=465; \(\bar{X}=36.8, \sigma=15.15\)). The eldest victim recorded was 96 and the youngest 6 years old.

Table 5.16: Sex of e-crime victims in sampled incidents, 1999/00-2003/04

<table>
<thead>
<tr>
<th>Sex of Victim</th>
<th>Frequency</th>
<th>Percent</th>
<th>Valid Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Female</td>
<td>360</td>
<td>10.1%</td>
<td>44.6%</td>
</tr>
<tr>
<td>Male</td>
<td>249</td>
<td>7.0%</td>
<td>30.8%</td>
</tr>
<tr>
<td>Not applicable</td>
<td>199</td>
<td>5.6%</td>
<td>24.6%</td>
</tr>
<tr>
<td>Not recorded for incident</td>
<td>2760</td>
<td>77.4%</td>
<td></td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>3568</td>
<td>100%</td>
<td>100%</td>
</tr>
</tbody>
</table>


* Total exceeds number of incidents (N=3529), as some incidents recorded more than one victim.

Only 35 incidents recorded age information for a juvenile victim; it was very common that the dates of birth for juveniles and victims in general were not recorded in LEAP.

**Relationship of alleged offenders to victims**

Table 5.17 illustrates the relationships between alleged offenders and their victims. Where a relationship was discernible from the incident narrative, most often this was a “customer” relationship, where the customer was the offender. In only one of the sampled incidents could that customer relationship be further characterised as that of a “mule”. In 19 incidents of Internet sales fraud or auction site fraud the online merchant was the offender and the customer the victim. However, in a large number of incidents there was no relationship between the alleged offender and the victim, such as in many credit card frauds and unauthorised accessing of Internet accounts. Overall, e-crime offenders were unlikely to have had a

\textsuperscript{76} Excludes one incident for which Date of Birth was clearly entered incorrectly.
personal or close business relationship with their victims on the basis of the sampled incidents.

Table 5.17: Relationship of alleged offenders to victim in e-crime incidents

<table>
<thead>
<tr>
<th>Offender's status</th>
<th>Number of Incidents</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer</td>
<td>70</td>
<td>19.2%</td>
</tr>
<tr>
<td>No relationship</td>
<td>68</td>
<td>18.6%</td>
</tr>
<tr>
<td>Not recorded</td>
<td>68</td>
<td>18.6%</td>
</tr>
<tr>
<td>Current employee</td>
<td>51</td>
<td>14.0%</td>
</tr>
<tr>
<td>Acquaintance</td>
<td>37</td>
<td>10.1%</td>
</tr>
<tr>
<td>Online Merchant</td>
<td>19</td>
<td>5.2%</td>
</tr>
<tr>
<td>Former personal relationship*</td>
<td>17</td>
<td>4.7%</td>
</tr>
<tr>
<td>Family</td>
<td>14</td>
<td>3.8%</td>
</tr>
<tr>
<td>Current personal relationship</td>
<td>9</td>
<td>2.5%</td>
</tr>
<tr>
<td>Other business relation</td>
<td>6</td>
<td>1.6%</td>
</tr>
<tr>
<td>Student</td>
<td>5</td>
<td>1.4%</td>
</tr>
<tr>
<td>Former employee</td>
<td>1</td>
<td>0.3%</td>
</tr>
<tr>
<td>Total</td>
<td>365</td>
<td>100%</td>
</tr>
</tbody>
</table>

* Personal relationships were characterised as spousal, de facto or boyfriend-girlfriend, and in one case housemate.

Locations of alleged offenders and victims

Most alleged offenders in this study were located in Victoria (see Table 5.18). Of course, this may be an artefact of Victoria Police recording offences alleged to have occurred in Victoria, referring others to different jurisdictions or the cleared sample.

Table 5.18: Location of alleged e-crime offenders

<table>
<thead>
<tr>
<th>Location</th>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Victoria</td>
<td>334</td>
<td>91.5%</td>
</tr>
<tr>
<td>New South Wales</td>
<td>13</td>
<td>3.6%</td>
</tr>
<tr>
<td>Not recorded</td>
<td>11</td>
<td>3.0%</td>
</tr>
<tr>
<td>Queensland</td>
<td>3</td>
<td>0.8%</td>
</tr>
<tr>
<td>Overseas (mainly Russia)</td>
<td>3</td>
<td>0.8%</td>
</tr>
<tr>
<td>South Australia</td>
<td>1</td>
<td>0.3%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>365</strong></td>
<td><strong>100%</strong></td>
</tr>
</tbody>
</table>

Similarly, most victims who reported e-crime incidents to Victoria Police were located in the state of Victoria (see Table 5.19). Only one incident narrative in the sample recorded a victim company from overseas, in Bulgaria. In each incident for which the location of the victim was not recorded the offender was located in Victoria. No narrative recorded any incident where neither the victim nor alleged offender resided in Victoria.

Table 5.19: Location of e-crime victims

<table>
<thead>
<tr>
<th></th>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Victoria</td>
<td>311</td>
<td>85.2%</td>
</tr>
<tr>
<td>Not recorded</td>
<td>41</td>
<td>11.2%</td>
</tr>
<tr>
<td>New South Wales</td>
<td>4</td>
<td>1.1%</td>
</tr>
<tr>
<td>Queensland</td>
<td>3</td>
<td>0.8%</td>
</tr>
<tr>
<td>Western Australia</td>
<td>2</td>
<td>0.5%</td>
</tr>
<tr>
<td>Overseas</td>
<td>1</td>
<td>0.3%</td>
</tr>
<tr>
<td>Northern Territory</td>
<td>1</td>
<td>0.3%</td>
</tr>
<tr>
<td>South Australia</td>
<td>1</td>
<td>0.3%</td>
</tr>
<tr>
<td>Tasmania</td>
<td>1</td>
<td>0.3%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>365</strong></td>
<td><strong>100%</strong></td>
</tr>
</tbody>
</table>


Response zones

Most incidents are reported initially to local police stations and then referred to local criminal investigation units (CIUs). Figure 5.4 maps the top ten CIUs to have responded to e-crime incidents in Victoria for the five-year period. Eighty-four CIUs responded to an e-crime incident over the five-year period. Melbourne CIU handled the most incidents (n=431) and Melbourne Airport the least (n=1).

These top ten response zones between them cleared one third of all the incidents identified as e-crime in this study. Regional data was missing from LEAP in over 61% of incidents, but could be extrapolated from CIU response
zone data. Overall, response to e-crime was fairly evenly distributed across the five Victoria Police Regions. Region 1 cleared the most incidents (n=902), next Region 4 (n=705), then Region 3 (n=657), Region 2 (n=643) and Region 5 (n=603).

Figure 5.4: Map of the top ten response zones for e-crime incidents in Victoria 1999/00-2003/04


**Squad involvement in e-crime cases**

The LEAP database is a poor source of information about the involvement of the specialist Victoria Police squads in any particular incident. In the sample of e-crime incidents for which narratives were coded, the Computer Crime
Squad, the Sexual Crimes Squad and investigation squads of the Major Fraud Investigation Division were the specialist squads referenced most often (see Figure 5.5).

**Figure 5.5: References to squad involvement in e-crime incident narratives**

![Bar chart showing references to squad involvement in e-crime incident narratives](image)

* May not reflect accurately actual involvement of squads due to inconsistent reporting.

However, due to the inconsistent reporting in these narratives, this probably does not provide an accurate picture of the extent to which these squads are involved. For example, the Computer Crime Squad was only mentioned 39 times over 365 incidents. To be able to report their activities, squads often maintain their own databases about the work they undertake. The Computer Crime Squad compiles statistics on its workload for each fiscal year from its Computer Crime Jobs Database and these were made available for this research; however similar data was not available for MFID or the Sex Crimes Squad. The workload of the Computer Crime Squad is presented in comparison to the LEAP data (see Table 5.20) and this clearly exceeds 39 cases over five years.
In Table 5.20, ‘Internet Assistance Request’ includes liaison with Internet Service Providers, tracing of IP addresses and similar activities. ‘Investigative assistance’ involves investigating police members meeting with members of CCS to discuss possible avenues for an inquiry. ‘Case Assessment’ involves providing an assessment of the briefs of evidence to assess options for prosecution and whether they are ready for prosecution. The category of ‘Other’ tasks includes activities such as court ordered secure wiping of hard disk drives following prosecution, duplication of media for trial and format conversions, such as reformatting CCTV footage.

Table 5.20: Jobs received by Computer Crime Squad 1 July 2000 to 30 June 2005

<table>
<thead>
<tr>
<th>Task Category</th>
<th>2000/01</th>
<th>2001/02</th>
<th>2002/03</th>
<th>2003/04</th>
<th>2004/05</th>
</tr>
</thead>
<tbody>
<tr>
<td>Evidence Analysis</td>
<td>210</td>
<td>292</td>
<td>386</td>
<td>360</td>
<td>426</td>
</tr>
<tr>
<td>Internet Assistance Request</td>
<td>188</td>
<td>183</td>
<td>244</td>
<td>336</td>
<td>332</td>
</tr>
<tr>
<td>Investigative Assistance</td>
<td>88</td>
<td>52</td>
<td>55</td>
<td>40</td>
<td>28</td>
</tr>
<tr>
<td>Search &amp; Seizure</td>
<td>46</td>
<td>81</td>
<td>89</td>
<td>28</td>
<td>18</td>
</tr>
<tr>
<td>SIM Card Analysis</td>
<td>40</td>
<td>54</td>
<td>66</td>
<td>115</td>
<td>210</td>
</tr>
<tr>
<td>Other</td>
<td>10</td>
<td>9</td>
<td>36</td>
<td>37</td>
<td>25</td>
</tr>
<tr>
<td>CCS Investigation</td>
<td>1</td>
<td>1</td>
<td>5</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>Case Assessment</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>Offender Interview</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Witness Interview</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td><strong>Total Tasks Received</strong></td>
<td>584</td>
<td>673</td>
<td>881</td>
<td>917</td>
<td>1045</td>
</tr>
</tbody>
</table>


Telephone calls to the squad are not recorded in these figures. CCS receives a minimum of ten calls per day for advice, which are handled by the duty officer. Nor do the figures in the CCS Job database record the requests for assistance that are not accepted by the squad. If a request for forensic computing analysis is not accepted that analysis simply does not take place within Victoria Police.
Table 5.21: Jobs completed by Computer Crime Squad 1 July 2000 to 30 June 2005

<table>
<thead>
<tr>
<th>Task Category</th>
<th>2000/01</th>
<th>2001/02</th>
<th>2002/03</th>
<th>2003/04</th>
<th>2004/05</th>
</tr>
</thead>
<tbody>
<tr>
<td>Evidence Analysis Jobs Completed</td>
<td>216</td>
<td>276</td>
<td>346</td>
<td>332</td>
<td>272</td>
</tr>
<tr>
<td>Internet Assistance Completed</td>
<td>236</td>
<td>158</td>
<td>256</td>
<td>333</td>
<td>274</td>
</tr>
<tr>
<td>Other CCS Jobs Completed</td>
<td>180</td>
<td>242</td>
<td>249</td>
<td>227</td>
<td>292</td>
</tr>
<tr>
<td><strong>Total Tasks Completed</strong></td>
<td><strong>632</strong></td>
<td><strong>676</strong></td>
<td><strong>851</strong></td>
<td><strong>892</strong></td>
<td><strong>839</strong></td>
</tr>
</tbody>
</table>

Note: Completion figures include tasks received in previous years.

Although the total number of jobs completed by CCS declined in 2004/05 from the previous year, this should not be interpreted as meaning there has been a decline in the amount of e-crime or the number of jobs brought to them. Instead, it reflects the increasing complexity and growing amount of data needing analysis in those jobs accepted by CCS. In 2005, stores are often no longer selling hard disk drives smaller than 80GB, compared to average capacities of 3GB to 5GB hard drives only a few years previously in 1999 (Porter, 1999). And storage devices now come in such a varying array—from floppy diskettes to USB thumb drives, watches and even Internet connected fridges—for which investigators need to be trained where to look for digital evidence. From 2003/04 to 2004/05, CCS analysed an additional 5.3 terabytes of data.

Breakdowns of the type of offences dealt with were available for the period July 2001 through 30 June 2005 (see Figures 5.6 through 5.9). Notable from these figures is that the Computer Crime Squad provides regular assistance in homicide and drug cases; two offence types not sampled in this study. This is

---

77 The number of CCS jobs remaining outstanding each year cannot be derived from the figures in Table 5.20 and Table 5.21, as to do so would not take account of tasks carried over from the previous years. Victoria Police considered the figures for outstanding tasks too sensitive for public release.
not to say these offences are ‘e-crime’. An officer from the Computer Crime Squad explained that in those cases it is more about locating digital evidence:

[Y]ou analyse someone’s computer, you can build up a profile of the person. A knowledge and an understanding of them, their circle of friends, their contacts, places they’ve been, when and where they’ve done things and it is that use of that information which identifies, in many cases, the offender. So that’s how computers become involved in far more crime (VP#4).
Figure 5.6: Analysis jobs by offence type performed by Computer Crime Squad 1 July 2001 - 30 June 2002

Figure 5.7: Analysis jobs by offence type performed by Computer Crime Squad 1 July 2002 - 30 June 2003

Figure 5.8: Analysis jobs by offence type performed by Computer Crime Squad 1 July 2003 - 30 June 2004

Figure 5.9: Analysis jobs by offence type performed by Computer Crime Squad 1 July 2004 - 30 June 2005

Digital evidence seized during investigations

Sixty-nine e-crime incident narratives recorded items that were seized by police as evidence during their investigations. Computers and associated equipment were most often seized (n=44, 12.1%). Documents were the next most often seized items (n=5). Various other items were reported seized, including DVDs and CDs, credit card skimmers and card blanks, credit cards, video recorders, listening devices and mobile phones.

The Computer Crime Squad does not record centrally the number or type of exhibits seized for analysis, whether these are computer hard drives, compact or floppy diskettes. Instead, they record the volume of data analysed by squad members in gigabytes, as shown in Table 5.22. The average amount of data analysed by CCS per job each year increased ninefold over the five-year period to July 2005.

Table 5.22: Gigabytes of data analysed by Computer Crime Squad by region or division, 1 July 2000-30 June 2005*

<table>
<thead>
<tr>
<th>Region / Division</th>
<th>2000/01</th>
<th>2001/02</th>
<th>2002/03</th>
<th>2003/04</th>
<th>2004/05</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>110.62</td>
<td>460.00</td>
<td>1245.40</td>
<td>1158.43</td>
<td>2486.79</td>
</tr>
<tr>
<td>2</td>
<td>184.90</td>
<td>586.88</td>
<td>687.20</td>
<td>2387.31</td>
<td>1485.55</td>
</tr>
<tr>
<td>3</td>
<td>353.91</td>
<td>961.09</td>
<td>1289.74</td>
<td>2424.62</td>
<td>2606.87</td>
</tr>
<tr>
<td>4</td>
<td>99.64</td>
<td>421.30</td>
<td>2437.90</td>
<td>2490.09</td>
<td>3210.20</td>
</tr>
<tr>
<td>5</td>
<td>117.81</td>
<td>296.81</td>
<td>516.50</td>
<td>2102.60</td>
<td>2391.82</td>
</tr>
<tr>
<td>Crime</td>
<td>941.33</td>
<td>2352.13</td>
<td>4218.07</td>
<td>5665.01</td>
<td>8580.84</td>
</tr>
<tr>
<td>ESD</td>
<td>15.10</td>
<td>43.31</td>
<td>312.00</td>
<td>198.90</td>
<td>695.54</td>
</tr>
<tr>
<td>Transit</td>
<td>10.00</td>
<td>6.15</td>
<td>82.06</td>
<td>176.10</td>
<td>358.50</td>
</tr>
<tr>
<td>Tactical Ops</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>182.00</td>
<td>0.00</td>
</tr>
<tr>
<td>Other</td>
<td>33.01</td>
<td>82.52</td>
<td>21.00</td>
<td>4.10</td>
<td>450.00</td>
</tr>
<tr>
<td><strong>TOTAL (Gb)</strong></td>
<td>1866.33</td>
<td>5210.20</td>
<td>10809.87</td>
<td>16789.15</td>
<td>22266.11</td>
</tr>
<tr>
<td><strong>TOTAL (Tb)</strong></td>
<td>1.82</td>
<td>5.09</td>
<td>10.56</td>
<td>16.40</td>
<td>21.74</td>
</tr>
<tr>
<td><strong>AVERAGE (Gb/ Job)</strong></td>
<td>2.95</td>
<td>7.7</td>
<td>12.7</td>
<td>18.8</td>
<td>26.5</td>
</tr>
</tbody>
</table>

Source: Computer Crime Job Database, Victoria Police.
* Figures relate to “Evidence Analysis” tasks performed by CCS. 1 Gigabyte (GB) = 0.0009765625 Terabytes (TB) and 1024 GB = 1 Terabyte.
External government agency involvement

In 93.2% (n=340) of the stratified sample of e-crime incidents no other government agency was involved in the investigation. In those 25 cases where other agencies were involved, this was mostly other state police services (n=13), the AFP (n=2) and agencies such as Customs, VicRoads, the Department of Human Services, Department of Social Services and even the Magistrates Court. In only one incident was involvement of a foreign law enforcement agency noted. In most cases the involvement of another state police force indicated referral of an incident to Victoria Police for investigation or referral by Victoria Police of the incident to another police force for investigation.

Private sector involvement in police e-crime investigations

Personnel, mainly investigators, from the private sectors were involved in 20% (n=73) of the examined e-crime incidents. The main activities undertaken by these personnel as described in the incident narratives were provision of bank or other transaction records (n=22, 27.8%), conducting their own internal investigation (n=17, 21.5%), reporting the incident to Victoria Police (n=9, 11.4%) and conducting surveillance (n=6, 7.6%). Table 5.23 displays the activities private personnel were recorded as contributing to the e-crime investigations.

The LEAP incident narratives did not frame this private sector involvement as partnership, nor refer to any formal partnerships, although in most cases interaction was clearly “cooperation” with police. Private sector personnel were not always of assistance to police in these investigations. In a very small number of cases some provided incorrect information about their clients,
Table 5.23: Involvement of private sector personnel in e-crime investigations

<table>
<thead>
<tr>
<th>Activity Performed</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provide Bank / Transaction records*</td>
<td>22</td>
</tr>
<tr>
<td>Conduct an investigation</td>
<td>17</td>
</tr>
<tr>
<td>Report incident</td>
<td>9</td>
</tr>
<tr>
<td>Conduct surveillance</td>
<td>6</td>
</tr>
<tr>
<td>Conduct Reverse Call Charge Record (RCCR) check</td>
<td>5</td>
</tr>
<tr>
<td>Prepare and submit evidence</td>
<td>5</td>
</tr>
<tr>
<td>Identify victim</td>
<td>3</td>
</tr>
<tr>
<td>Decide not to report matter</td>
<td>3</td>
</tr>
<tr>
<td>Identify suspect</td>
<td>3</td>
</tr>
<tr>
<td>Report matter to other jurisdiction</td>
<td>2</td>
</tr>
<tr>
<td>Trace intrusion</td>
<td>2</td>
</tr>
<tr>
<td>Provide other advice</td>
<td>1</td>
</tr>
<tr>
<td>Image HDD</td>
<td>1</td>
</tr>
<tr>
<td><strong>Total†</strong></td>
<td><strong>79</strong></td>
</tr>
</tbody>
</table>

* Includes computer logs.
† Total exceeds 73 incidents, as some private actors undertook multiple investigative activities.

failed to return telephone calls or chose to not formally report matters already brought to police attention by other persons, which delayed or ended investigations.

Duration of offences, delays in reporting and length of investigations

As mentioned, the incidents for this study had to come to police attention during the financial years of 1999/00 through 2003/04. However, that does not mean that offences reported in those years actually occurred during those years. Officers record the date in LEAP that an incident was COMMITTED FROM as well as the date it was COMMITTED TO. If the LEAP data were to be taken at face value, then it would be concluded that the earliest incident included in this sample began in 1931 and continued through 2001 when it was reported to Victoria Police. However, computers were not available in 1931 to facilitate this offending; hence this must be a data entry error. The
narrative for this incident revealed that the offender was not born until 1978, confirming this. Excluding this and another extreme outlier incident, the data reveals that the average length of time from the commencement of an incident to when an offender finished committing the offence was 94 days (n=3527; $\bar{X}=93.9$, $\sigma=329.19$). One respondent investigator linked the length of offending to internal fraud:

It remains hidden for lengthy periods of time, whereas e-crime attack by an external party: you can get on to that within a short period of time. They might have whizzed off with millions of dollars, but at least you’ll know – it’s not going on in the background. Whereas employee fraud you won’t know about it, even when it’s happening, because it’s concealed. External attack you can’t conceal as well as you can internal (PS#4).

In 42.4% of cases, the incident lasted less than a day (n=1496). The longest running e-crime incident in this study ran for 7548 days or twenty years. It involved child pornography and child sex abuse.

Most e-crime incidents were not reported quickly to police. Only 822 e-crime incidents were reported to police on the same day they ended (23.3%). Another 23.6% were reported within one week of the incident concluding. Most were reported between eight days to one year later (n= 1477, 41.9%) and 2.95% (n=104) between a year and two years after the incident. Some incidents were described in their narratives as “historical”. The longest time between the end of an incident and reporting it to police was 2579 days or seven years. Only one percent of sampled incidents were reported more than two years after the incident had ceased.78

78 This is not to suggest that the cessation of offending can be equated always with having detected the offence at that time. No data was available on that issue.
However, not all e-crime incidents had already stopped or then stopped when they were reported to Victoria Police. Offending continued in 253 incidents in this study, representing 7.2% of the main sample. This may not reflect negatively on police, because reporting to police does not always mean that they are able immediately to identify and process an offender without further investigation. The longest time for an incident to finish after having been reported to police was 556 days, or eighteen and a half months later, for a fraud. Where the incident had ceased before reporting it to police, the average length of time between an e-crime incident finishing and it being reported to police was 69 days (n=3276, \( \bar{X}=68.7, \sigma=168.13 \)). Where the incident ceased more than a day after reporting to police, it took an average of 55 days for this to occur (n=253, \( \bar{X}=55.2, \sigma=87.94 \)).

Over the five-year period, the trend was for the length of time to increase between the conclusion of an incident and a complainant\(^79\) reporting it to police (see Figure 5.10). Initially, it was steady across 1999 to 2002, however in 2002 through 2004 there was a steep increase in the length of time between reporting.

\(^{79}\) Includes police as complainants.
A common complaint about e-crime investigation is that it is believed to be difficult to identify suspects. From the incident narratives, it was calculated how long it took to identify the correct suspect in an e-crime investigation. In 48 incidents (13.2%) no suspect was identified. However, in 87.7% of the remaining incidents the suspect was identified either before the incident was reported to police (n=42, 13.2%) or on the same day as the incident was reported (n=194, 61.2%). The longest time between identification of a suspect and then reporting to police was 665 days, or 22 months, for a credit card fraud reported by a financial institution. The longest time taken for Victoria Police to identify a suspect once the e-crime incident had been reported to them was 419 days or fourteen months. The average time for Victoria Police to identify a suspect in an e-crime incident was 15 days (n=275; \( \bar{X} = 14.5, \sigma = 329.19 \)).
Table 5.24 indicates the time between reporting and clearance of the incident by Victoria Police. In most e-crime cases, this was a “single year” clearance.\textsuperscript{80} In fact, the average length of a police investigation of e-crime incident, including processing of the offender where that was involved, was 105 days (\(n=285; \bar{X}=104.9, \sigma=178.56\)). Over a quarter of incidents were resolved on the same day they were reported to police (\(n=81, 28.4\%\)). Forty two percent of incidents were resolved within seven days. If the artificial end date of the financial year is ignored, only 24 e-crime incidents took longer than one year to investigate and clear (6.5%).

Table 5.24: Length of e-crime investigations conducted by Victoria Police, 1999/00-2003/04\textsuperscript{*}

<table>
<thead>
<tr>
<th>Frequency</th>
<th>Percent</th>
<th>Valid Percent</th>
<th>MFID</th>
<th>CCS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single year clearances</td>
<td>213</td>
<td>58.36%</td>
<td>74.74%</td>
<td>3</td>
</tr>
<tr>
<td>Between 1 - 2 years</td>
<td>62</td>
<td>16.99%</td>
<td>21.75%</td>
<td>6</td>
</tr>
<tr>
<td>Between 2 - 3 years</td>
<td>9</td>
<td>2.47%</td>
<td>3.16%</td>
<td>3</td>
</tr>
<tr>
<td>Between 3 - 4 years</td>
<td>1</td>
<td>0.27%</td>
<td>0.35%</td>
<td>0</td>
</tr>
<tr>
<td>Missing relevant dates</td>
<td>80</td>
<td>21.92%</td>
<td>-</td>
<td>1</td>
</tr>
</tbody>
</table>

| Totals | 365 | 100% | 78.1% | 13 | 39 |


\textsuperscript{*} Calculated from financial years in which incident was reported and then resolved.

When cross referenced against the Victoria Police departments involved, the data reveals that for those incidents where the information was available no investigation of e-crime involving the Major Fraud Investigation Division or the CCS took longer than 2 years (see Table 5.24).

Table 5.25 compares single year clearances for the sample with those reported in Victoria Police crime statistics. In 1999/00, all e-crime incidents from this sample were cleared within a single year. In the following year the overall single year clearance rate for the sample dropped to 70.7%. The next year this

\textsuperscript{80} Victoria Police Crime Statistics define single year clearances as when incidents recorded during a particular financial year are cleared within the same period (Victoria Police, 2004a).
rallied to over eighty percent, but has dropped consistently since. Table 5.25 might suggest that e-crime incidents of harassment are cleared more easily than other forms of harassment offences, having higher single year clearance rates than the official statistics; however this sample is too small to state this with certainty.

**Outcomes of police investigations**

The distribution of outcomes for e-crime incidents is shown in Figure 5.11. In the majority of incidents an offender was processed (n=3132, 88.5%). In six percent no offence was disclosed to Victoria Police despite the matter coming to their attention. In five percent the complaint was withdrawn. The category of ‘Other’ generally includes offenders who cannot be charged due to being underage, insane or deceased (Victoria Police, 2004a). “Other” outcomes were recorded in only 34 incidents (approximately 1%) in this sample of e-crime incidents. Remember that no “Unsolved” incidents are included in the data.

**Figure 5.11: Outcomes of cleared e-crime investigations**

![Chart showing outcomes of e-crime investigations]

Table 5.25: Comparison of e-crime sample and Victoria Police Crime Statistics for single year clearances by offence group*

<table>
<thead>
<tr>
<th>Offence Group</th>
<th>1999/00</th>
<th>2000/01</th>
<th>2001/02</th>
<th>2002/03</th>
<th>2003/04</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Sample</td>
<td>Crime Stats</td>
<td>Sample</td>
<td>Crime Stats</td>
<td>Sample</td>
</tr>
<tr>
<td>Deception</td>
<td>14 (100%)</td>
<td>31347 (84.0%)</td>
<td>19 (67.9%)</td>
<td>24444 (82.2%)</td>
<td>25 (86.2%)</td>
</tr>
<tr>
<td>Harassment</td>
<td>11 (100%)</td>
<td>1384 (63.6%)</td>
<td>13 (76.5%)</td>
<td>1288 (66.9%)</td>
<td>11 (84.6%)</td>
</tr>
<tr>
<td>Other</td>
<td>3 (100%)</td>
<td>5294 (75.5%)</td>
<td>3 (75%)</td>
<td>5115 (78.4%)</td>
<td>3 (60%)</td>
</tr>
<tr>
<td>Regulated Public Order</td>
<td>2 (100%)</td>
<td>1898 (96.6%)</td>
<td>4 (66.6%)</td>
<td>1649 (97.2%)</td>
<td>7 (100%)</td>
</tr>
<tr>
<td>Sex (Non rape)</td>
<td>1 (100%)</td>
<td>4789 (74.5%)</td>
<td>2 (66.6%)</td>
<td>4618 (72.8%)</td>
<td>0 (0%)</td>
</tr>
<tr>
<td>Total</td>
<td>32 (100%)</td>
<td>53809 (70.7%)</td>
<td>41 (83.6%)</td>
<td>41732 (73.1%)</td>
<td>46 (68.5%)</td>
</tr>
</tbody>
</table>

* E-crime incidents with clearance dates available (N=213).
The stratified sample was examined more closely as to the reasons for these investigation outcomes. In that sample, an alleged offender or offenders were processed in 314 incidents, no offence was disclosed in 29 incidents, 18 complaints were withdrawn and four incidents had “Other” results. In the majority of incidents, an offender was processed if located in Victoria.

What did “processing” of an offender mean? In the sample, most incidents had “Intent to Summons” as the final recorded outcome in the narrative. The next most common result was recording that the defendant had been bailed. Table 5.26 shows other reasons for recording the incident as “offender processed”. As court outcomes were not recorded uniformly in incident narratives, no inferences about sentences should be drawn from Table 5.26.

Table 5.26: Breakdown of outcomes recorded as “offender processed” for e-crime incidents

<table>
<thead>
<tr>
<th>Investigation Outcome</th>
<th>Number of incidents</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intent to summons (ITS)</td>
<td>101</td>
<td>32.2%</td>
</tr>
<tr>
<td>Bailed</td>
<td>63</td>
<td>20.1%</td>
</tr>
<tr>
<td>No detail recorded</td>
<td>47</td>
<td>15.0%</td>
</tr>
<tr>
<td>Summoned</td>
<td>24</td>
<td>7.6%</td>
</tr>
<tr>
<td>Remanded in custody</td>
<td>21</td>
<td>6.7%</td>
</tr>
<tr>
<td>Cautioned</td>
<td>19</td>
<td>6.1%</td>
</tr>
<tr>
<td>ITS not authorised</td>
<td>14</td>
<td>4.5%</td>
</tr>
<tr>
<td>Arrested</td>
<td>11</td>
<td>3.5%</td>
</tr>
<tr>
<td>Plead guilty at court</td>
<td>4</td>
<td>1.3%</td>
</tr>
<tr>
<td>Suspended sentence</td>
<td>3</td>
<td>1.0%</td>
</tr>
<tr>
<td>Charged</td>
<td>3</td>
<td>1.0%</td>
</tr>
<tr>
<td>Fine</td>
<td>1</td>
<td>0.3%</td>
</tr>
<tr>
<td>No further police action</td>
<td>1</td>
<td>0.3%</td>
</tr>
<tr>
<td>Exonerated</td>
<td>1</td>
<td>0.3%</td>
</tr>
<tr>
<td>Suspect committed suicide</td>
<td>1</td>
<td>0.3%</td>
</tr>
<tr>
<td><strong>Total Incidents</strong></td>
<td><strong>314</strong></td>
<td><strong>100%</strong></td>
</tr>
</tbody>
</table>


Why was “No Offence Disclosed” recorded for other e-crime incidents?

Generally, this means that the first of the four points to be proven in a
criminal investigation—that a criminal offence had been committed (Fairchild, 1994: 115)—had not been satisfied. However, in most of these incidents, it meant that the victim was advised to report the matter to another jurisdiction, because that was where the offender was located (see Table 5.27). It meant “no offence disclosed as occurring in Victoria”. The next most common reason was that a client of an ISP had reported unauthorised access of their account, instead of the ISP reporting the incident. This breached a reporting protocol devised by Victoria Police and discussed further in the next chapter. The ISP then refused to make an official report and Victoria Police took no further action.

<table>
<thead>
<tr>
<th>Reason</th>
<th>Number of incidents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Victim referred to other jurisdiction</td>
<td>8</td>
</tr>
<tr>
<td>Breached ISP/Merchant reporting protocol</td>
<td>5</td>
</tr>
<tr>
<td>Offence caused by &quot;computer error&quot;</td>
<td>3</td>
</tr>
<tr>
<td>Offence not applicable</td>
<td>3</td>
</tr>
<tr>
<td>Requested NFPA</td>
<td>3</td>
</tr>
<tr>
<td>Unsubstantiated complaint</td>
<td>2</td>
</tr>
<tr>
<td>Bank refused to report matter</td>
<td>1</td>
</tr>
<tr>
<td>Discovered identity of offender</td>
<td>1</td>
</tr>
<tr>
<td>Suspect exonerated</td>
<td>1</td>
</tr>
<tr>
<td>External investigation to be conducted</td>
<td>1</td>
</tr>
<tr>
<td>Offender rectified loss</td>
<td>1</td>
</tr>
<tr>
<td><strong>Total incidents</strong></td>
<td><strong>29</strong></td>
</tr>
</tbody>
</table>


Why were complaints withdrawn? In most incidents no reason was recorded for why the complainant had requested no further police action (NFPA).

Police find this one of the most disappointing aspects of their work:

Victim withdraws and decides that they aren’t going to go ahead with it. You put a lot of work in to get it to a stage when you can take it further, and then
they decide that “No, I’m going to make a statement of no complaint”, for whatever reason it may be. And that’s disappointing (AHTCC#3).

Table 5.28: Reasons complaints were withdrawn for e-crime incidents

<table>
<thead>
<tr>
<th>Reason</th>
<th>Number of incidents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reason not recorded</td>
<td>8</td>
</tr>
<tr>
<td>Discovered identity of offender</td>
<td>3</td>
</tr>
<tr>
<td>Service provider required police report</td>
<td>2</td>
</tr>
<tr>
<td>Victim shared culpability</td>
<td>2</td>
</tr>
<tr>
<td>Report for insurance purposes only</td>
<td>1</td>
</tr>
<tr>
<td>No monetary loss</td>
<td>1</td>
</tr>
<tr>
<td>Victim taking other action</td>
<td>1</td>
</tr>
<tr>
<td><strong>Total incidents</strong></td>
<td><strong>18</strong></td>
</tr>
</tbody>
</table>


Table 5.28 shows the other reasons discerned from the incident narratives, including that some police reports were made simply to satisfy service providers or insurance companies. In the four sampled incidents where “Other” had been recorded as the outcome, the incident had either been referred to a different jurisdiction for investigation or there was a breach in the reporting protocol as mentioned above (see also pp. 200-207).

**Chapter conclusions**

This analysis of incidents records paints a clear yet partial picture of the many types of e-crime that Victoria Police encounter and investigate. Unfortunately, it is partial because it was not possible to identify, count, classify or in any way examine the population of “unsolved” e-crime incidents, because of restrictions preventing access to those cases. This analysis revealed deficiencies in the routine official records made by police in the LEAP database. In most cases this was simply missing data, but in more than a few cases it was inaccurate data requiring time consuming correction to permit analysis. This and the format of the police data used in this study, contained
mostly in free text narratives, is likely to continue to rule out regular reporting of the characteristics of e-crime incidents by police. This may also hamper coordinated, intelligence-based police responses to e-crime. For example, modus operandi entries did not sufficiently detail involvement of computers or the Internet and narratives used many different terms, such as “PC”, “computer”, “hard drive”, “net” and “web” and contained misspellings that would complicate the work of police crime analysts trying to identify incidents for analysis. Much missing data, such as offence grouping and police region, should be hard coded into the police database and not require manual input.

These results indicate that there are many types of e-crime that state level policing services are very capable of investigating and resolving. The types of e-crime that are reported to police in Victoria are diverse, ranging commonly from possession of computerised child pornography to credit card fraud. However, e-crime is a small proportion of incidents reported to and investigated by Victoria Police. Most e-crime incidents involved deception or harassment offences and for the most part were much less sophisticated forms of electronic crime than those described in Chapter Two and Appendix A: Phishing, Pharming and DDoS. “Pure” or new e-crime offences were encountered rarely in comparison to those that are considered “traditional” offences, such as deception offences.

Victoria Police processed offenders in the vast majority of cleared e-crime incidents. Incidents investigated successfully occur locally within the state of Victoria, involving local offenders and victims. This nexus to Victoria reflects the points of proof that police need to determine in order to proceed with a prosecution. Multi-jurisdictional investigations were rare. Rather than conduct a multi-jurisdictional investigation, “no offence disclosed” was
recorded routinely and the complainant was referred to the other jurisdiction where the offender was located.

E-crime victims and offenders were less likely to have had a personal or close business relationship, and were more likely to have a “customer” relationship, whether this was computer mediated or face-to-face. Alleged e-crime offenders were on average 29-year-old males. E-crime victims were generally 39-year-old women. Ethnicity data was not available.

Individuals and companies in the retail trade sector reported the most e-crime incidents. Banks were complainants in only about five percent of incidents. Internet Service Providers very rarely reported incidents, although this can be expected to change in future due to new federal mandatory reporting legislation. Only one third of e-crime involved monetary loss according to the LEAP data. Where there was monetary loss, the average loss was AUS$46,499.31.

Most police e-crime investigations were conducted at local crime investigation units, especially the Melbourne CIU. The fairly even distribution of e-crime suggests Victoria Police must provide e-crime investigation training across the board. The workload on the Computer Crime Squad as an investigation support unit has increased exponentially in recent years. The CCS acts as sole provider and gatekeeper in relation to forensic computer analysis. If a request for forensic computing analysis is not accepted that analysis simply does not take place within Victoria Police.

Contrary to common perceptions expressed by respondents, police cleared most of these e-crime incidents as “single year clearances”. Reporting clearances based on financial year can be deceptive of the actual length of investigations, due to the artificial end dates that were found to often push
short investigations into the next “year”. Often e-crime was actually resolved within a week of reporting to police. However, it was clear that the time between detecting e-crime incidents and reporting them to police was increasing and on average was almost three months in 2003/04. As is common practice with most criminal defendants, most e-crime offenders were charged via summons or bailed if arrested.

Most importantly, in relation to the central thesis of this study, reliance on the private sector for successful resolution of e-crime incidents was not apparent from the cleared incidents examined in this study. Nor were other police forces or government agencies often involved according to this data. In the 20% of cases where private investigators were involved, they were most often employees of companies such as telecommunications carriers, financial institutions or Internet Service Providers. Most often their involvement was provision of documents to police, often under search warrants. Less often they conducted internal investigations and then reported back to police. While this suggests that partnership between police and the private sector may not be as important as argued by police, it is possible that the unsolved incidents would tell a different story and remain unsolved due at least in part to lack of evidence resulting from a lack of closer cooperation.

The next chapter examines the respondents’ views on factors impacting upon the successful and unsuccessful investigation of e-crime incidents to further address this question.
Chapter 6: Factors affecting the investigation of e-crime in Victoria

This chapter outlines the current investigative environment in Victoria according to state and federal police and private sector investigators who work e-crime investigations. The chapter provides context to the question of partnered investigations of e-crime between public police and private investigators by exploring the current environment and issues that impact upon their work and triangulating with LEAP data. The next chapter explores these respondents’ reactions and suggestions to the proposed strategy of partnership policing for e-crime investigation.

Interviewees were asked to speak about the most important factors they saw impacting on the success or failure of e-crime investigation in Victoria. What they said revealed influences affecting pivotal stages in the investigative process, which are used to structure the chapter:

- understanding the phenomena of e-crime;
- detecting incidents;
- reporting to police;
- identification of appropriate offences;
- acceptance of incidents for investigation by police;
- prioritisation of investigations;
- goal setting and outcome measurement;
- obtaining evidence;
- providing feedback to complainants; and
- forfeiture of tainted property and victim compensation.

Other factors cited as influencing the overall capacity of police and private investigators to conduct e-crime investigation, such as costs, training, the role
of the Computer Crime Squad, understaffing, backlogs and headhunting are also discussed.

**Shared understandings of ‘e-crime’ or syntax discrepancy?**

As seen in Chapters Two and Five, “e-crime” can refer to a broad range of offences, because the definition relates to modus operandi more than the harm involved. Do the police, private sector investigators and community have the same or different understandings of what constitutes ‘e-crime’? And if they are not on the same page does this affect their agenda and efforts to address these problems together? To begin to address these questions that are fundamental to partnership efforts (see generally, Stenning, 1989: 185), interviewees were first asked what the term “electronic crime” meant to them. Then they were provided with the Australasian Centre for Policing Research definition of e-crime and asked to comment on that and its relevance to their work:

Electronic crimes are where a computer is used as a tool or as a target in the commission of the crime. It includes using a computer as a storage device for illegal data (Etter, Dec 2002).

The e-crime victims interviewed for this study reported a lack of understanding among the police with whom they dealt. “First there’s a blank look” (Victim of identity theft and cyberstalking, PS#20):

The police themselves didn’t seem to know very much about cybercrime either when I first went to the front desk and spoke to the sergeant. I said “I want to declare a cybercrime”. The sergeant just said, “What? Excuse me? What are you talking about?” (PS#3)
said, “I’ve had some money stolen from my bank account via the computer.” Still didn’t quite compute with him then either (Victim of Internet banking fraud, PS#3).

The investigators in this study conveyed a belief that the ‘other side’ does not understand the issues:

Local law enforcement doesn’t understand e-crime at all and they think it’s too hard to do. But it still comes down to theft, essentially, if you’re talking about banking fraud … We would consider that e-crime covers the misuse of cards over the Internet, card numbers and that sort of stuff. And then you’ve got your straight internet banking fraud, such as phishing sites, trojans, malicious code … We would also look at inappropriate use of the internet, downloading pornography, sending pornographic emails through our email system and that sort of stuff as overall part of the same thing (PS#11).

To a bank, someone in a bank, e-crime is use of the Internet and a bogus credit card. If you talk to an ISP it’s probably bogus credit card, or someone signing up to their ISP with bogus details. And that’s what they see as e-crime. A business who sells something to someone on a credit card, turns out they’ve got a bogus credit card or for some reason they don’t get paid, that’s what they see as e-crime. However, from a policing perspective, e-crime to us takes on a whole new ball game. Those things that we’ve just described are a very minor portion of e-crime. E-crime now is much larger: it’s drug dealers who are using it as a form of communication to sell their wares. It is murderers looking to conspire in relation to deaths or hired killers. It is far easier now to steal a million dollars using your Internet and a computer than it is to walk into a soft target with a gun. And far harder to identify you. So that’s where we see the e-crime from the policing perspective (Police#4).
When explaining their understandings of e-crime, respondents naturally focused on their own employment contexts: MFID investigators focused on fraud and identity theft, CCS members focused on digital evidence analysis and child pornography, because of Operation Lodden. Theft of laptops, which is often excluded from discussions of e-crime, was important to CCS members, because of their need to utilise digital evidence analysis to identify the owner of the stolen goods (Police#5). Private sector investigators focused mainly upon fraud and inappropriate content that may or may not be illegal but was against company policy. IT administrators also often focused more on “security” and downloading of illegal or inappropriate content.

The ACPR definition of e-crime was generally understood and accepted, but not used in the routine activities of investigators. As to be expected, most focused upon legislative definitions of offences or IT standards. More important to investigators is the process of investigation, determining whether a crime has been committed and which one, what techniques were used in the offence and if there is a victim (Police#17). A third of respondents contested the definition in terms of its reference only to computers:

Well, it’s not incorrect. I’ll tell you what I don’t like about it: it uses the word computer. Digital. I prefer using the words “digital technologies” rather than computers, because with a camera or video, mp3 player, sound recorder and the memory stick that can contain so much evidence (Police#19).

Outside of law enforcement, the term e-crime is not used as much, “If someone wrote that in a report or told it to someone they’d say, ‘What do you mean?’… I think most people would think ‘electronic crime, it might be some sort of electronic misconduct that may or may not be a criminal offence’” (PS#15). In the private sector “e-crime” investigation often included civil torts
and “improprieties”. Basically, “it’s a new technique, it’s not a new form of crime” (PS#4).

Some saw “e-crime” as only the complex forms of crime involving information technology, which might be termed high-tech crime:

My idea of e-crime would be the use of computers, but I tend to think more of using a transmitting process to complete the crime. Where you’ve got a computer, but you also transmit something that’s false somewhere and as a result of that you get some sort of advantage or money or gain or whatever. Just simply storing stuff on a computer—to me—doesn’t make it e-crime (Police#15).

E-crime to me is more limited than that definition. That definition to me would include creating counterfeit documents and those sorts of things… E-crime for me tends to talk about remoteness and anonymity in transaction. Bridging distances, creating huge amounts of transactions through the use of computers, then Internet or intranet or even data-cables those sorts of things. That’s probably much more defined as a transactional sort of crime, than just… I wouldn’t call somebody who creates some false pay slips on a computer, I don’t call that an e-crime (PS#16).

In the private sector computer storage of information was central to their investigations, in consideration of computers as the new accountancy “books” (PS#15; PS#7; PS#17). The meaning of high tech crime was also disputed, since the establishment of the Australian High Tech Crime Centre.81

High tech crime is not computer forensics. A lot of people and particularly in the states say, “We don’t need a high tech centre, we’ve got our own high tech

---

81 Members disagreed over whether the AHTCC should tackle phishing or not, based on disagreement about what constitutes high tech crime (Police#19; Police#21).
crime capability”. So, where are they? “They’re our computer forensics people.” ... Computer forensics is a bolt on to an investigation, like a telephone intercept is, like surveillance is, like, it’s an avenue of inquiry, it’s, we might use computer forensics in a job or we might not. Just like the drug squad might or they might not. So that’s a huge barrier. Victoria police are a classic with that... they’d tell us black and blue that they were doing investigations, they don’t, they do computer forensics (Police#19).

People have made numerous observations to me that [phishing] is not a high tech crime, it’s just the creation of a false website. But ordinarily, your normal person on the street wouldn’t have the requisite skills to actually go up to that level of sophistication, spamming stuff, botnet stuff. Now with the Trojan keylogger technology that’s being used, I’d have to say I think that is high tech crime. And ok, it’s end user; it’s not defeating the security systems of the banks etc, but certainly the level of sophistication is significant (Police#21).

Not sharing a common understanding of “e-crime” could lead to problems within the investigation community and its clients:

This becomes confusing with, like if I was to say I was an “e-crime investigator”, which a lot of people often put me down as, then people would think I know the whole thing. I know bits and pieces of other things, but I specialise in Internet banking fraud. So, I’m an electronic Internet banking fraud investigator... Whereas an e-crime investigator is sort of saying ‘I know all e-crime’ (Police#16).

The definition did not establish clear boundaries for investigators. If not for common sense and other motivators discussed below, this definition of e-crime could lead to significant net-widening and overlapping of responsibilities:
The definition of a particular type of crime can have many, many different interpretations and it can be taken to whatever nth degree you choose to put on it. If I was to look at a definition of high tech crime or cybercrime or e-crime, I could basically say to the AFP and the jurisdictions, “Well everything that you do, we would like to know about”, because now with the advent of technology it touches on every aspect of every traditional type of crime that we investigate (Police#21).

The lack of boundaries was clear as one respondent considered that even perjury could be an electronic crime, because an offender “might have recorded a different account of events on a computer or they may well have undertaken a lawful procedure online or on a computer then given false testimony of that” (Police#14). Without further consideration, it could even potentially derail proactive allocation of resources:

Now, people actually talk about setting up an “e-crime investigation unit” at the fraud squad or here without actually knowing what they’re talking about. What is e-crime? You could say the same about what is computer crime. We’re called the Computer Crime Squad. Alright, what does computer crime entail? Where is that? Where does it end, where does it start? But no one has a definition that we use (Police#9).

The need for common understandings was clear on both sides of the road and education was key to this according to this investigator:

And whether that’s us giving them [police] the opportunity to educate or other classes or things that we can sponsor in the future, who knows. But, just having them being more informed when they’re coming for data. So that you know, we don’t have to spend three weeks going back and forth, mired in a syntax discrepancy (PS#8).
Asked what police do not understand about their workplace or industry respondents listed business processes, volume, the importance of confidentiality within their business, the value of information and one even complained police did not understand “the laws under which they claim to operate or act. Making it up and making it sound like law doesn't make it law” (PS#23). Overall, there was concern that “police have little understanding of workplace needs... They have formal authority and have little regard for the consequence of the workplace issues they leave behind” (PS#21). Not knowing enough about the other side’s working context was cited as a driver for information sharing and partnership efforts.

**Detection of incidents**

Chapter Five detailed how most e-crime incidents are reported to police rather than detected by them. Detection described by private investigators fell generally at three points along a spectrum: the individual who notices something amiss, detection through traditional, internal control systems, such as periodic auditing, and organisations that employ sophisticated computerised profiling tools to model and detect improper transactions in real or near real time. Less difficulty was reported when the latter was in place, although these tools were only available in the largest organisations.

What we’ve traditionally done is wait for someone to say ‘I got money missing from my account and I didn’t do it, where’s it gone?’ And we pick it up that way.

Now what we’re doing is we’ve got the data to start modelling what an e-crime transaction looks like so that as those sorts of transactions flow through our system we know what they look like, they’re spat out and we get to have a closer look at them and we pick them up a lot sooner and we’re blocking a lot more (PS#16).
The main problem was in terms of detecting new forms of offending, for which there has been a steep learning curve:

In terms of detecting it, a lot of the banks have come a long way pretty fast. And they’ve had to, because they’ve written off big amounts of money. We’re getting better at it, but there’s no silver bullet. Because where’s it going to go? We introduce tokens, what’s the next step? The next step’s “man in the middle”. Now, man in the middle could be a complete man in the middle attack, it could be DNS poisoning, it could be a whole heap of stuff. In terms of being able to detect e-crime, it’s a never-ending fight. We started off mainly with the phishing sites, we’ve moved to trojans and malicious code. What’s the next step in it? And as we move to decide that you’re going to have a password and also you’ve got to ring up telephone banking to get them to activate it: Crooks would then start looking at “How do I get the telephone banking pass code?” … So it’s going to be a continual battle and we’re not going to be able to detect e-crime all the time (PS#11).

Investigators are looking ahead to try and predict the next criminal trend, however there is concern that very soon financial institutions will suffer from zero-day exploits and be “pretty well powerless”. For others, this is already happening regularly:

They will go out and find something, completely exploit it, write a fix, write another exploit for the fix you just wrote, because they know what we’re going to do, and then they’ll plan it out three, four fixes down the road and then write to us and say, “Oh by the way, I figured all this out, here’s the hole, I’m releasing it in six hours. Let me know what you’re going to do for me?” (PS#9)
Every day something new has come out, there’s a new way to do something. The crooks are finding those new ways. And for us, as investigators, it's always going to be catch up, because, we can't keep a step ahead of them, if they’re developing new ways to do crime (Police#17).

Not all investigators are actively looking for e-crime (PS#8), because to do so may affect their organisation’s liability. Internet banking arguably makes it easier for bank customers to more regularly review their accounts and detect discrepancies. Many LEAP narratives indicated this was how complainants had discovered frauds committed against them. However, the introduction of unlimited broadband accounts arguably makes detection of unauthorised access to ISP accounts less detectable by the public.

When I first started...everyone was getting their dial-up accounts taken over, but I think with the introduction of broadband then it’s probably stopped a little. A lot of people are on unlimited [downloads] so they don’t notice how much they download or how much their account is used; therefore they don’t report it (Police#2).

**Under-reporting of e-crime**

As demonstrated by the LEAP data analysis, individuals were more likely to report e-crime than companies. The interviews shed light on why law enforcement faces difficulty engaging private sector companies in terms of reporting e-crime. There were two distinct groups within the respondents: those who do not report e-crime incidents to police and handle them in-house and those who report more regularly, but are selective to whom within police they report. The respondents did not think this was peculiar to Victoria. Police generally held the view cited commonly that private sector organisations under-report to police to protect the profits and reputation of
their companies (Shearing and Stenning, 1981; Prenzler and Sarre, 1998; Etter, 2000):

Well, the banks don’t report it. The banks are the main, major victims but they won’t report it, because they don’t want their shareholders to know that their systems have been corrupted and that they’ve been fleeced by their employees or people targeting them via the Internet from cyberspace. They try their best I guess, but they’ll continue to be victims, because that’s where the money lives and that’s where the—particularly the Asian gangs—that’s where they will target (Police#10).

I can only assume that it’s that small of an amount that they [ISPs] refund it and write it off and just say “Well, this will cost me more to investigate it” and not bother and just get rid of it and be done with it (Police#2).

ISPs do treat their losses as “shrinkage”, however the costs are not small according to the one, small ISP who replied to this study. At a cost of five cents per MB, the 5GB in fraud-related spam he receives daily costs his company over $90,000 per year.

We are inundated with surplus bandwidth as a result of spam whether generated directly or indirectly via a worm virus. We have had to acquire and install a separate server and software configuration in order to reject unsolicited (spam) emails. This of course costs us both in hardware, network contractor fees and ongoing bandwidth but at least it avoids our customers’ postboxes getting blocked up needlessly. In this regard, we are “victims” with legitimate claims for recovery of costs. But to whom do we submit our claims? Identifying the perpetrators is the problem - most of whom emanate from overseas countries where “it’s anybody’s game” (ISP).

Police also argued that beliefs that “they think they can deal with it internally” (Police#19) contribute to under reporting. Others argued that most
of the corporate world does not know that the Computer Crime Squad exists or that Victoria Police has a capability to conduct forensic computing (Police#2). Reimbursement of funds by financial institutions was credited for individuals deciding not to report formally, even though they may have already contacted police (Police#6). Private sector investigators took a different view of the problem, focusing on their negative perceptions and experiences of police e-crime investigations and court outcomes.

People will only tend to report things to the police if they can nominate a suspect, when you talk about fraud. For example, the banks would have a whole lot of credit card fraud that goes on and they’ll say “What’s the point of reporting that to the police, because we’ve got no offender, no suspect to refer?” … A lot of fraud is not reported because we don’t have a suspect (PS#4).

When investigation was unlikely to recover stolen funds then the cost of an investigation was seen as throwing good money after bad, “We’ve lost our money cold. Is it going to help us get our money back? No? Then why would we spend two more seconds on it” (PS#4)? Court sanctions were often considered lenient and not worth pursuing. Involving private investigators instead of police also retains control for a victim company, due to the financial, contractual relationship (PS#17; Police#1).

Contrary to Chan’s (2000) findings, one IT security officer detailed how his organisation considered involving police until their own internal investigation determined that an incident did not involve an outside perpetrator (PS#12). Knowing an offender contributed to under-reporting (PS#15) not reporting as argued previously. Also contrary to Chan’s finding that superior IT knowledge contributed to under-reporting another IT
administrator attributed non-reporting by his organisation to lack of IT knowledge (PS#7).

Not everyone interviewed for this study was averse to reporting e-crime. A longer-term philosophy focused on building police intelligence through reporting:

My philosophy is I will always tell the police. The problem from the policing side is that there’s only two speeds, go or whoa. They don’t really have a mechanism yet for recording for information’s sake. So that they can build a profile themselves, and that is where I think there is a big gap. Because if they could do that then we could actually batch jobs once a month. “Here’s our figures for the month. These are the one’s worth investigating, but these ones, the money’s gone, it’s in Minsk” (PS#16).

Also matters tended to be reported when private investigators cannot investigate further themselves due to legislative constraints:

A matter gets reported to police once the private individual is stopped by issues of access or privacy. We do it; we go along to a partner and say we cannot do anymore on the case, because we can’t access the bank accounts (PS#15).

In many instances, incidents such as phishing were reported regularly to AusCERT, because of the effectiveness of the network of Computer Emergency Response Teams globally. Those that do report described avoiding sending e-crime to uniform state police, instead focusing reports to local CIUs or the newly formed AHTCC (PS#11).

Now predominantly with state police forces we deal with the local CIU units rather than uniform Although on occasion with some of the smaller jobs, they
will go to uniform, because it’s a good training ground for them anyway; and sometimes we get quicker results by them going to the uniform branch than to the CIU when they’re relatively small (PS#1).

Bank investigators stated they would not report to the Major Fraud Investigation Division, “because jobs can sit for three or four years before they’re actually brought to a conclusion” (PS#11). This was similar for the Computer Crime Squad, “We don’t get a lot of reporting. I think primarily because of that reason, because of our back log, there’s no chance that things are going to get looked at” (Police#2).

Police are not the only ones requesting reports of e-crime. Software developers ask victims to report to them:

We’re always looking to gather information during a malicious code outbreak and we’re asking other companies to report to us what kind of activity they’re seeing. Send us maybe some logs. Cybercrime is one of the most under reported crimes, because once you let somebody know you’ve been hacked, customers start to question the integrity of your software. We have no choice; we’re going to get blasted no matter what. We know we have to be on the front. But, we ask partners, we ask a lot of companies to help us during an outbreak to share information with law enforcement, let’s go find the bad guy (PS#8).

Concern was expressed that reporting to some initiatives may be used to feed commercial services that would then be sold back to the reporting organisation:

We have some concerns in relation to that, in that some of the people involved in that will go in and grab our information out of there and then offer to give it to us. But they’re prepared to give it to us if we sign up to an ongoing agreement. They’ll do all this sort of stuff for us, but we have to pay
...[and we shouldn’t have to] because it’s not their information in the first place. They’ve only retrieved it off a site. We’ve got issues around that (PS#11).

The pilot survey of the private sector asked specifically about other factors, suggested in response to Chan’s (2000) work, that may affect decisions to report or not report e-crime to police (Item C8, Appendix G: Private sector survey). Each item used a five-point, ordinal Likert-type scale ranging from Not At All Important (1) to Extremely Important (5).\textsuperscript{82} The seriousness of the incident was the most important factor in the decision to report to police (see Table 6.1). A third of respondents did not consider shareholder views at all important, ranking it low; however many respondents did not come from organisations that had shareholders.

\begin{table}[h]
\centering
\begin{tabular}{|l|l|l|l|l|}
\hline
Rank & Factor & N & Mean & Std. Deviation \\
\hline
1\textsuperscript{st} & Seriousness of incident & 31 & 3.71 & 1.16 \\
2\textsuperscript{nd} & Company policy & 30 & 3.33 & 1.49 \\
3\textsuperscript{rd} & Suspect worked for company & 30 & 3.23 & 1.61 \\
4\textsuperscript{th} & Potential positive media reporting & 31 & 3.23 & 1.48 \\
5\textsuperscript{th} & Advice from IT staff & 30 & 3.13 & 1.22 \\
6\textsuperscript{th} & Advice from police (ie prior to official complaint) & 30 & 3.10 & 1.45 \\
7\textsuperscript{th} & Measurable loss & 31 & 3.10 & 1.47 \\
8\textsuperscript{th} & Mandatory reporting requirement & 29 & 3.03 & 1.59 \\
9\textsuperscript{th} & Potential negative media reporting & 30 & 2.97 & 1.47 \\
10\textsuperscript{th} & Partnership or alliance with police & 30 & 2.73 & 1.44 \\
11\textsuperscript{th} & Advice from security consultant & 30 & 2.70 & 1.39 \\
12\textsuperscript{th} & Inability to measure loss & 31 & 2.61 & 1.52 \\
13\textsuperscript{th} & Shareholder views & 29 & 2.28 & 1.36 \\
14\textsuperscript{th} & Past experience with law enforcement & 30 & 2.27 & 1.20 \\
\hline
\end{tabular}
\caption{Ranked importance of factors in reporting decisions*}
\end{table}

* Calculated from responses using a five-point Likert scale.

\textsuperscript{82} These items are referred to as Likert-type items, because Likert (1932) intended his scale to be a summation of all the items, not an analysis of individual items (see Clason and Dormody, 1994: 31). Here they are analysed individually.
Where Chan (2000: 324) found no difference in reporting whether the offender was internal or external, these results suggest it is an important decision making factor, possibly due to ability to identify a suspect. Internal IT staff advice was more important than police or consultant advice (see Table 6.1). Having a partnership or alliance with police ranked only tenth in importance. Surprisingly, given comments of private investigators about the influence of their past experiences with police, this was the least important factor in deciding whether to report to police.

Under the Australian Stock Exchange Listing Rule 3.1 on continuous disclosure, companies listed publicly have a duty to disclose security incidents (Deacons, 2000). However, the question is still raised, “if you’re a listed company and you’ve suffered attacks, do you tell the market” (Police#19)? Another officer commented, “It’s better to work cooperatively with them than to try to wave a big stick at them. If you try and wave the big stick you don’t foster any sort of cooperation, which is what we want to do” (Police#18). However some respondents argued that unless there is a mandatory reporting law, banks and other institutions would continue to not report offences unless it suits them. The recent Parliamentary Inquiry into Fraud and E-Commerce recommended mandatory reporting of fraud (DCPC, 2004: 227), although concerns were noted about the enforceability of such legislation.

**Reaching “a sympathetic ear”**

Police were candid about the importance of finding “a sympathetic ear” (Police#9) when complainants attempt to report e-crime. “It’s like catching a lift, you know, the doors open, if you’re lucky you get the elevator, if you’re
unlucky you get the shaft. It’s no different in the police force” (Police#9). Police have considerable discretion to dismiss reports of an offence.

Well, [under-reporting] starts at the station, the uniform station, where people walk in and say I’ve got this to report and they really get fobbed off. And there’s probably a lot of reasons for that. A lack of knowledge about legislation. Or maybe the uniform guy has knowledge that, “Look, this isn’t going to go anywhere, because you sent money to Latvia via [a money transfer company]. It’s just not going anywhere, sorry there’s nothing we can do”. So there’s no report taken (Police#3).

As an example of not knowing the legislation, a woman described an incident to me that fell clearly under amendments to section 21A of the Crimes Act 1958 (Vic) for cyberstalking, because of publication of materials on a website, yet she was initially told no crime had been committed and it was not recorded. When she returned with the Act in hand to point out how the offence applied the matter was recorded. Few individual complainants would be knowledgeable enough to do this and would simply accept the word of police. Another officer advised, “You’re quite entitled to go to a police station and get them to fill out a form. They might say there’s nothing we can do about it, but you can say, ‘No, I want a report done and you’ll take it. If you don’t take it, I’ll complain’” (Police#9).

Difficulty reporting incidents can also hinge on the attitudes of police about whether it is their job to investigate such matters.

I guess one [factor] would be the investigator that gets it, depending on how keen they are, I suppose. A lot of people out in the real world, I know when I was out there being a normal copper will hear ‘computer’ and just switch off. “It’s too hard so I’m not going to do anything about it”. Others will chase it to the end of the earth to get a result... There is a lot of—and it’s not a blight on
the coppers who are there, because a lot of them are very computer literate now, everyone is—but there are lot who just switch off when you say there is a computer, then it’s too hard. If it’s an Internet computer then, “Nah. I’m either going to get rid of it to computer crime, to a CIU or just write if off”. And that’s unfortunate, but that’s the way it goes (Police#2).83

I would suggest that it even happens at the national level. And I think it comes down to a culture of policing, they’ll do anything to flick past a job. Whether they’re working on a traffic matter or high tech crime matter or anything in between, anything they can punt to someone else, any one that they can say “Oh, that’s Spam, ring up the Australian Communications Authority” (Police#19).

Another victim of cyberstalking who reported her incident to Victoria Police and the AHTCC experienced exactly this sort of handballing. Despite her Australian citizenship, she was advised by AHTCC to report her matter overseas on the basis she appeared to be a national of another country (PS#20). The response might have been affected by the victim’s attitude towards the case, despite reporting:

I’ve been thinking about this for the last seven months and I would want to know who the person is, without necessarily bringing the person to court. Because my decision on whether or not to pursue this as a case will depend on who the person is (Victim of identity theft and cyberstalking, PS#20).

Police were concerned that people would withdraw complaints down the track not making investigation worthwhile:

It’s harder to be able to say you can dedicate all these resources just to get stuff removed off the web and that’s it. It’s probably not a police role to do

83 These comments reflect those made over twenty years previously (Detroit Free Press, 1983).
that. That would more involve people in the public sector and people who
own all these dating sites and singles sites and all that sort of stuff being able
to have the power to say to the victim, “Send us all your details and we’ll take
it off”. Rather than the person going to the police, making a report, and the
police doing the investigation, getting it taken down and then the person
going "Well, I’m happy with that". That’s a lot of wasted resources in my
opinion (Police#2).

The discretion to not record incidents exists because of the
evidentiary model of reporting employed by Victoria Police
(Carcach and Makkai, 2002: 2). Under this model, police have
to be convinced there is sufficient evidence of a crime to
record it;\textsuperscript{84} and some clearly choose not to be convinced when
e-crime is involved, which impacts on the dark figure of e-
crime.

The interviews also revealed a tendency among investigators to belittle
certain victims of electronic crime, blaming them for their own victimisation
when the investigators were not in a position to investigate incidents
successfully. Comments were aimed at organisations that did not have
adequate IT security — “Well, it’s no wonder you’ve been hacked… And
that’s all that happened to you?” (Police#4)—and “fools” deceived by
offenders despite public education campaigns (Police#6). Victims were
afforded the least respect if they had fallen for the advance fee scams known
as Nigerian scams. “Nigerian scams are really an education thing. If people

\textsuperscript{84} The Victoria Police Manual (2005a: 108-3: s1) states the policy as “Any police member
receiving a report of an incident must make sufficient initial inquiries to satisfy themselves
that a crime has been committed or not. Where the facts indicate that a crime has been
committed, complete and submit all relevant LEAP reports, containing the best quality
information available at the time.”
are really that silly to hand over money…” (Police#17). Private investigators were aware of this attitude among police: “the attitude is ‘Well, if you’re stupid enough to get involved, why should we help you?’” (PS#11) but also displayed the attitude themselves, “That’s an education thing. Trying to protect stupid people from themselves” (PS#16). And, “if you’re dumb enough to send your money across to Nigerians, you deserve what you get” (PS#15). Similar comments were directed at victims of phishing (PS#6) and illegal online gambling, “Look, anybody who gambles, puts their money into that kind of thing, then they deserve to lose their money” (PS#4).

Thankfully, this was not an attitude taken by all police or investigators:

Irrespective of whether it’s silly to disclose details or not, it's still an offence. I mean that’s what deception is all about. It's all about trickery; it's all about false pretences… It's going to happen to some people, it's not going to happen to everyone, but it will happen to some people. And when it does happen to some people, it needs to be dealt with (Police#8).

**The model computer crime offences**

On 6 May 2003, Victoria repealed the computer offences of unauthorised access to a computer under Section 9A of the *Summary Offences Act 1966* and replaced them with new sections in the *Crimes Act*. Identification of an offence is central to initial reporting as discussed above and later charging of offenders. Respondents were asked to comment on the new legislation, particularly to highlight benefits and any difficulties they had with it. Six of the police respondents, all outside of CCS, had not seen this legislation before.

Police are pleased that there are now appropriate offences for sabotage of critical infrastructure, including computer networks:
What would you have really done if someone had gone in and taken out Telstra’s computers and Australia went into the black? No telecommunications all of a sudden. How huge an offence would that be in terms of political rebound, public outcry? Be huge. What would you give him? Maybe a criminal damage? Before, that’s all you could have done. You could have given him under the old act, summary offences, unlawful access (Police#4).

Extra-territoriality provisions that permit prosecution of offenders as long as there is some connection to the state of Victoria is another important benefit of the new legislation (Police#4). Providing indictable offences was useful to police, permitting them to apply for search warrants. Police desired that the summary offences in section 247G prohibiting “unauthorised access to or modification of restricted data” and section 247H “unauthorised impairment of data held in computer disk, credit card or other device” were also indictable offences for this reason. Section 247E that prohibits “possession of data with intent to commit a serious offence” was seen as the electronic equivalent of “going equipped to steal”. It was considered almost useless:

It would be pretty near impossible to prove [that] you’ve got that virus to allow you a backdoor entry into this computer, so you could get financial data so you’re going to commit some huge robbery (Police#4).

Police did not believe that the new offences adequately cover the type of offending that they regularly encounter, such as identity theft or theft of intellectual property (Police#5):

---

There’s no offence for stealing your information, which is where your crimes start. And that’s where this legislation lets you down, because you should be able to [charge with] “did steal information”. We’ve had matters reported here where people have had their computer program that they’ve worked on and patented for five years stolen and you go, “Well, did they put it on a disk that belonged to you?” And they go, “Why?” “Well, I can charge them with the theft of the disk. I can’t charge them with the theft of the twenty million dollar computer program” (Police#6).

Police believed the definition of property would need to include intellectual property to address this.86

To make it easier for any of this, they need to change the definition of property. In that property has to change to intellectual property, to include it. Has to be included, because to me this doesn’t cover identity fraud, which is… where are you going to get most of your information for identity fraud? Other than dumpster diving or a letterbox? You’re going to get it online. And you can have it, basically, because it is not covered in here. Can’t steal information, because it is not in here (Police#6).

Of course, some were emphatic in warning against this amendment:

Theft of data? You thought Operation Lodden—child pornography—was big? Man, theft of data would be monstrous. How would you keep up with it? Every Joe Blow – go to the bank [for example], employee pinches something, bank: “Theft of data”. Bloody hell (Police#5).

There was a fairly consistent view among police that the model computer offences were not going to receive a lot of police attention. In the Computer

86 See note 95 below for discussion of whether the definition already includes intellectual property.
Crime Squad, there was debate about the applicability of the new offences to incidents that had been reported and comment that incidents should be referred to other agencies even if applicable; “you sort of get encouraged to ‘Well we’re not, we can’t do that, send it off to that mob, they can do it’” (Police#13). Elsewhere, the offences were considered “the most confusing amount of mumbo jumbo that I’ve ever come across when it comes to something that could be explained simply” (Police#6).

I’ve never actually prepared a charge under them, because, yeah, it would take a fair amount of time and effort to actually delve into them and see if any of the offences were actually appropriate in the circumstances, because we generally, normally, go for the money offences and these are seen as more secondary or tertiary down the scale. So you’re either chasing the deception that’s caused the loss of money—so yes, you’ve got a value on the end of it—or a financial deception or a theft or a conspiracy that all work together and there may well be offences of this nature that would also be preferred, but you’re going for the big ticket item: this is more lower down the scale. And if you couldn’t get them on anything else, well, you might look at them as something like that that was a third best sort of view (Police#10).

These are not the “big ticket” offences with which offenders will be charged. Even though the model computer offences introduced higher penalties than existed previously under the Summary Offences Act, respondents did not believe this was commensurate with other offences that would be used instead.

I think the penalty needs to fit the crime. If you can fit it under another statute then why can’t you move the penalty up? Or increase the penalty, so that people start using the cybercrime law. You know in my view, to really deter people in cybercrime, you need to use the statutes, right? “We’re going to prosecute you under this statute” and the only way you’re going to do that is
if the penalty is consistent with the other crimes that they’re trying to charge them with (PS#8).

Section 247B would not be used. Instead the “serious offence”—for instance OFABD—would be charged. In fact, police respondents went so far as to say that other police are “frightened” even “terrified” of the offences (Police#13):

Well, because they’re not brought up with it—it’s not necessarily taught at the academy—they don’t have an understanding of it, they look at reams and reams of definitions, “Where does it fit? What’s appropriate?” They need to go away and seek some fairly high profile legal advice in relation to whether they’d actually would be able to prepare a charge like that. The person that it is given to, maybe out in the stations, would look at it and say, “God where did you get that from?” It’s like from the dark side of the moon. It’s on the books but it’s very exotic (Police#10).

I think that’s the way we interpret it. What’s the real offence? Sure they’ve used a computer to do this and perhaps they’ve gone away from this particular Act or section of the Act. The offence is here because it’s been an unauthorised use of computer. Another part of the offence being he’s defrauded somebody: “Oh, we'll run with that”, because this is too scary for me to deal with. And I would hope now that we are starting to get enough people who are experienced enough to say “Look we've got the fraud, we’ve got the unauthorised possession of whatever it is here, let's give them a deal” (Police#17).

Lacking precedent and established case law to support a prosecution, police were loath to bet on this new legislation.

Maybe there's something in here that's quite close, but not quite close enough. Are we going to win it? Any element of doubt comes into it prosecutors are going to say, “Well, we're going to pull that”. So, it is out the door and we
haven’t got it in. So we haven’t got something to go on before, we haven’t got that precedent. We’ve got them on this before, using this [other] section, will we get this next person on that (Police#17)?

It was suggested that the format of the legislation with its many definitions would put police off using the legislation and might need redrafting. In particular, definitions of “impairment” and “modification” were considered imprecise; “it could mean anything to anybody” (Police#6). Police were discouraged by the quality of legal advice provided by police solicitors and suggested that legal research should be outsourced:

I’ve had poor experience with getting changing advice, because the advice is poorly researched, I suppose. They’re doing it off the top of their heads, maybe so they can comply with the workload. I genuinely don’t think we get value for money out of our solicitors here. Shouldn’t say all of them, because I believe there are some great ones…Changing advice and then almost refusing to do legal research when you go in with a question: I’ve had a couple of times of getting advice of “Don’t bother”, when I’m simply saying can you look up that bit of legislation? Poor advice where I’ve asked about offences and they’ve come out with very simplistic answers off the top of their heads. Maybe gone to the book, and said “Yes, that offence applies”. Oh well, I went in with a question of “what offences?” Six months later down the track in the investigation I’ve come up with another half dozen offences all of which should have different points of proof and different elements of evidence that I should have been collecting for the whole time. If you outsourced this, they would be liable for the advice they gave. It would be written and they would research it. They’d be paid to do that. They would do it. So I think you’d get a better job done if you outsourced it (PS#7).

At the time of interview, police were unable to find consistent advice as to how to apply these offences:
I rang the OPP to get some direction on what they wanted in the summary and in the charges, and they went "First one we've heard of, don't know anything about it, haven't even looked at it" (Police#2).

In the private sector, half the interviewees did not know of the new offences. Some suggested this was because private investigators generally do not suggest to police what offences to charge when they report incidents. The model computer offences were seen as a last resort, behind more substantial offences (PS#1; PS#14) or because “criminal offences tend to escalate a dispute whereas we’re always looking for those killer things to resolve it” (PS#17). Interpretation as to the applicability of the offences was again an issue:

So as soon as they get money out of the system, it takes you outside of this, and you’re looking then at obtaining property by deception or theft… So this has no application unless they haven’t actually been successful at getting data out. So this is to do with manipulation of data prior to, or unauthorised access and that sort of thing (PS#4).

However, difficulties with legislation was accepted more in the private sector,

I think the trouble is when you’re crafting legislation like this, sometimes it is hard to anticipate what the next sort of strain of crime is going to be. I mean, we would not have anticipated botnets, probably. You know, technology is always going to move faster than policy is in any case. So usually by the time that you implement a bill in legislation then it is out of date (PS#10).

---

87 Excludes interviewees who learned about the legislation through the course taught by the researcher.
Reporting protocols and acceptance criteria

Examination of the LEAP data revealed comments in the narratives about unauthorised access incidents:

This type of offence is not investigated by Victoria Police… Police and ISP have an understanding that if the victim can prove that they are not using the download time then the victim is reimbursed. Not a police matter (Incident narrative, March 2004).

This statement surprised me, as Victoria Police was the first police force in Australia to investigate hacking to gain unauthorised access to other people’s accounts. Why would police not investigate an incident—or even a whole class of incidents—where presumably a crime had occurred?

The answer lay in a new reporting policy. Since May 1998, the Computer Crime Squad has been the liaison point for Internet Service Providers. In a submission to the Parliamentary Joint Committee on the Australian Crime Commission, Victoria Police detailed how the Computer Crime Squad instituted an “ISP Fraud Reporting Methodology”, which required that ISPs provide an evidence package to Victoria Police whenever requesting police investigation of an incident:

in the 1998-1999 fiscal year, the number of requests for investigative assistance soared due to the sudden increase in the number of frauds being committed on Internet Service Providers (ISPs) and/or their clients…On identifying this issue, the CCS immediately instituted a national push to hold ISPs responsible for their lax on-line sign-up procedures and client account security. As a result, after several meetings with the top three Internet Service Providers and the Internet Industry Association (IIA), the CCS developed an ISP fraud reporting methodology, which in essence has held ISPs to account,
and made it incumbent upon them to provide an evidence package with each report made. Consequently, the previous rising tide of reported ISP related frauds, and therefore the associated request for investigative assistance was stemmed and the number of reported frauds dropped (Victoria Police, July 2003).

The number of reported frauds involving unauthorised access dropped. However, this should not be taken to indicate definitively that the incidence of ISP-related fraud decreased, but instead that the reporting dropped due to these new reporting requirements. The underlying problem was explained as follows:

Well, there wasn’t an over-reporting; there was a reporting by the wrong group, by the witnesses instead of the actual people responsible for… that were actually the victim. Not that we can’t take a report from someone who’s reporting a crime against someone else, but generally it’s not good business sense and it’s not good legal sense when you don’t have your victim reporting “We’re the victim of a fraud. And here’s all the evidence that says we are” (Police#4).

The protocol indicates that an ISP, merchant or bank involved is to be considered the victim not an individual citizen who reports a matter to the police. In fact, it became clear from the incident data that these crimes were still reported to Victoria Police, however police were refusing to investigate them, unless the ISPs, banks or merchants themselves reported them, in the format demanded:

---

88 See Appendix Q: Forms for ISPs and online merchants to report incidents for the forms that are required. Note the “Access details” and “Application Validation” sections, from which police might hold complainants responsible for lax security.
The manner in which this matter has been reported does not follow the protocol. The victim in such frauds is ISP, even though a member of the public may be out of pocket, it is a deception committed on ISP and it is up to them to report the matter. In practice, what happens is that ISP advises people to report the matter to police to try and get in the back door so that the department ends up paying for the reverse CCRS etc. This is in direct contravention with protocols in place between communications carriers and the computer crime squad/fedpol (Incident narrative, Feb 2001).

This narrative suggests the underlying reason for discouraging the reporting of unauthorised access incidents was the potential for Victoria Police to incur investigation costs, such as Call Charge Record Searches (CCRS).\textsuperscript{89}

Advised by CCS ruling on such matters now stands as follows. Victim in this matter is Internet service provider. All matters reported by them go to the computer crime squad. The issue of any unauthorised use of Internet as reported by the victim in this matter, becomes a civil issue between her and ISP as in this case. All moneys [sic] owed by her... is [sic] part of their contractual agreement. At this point nil further enq's to be made as nil offence disclosed. Req matter to be marked completed (Incident narrative, Oct 2000).

Further, the narratives suggested that Victoria Police often redefined the incidents as “civil matters”, because there were contracts in place between the account holder and the service provider. The police reasoning was further explained:

ISP's used to take the view that “No, our client’s defrauded because someone used their account. So we’re charging them the money”. Look, we don’t have a bleep [sic] that they have a contractual agreement with their client, that

\[\text{\textsuperscript{89}}\text{If police request non-interception help, termed “agency specific delivery capability”, the cost falls to police under section 332L of} \text{Telecommunications Act 1997 (Cth).}\]
their client is responsible for any usage of the account. That’s fine, that’s a contractual agreement. Legally, the client provided no access, he didn’t provide this unknown person with the ability to connect to there, he wasn’t the person who was therefore deceived into supplying it. Ergo he’s not the victim. He is just, he is the same as, say, your credit card. And we apply the same to merchants: you happen to hold credit card ABC, now unbeknownst to you someone gets on the Internet in America and they buy a dozen eggs from Wally the egg farmer, and they put in their credit card ABC. So your account’s debited $200 for the good eggs, they were. Are you a victim? Let me tell you, you’re not a victim. Were you deceived? Did you even know the transaction was going on (Police#4)?

The basis for this reasoning by police is the definition under section 81(4) of the *Crimes Act* (Vic) that a computer may be deceived. This provision was introduced to account for offenders who deceived automatic teller machines to dispense cash they were not entitled to receive (see *Kennison v. Daire* (1986) 160 CLR 129). Even though as an account holder who has had money stolen from their account, you may feel victimised, the police insist you were not the victim and you are not out of pocket:

No, you’re not... No, you’re thinking you’re out of pocket. And when you look at your statement, you go, “Geez, I’m out of pocket!” But, you’re not, because with all online transactions it is a merchant beware. You complain, your money is refunded by the bank, immediately. They have no right to keep your funds. You’d go straight to the banking ombudsman if they decided they wanted to question you about it. So, number one, did you provide anything? No, you didn’t. Did you even know what was going on? No, didn’t. You were deceived? No, you weren’t. How can you possibly be the victim? What you are is, you are the witness who happens to be the holder of that credit card number. So you make a statement saying, “No, this transaction’s unauthorised, it’s not my transaction”, the bank refunds your
money because it wasn’t you, and in fact: you see, you say that I’m out of pocket $50, but you’re not, you didn’t pay anyone any money. The bank sent $50 to them, and then took it from your account (Police#4).

This logic becomes more difficult to follow, especially when the victim thought they were the victim of theft, not deception. Regardless, the protocol was further justified as a means of “assisting business to come to terms with the reality of fraud and electronic communications and protect their clients” (Police#4). Grabosky (1995) refers to this practice as “conscription”, whereby law enforcement coerces organisations to engage in certain practices for the benefit of law enforcement. In this way it reflects a problem-oriented policing strategy (Felson, 1998: 137-8) and “third party policing” (Beurger and Mazerolle, 1998):

We cannot as an individual say to them, “Go and do this”, but as a collective, we can say, “We are going to treat the law exactly as the law says and that law says this. Now you need to deal with your client, because your client is not a victim. Your client is our witness. You were the victim and when you’re the victim we want you to provide us with this package of evidence, because all of this evidence happens to be in your possession”. So then they need to put in place the ability to provide this evidence to the Force, rather than—and in the case of telecommunications, telecommunication companies have the right—to expect expenses to be paid by the forces requesting information. Why are we paying, why should a Force pay for information when they are the victim wanting to report an offence? No logic (Police#4).

In contrast to calls for greater reporting, many police reported that they wanted to actively discourage reporting because of their backlogs:

We’ve taken a fairly hard line with the banks. And whilst we haven’t got the authority to say “No, we are not going to investigate your matter”, we have
got the authority to prioritise it and stall it – which essentially means the same thing. And as a result, to get out backlogs down, we’ve taken this fairly pointed and almost ruthless action, which has cut off the opportunity for any close networking or practices that might allow mateship to get a job investigated, because there are certain criteria. Investigations are no longer done for who you know – they’re done for a criterion. There’s no such criteria, to my knowledge, in divisions. So if I happen to know someone who is an ex-police officer and working in a division, that is more likely to get a result. That’s why they do it. And secondly, our jobs take a long time to do. And if we’re doing somewhere between 40 to 45 investigations a year, that’s not a lot. So if you’ve got the banks all vying to be one of those 45, they haven’t got a lot of chances. They’ve got more chance of going outside, to the regions, and getting part of a job done. But that’s a direct result of our stance and as a result I know that the amount of investigators I’ve got will only allow me to do X number of investigations. Doesn’t matter how often I move things around or change it – the fact is, if we don’t take that line, then the amount of jobs waiting just gets bigger and bigger. It’s ridiculous. And so, we just put them on hold or say “Don’t send them” (Police#14).

It was a similar story for members of the small Computer Crime Squad:

I think in those days, and I got just the end of it, you had to promote the squad a lot more to get the work. Unlike a lot of places in the early days you had to sell yourself to say, “Look we’re here, we’re a role. We can do this, we can do that”. We don’t have to do that anymore, we’ve got more work than enough. It’s almost a case like, “Go away, we’ve got enough now”, you know? We don’t have to be as proactive to get the work here. We no longer have to justify ourselves. I mean, one of the reasons a lot of minor investigations were getting done, even though they were electronic investigations, they were relatively minor things like, might be just a hundred dollar Internet fraud, which we were getting investigated at the squad level. And no other crimes of that seriousness, and I use seriousness looking at the
dollar value again. In this building, that would be investigated normally at uniform level. And we were just doing it to justify our existence. No longer required now. It’s beyond that (Police#9).

However, other police were more forward in noting that this reporting methodology does not often succeed in directing the correct entity to report the matter.

John Citizen might report to the police that he’s the victim but he’ll get the constable at the counter saying, “Well actually you’re not the victim, it’s the bank so you get onto the bank and get them to report it to us”. But that won’t happen: the bank are going to report the big issues where they want us to try and recover something (Police#10).

Individuals who are unable to convince financial institutions that they have had funds stolen from their accounts must turn to the Banking Ombudsman, as was the experience of an older woman interviewed for this study, who had $1000 stolen from her account (PS#5). The Telecommunications Ombudsman handles similar disputes with Internet service providers. In the meantime, what happens to the offender? They fall through this crack in the system.

**Evidence packages**

Requesting “evidence packages” with reported crime is becoming a more widespread trend than just at the Computer Crime Squad as noted by most of the interviewed private investigators:

There is a devolvement happening between the law enforcement bodies and the private industry of people such as myself, where they’re saying to us “We have so much street crime we don’t have time for this. Prepare a brief, give us a brief, if we like your credibility all we’ll do is go and pick up the offender and bring them in and question and charge them (PS#1).
At least five investigators interviewed in this study already provide partial or complete briefs of evidence to police when they report matters. Some investigators saw that packaging investigations for police was their bread and butter:

You’ve got to box it all up with a lovely bow on top for them. That’s what you’ve got to do. That’s why I exist, to do that for them (PS#15).

It was often a calculated decision to improve the probabilities of achieving police attention for a case:

I didn’t have to do it, but in a way I was getting value for my bank, because I was working for the bank then... And don’t forget I did that voluntarily, because I wanted to get her. And so I did what I thought was appropriate to start the ball rolling. I gave them virtually a ‘lay-down Misère’, and they said, “Yeah ok”, so they went and all they had to do was front up this one, this one and this one. Here’s a copy of everything. Went in front of her and she admitted it... Well, see I knew with that case, they’d probably get lots of those little ones. So, what makes them work on the little ones? It’s a lay-down Misère. Or it’s near enough (PS#13).

While for others, it was in recognition of the responsibilities and limitations of public police and acceptance of their own corporate responsibility:

[Police], because they are a government agency, they are the resolution process for government. So they have to do all the government work, there’s nobody else to do that. There’s one draw on their resources that’s non-negotiable. It has to be there. But, I think that they should also be the resource who looks after corporate fraud where the company defrauded doesn’t have the means to be able to do much else about it themselves. So the ones that are absolutely gutted by the incident. They’ve got to be able to help these people.
We’re a big bank and we make a whole lot of money. We can always throw more resources at it. And perhaps there is a very, very sound reason for saying that those institutions or those companies that have got the means should do a lot more of the grunt work and prepare and build the brief for the police: So that the police are not tying up a huge amount of resources for something that they don’t necessarily have to and then they can devote their resources to those non-negotiable state problems (PS#16).

Police have actively encouraged this requirement for “packaged investigations” from complainants when reporting matters:

As a result that’s made life a little bit easier for the police. And it’s something that maybe in future we’ll demand rather than hope that we get, because of our limitations (Police#10).

The clear benefit for police of this process is a reduction in their workload:

I think it’s hardly a partnership… But it does get around a lot of "Well, give us your report" and back and forth for six months until everyone’s got all the information. The bank knows exactly what’s going on. They can go bang, sit down with the investigator and all of a sudden, coppers are clued up in a day, and away they go. I think there are definite positives in it from the police point of view, probably not from the public sector because they got to do all that work, and if they can avoid and have the coppers do it then they don’t have to pay for it. So I guess that’s where they’re going to look at it (Police#2).

There appeared to be three lines of reasoning behind the call from within Victoria Police to make provision of an evidence package at the reporting stage mandatory. The first came from a self-confessed disinclination for the investigative process by some police:
Because of the slothness: I suppose it’s so slow, our ability to actually put all this stuff together, because we have to identify where it is. And if it is archived the banks have to go away and get it and if they can find it, and then we have to prepare an affidavit in great detail and then a warrant attached to the affidavit and then send a notice off to the bank to say “This is the stuff we’re looking for and we’ve got an affidavit and a warrant here. Will you go and source that material?” And they might come back in a few months and say, “Well we’ve found most of it come on down and get it”, so we and go and have the warrant issued and then we go down and execute the warrant and give them a copy and then bring all the stuff back and then we sit at our desk and we might type it into the TAYSIS system\footnote{One of the seven databases used at the Major Fraud Investigation Division.} as exhibits and it’s a laborious task (Police#10).

I want auditors to have gone through a case before I go there. So if I’m going to have a look at a job I want well presented spreadsheets, images of hard drives, I want everything that [they] can provide for me, using all of the resources that they’ve got. As long as the victim has got the resources to do that… I would love to see more of it, so when I get it I don’t have to go and do all the mundane stuff or even try to do the stuff [for] which I don’t have the skills (Police#7).

The second came in response to the above attitude:

I don’t know how policing has been allowed to get away with it for so long, and it’s not just Victoria, it’s all states… I just find it outrageous how policing has been able to: they used to investigate crimes, why aren’t they now? If I was a big company—and the banks are a classic—the police won’t touch their matters. They won’t touch them unless they’ve got witness statements and this that and the other. And I just, there’s police, particularly in the states, that are absolutely cash strapped. That’s the way it is. But I just find it
unbelievable now how they just don't do investigations unless it's handed to them on a platter and then they decide. It opens up all sort of issues for the private sector, particularly in the trading environment, because bank staff or any sort of staff aren't trained to take a witness statement properly, so there's no hearsay in it and it's actually got evidence in it, it can actually be led and go with a brief. I just find it unbelievable. Fraud squads just knock back stuff all the time. It's just gathering more steam. It's not community policing (Police#19).

If, we had things presented to us that were already completed to a certain respect, we wouldn't have to try and get work out of people who aren't going to do it. If I went to my forensic accountant in my squad and asked him to look at these accounts, tell me where the money's gone between and present me with a statement I would be waiting, I think at the moment about two years to get that back. And that's after waiting for the banks to get the documents, for me to execute the warrant and try to put it together. So, it's pretty well an impossible situation (Police#7).

The other rationale in support of this process was to avoid corporations taking advantage of Victoria Police:

Law enforcement obviously can't do everything. Particularly when it comes to say a large network where they've been hacked or something, you certainly just can't expect law enforcement to come and audit the system, extract all the evidence and put the package together. I mean, ideally that would be nice, but then you get the situation where law enforcement are taken advantage of in a sense (Police#3).

Different companies would have different capacities to comply with this requirement (PS#11). Currently, police judge when a company should be required to meet this condition. There was a strong belief that private
investigators who could not produce evidence packages of sufficient quality for police would get squeezed out of the market place informally as police would refuse to accept their jobs. This reflects the privileging of “the market” described by Garland (1997).

However a senior police officer urged caution in regard to implementing this sort of reporting requirement:

We need to be careful because Victoria Police, and policing, represents the whole of the community. Not just the ones that can pay. So my issue is, we have to be careful about it, because if we make it so much of an overarching – almost a condition – that people do this before we take it on, we only represent a small part of the community, and that’s wrong, morally… We have to be very careful, but if they can afford to pay for that resource and facilitate it, then we are dealing with those people to try and get that result (Police#14).

The private sector investigators in this study wanted to know by what rules and what standards they are expected to perform:

I think the industry doesn’t understand the requirements of a brief; of what the police require. So on the other side, I think it’s up to the police to educate them what their requirements are… I think also for the police to give guidelines to the corporate sector. I mean, let’s not sort of muck around with trying to understand where the financial levels are: “What are the points upon which we would take that on board?” “Yes, that would fit in the criteria”. Whether in a brief you would need to have interviewed every member or the alleged offender, those sort of points, then one knows what to pass over (PS#1).  

---

91 The Victoria Police Manual (2005a: 116-1) outlines publicly the requirements for the different types of briefs of evidence.
Senior police questioned that they really want this:

They want to know what rules to play by. But then, once you get the rules in, they’ll be subject to appeal, almost – and to review. To be reassessed or second opinion – and that can bog down of itself. Because once you’ve got those rules down, they’re really open to review, aren’t they? When there’s no rules, it’s a bit like taking notes: remember what you like. They don’t take them… specifically because they can be held to them (Police#14).

Another difficulty with providing standard advice is that the uniqueness of each incident and the elements needed to prove an offence determines to a large extent what actual information or evidence is required for a successful prosecution. This makes it difficult for police to standardise advice beforehand. It was considered that it is easier to provide advice individually to an investigator on the circumstances of particular incidents (Police#14).

Providing standardised advice to private investigators has been attempted in NSW. It was believed by respondents in this study that had impacted negatively on the reporting of fraud in that state.

**Prioritisation of different types of e-crime**

Even if there is a shared understanding of what e-crime is, the different sectors may give different priorities to different types of offences that may affect efforts to combat them effectively. Respondents were asked first to rate the priority they believed police currently give different types of e-crime and then to rate the priority they believed police should give those types of e-crime. Interview respondents were asked to talk through their responses. Each item referred to a different type of e-crime and used a five-point, ordinal
Likert-type scale ranging from Very Low Priority to Very High Priority. The items were pre-tested by a senior member of Victoria Police for appropriateness to the concept of “e-crime” and for how understandable they were.

Did the police and private sector samples differ in their beliefs about the priorities police do and should give to different types of e-crime? The comparative responses of the police and non-police participants for each item are shown in Table App P.1 of Appendix P: Respondents’ views of police e-crimes priorities. Table App P.2 of that appendix displays the combined responses for priority. Only one statistically significant difference was found between police and non-police beliefs about the current priorities for e-crime. This was for cyberstalking, using a continuity corrected correlation $\chi^2 (1, n=44)=3.86, \alpha<0.05$. Generally, there were no statistically significant differences between

---

92 Respondents noted occasionally that for some types of e-crime they would like to respond with “No priority”. This option was not included, because these items were based on Boni and Packer’s (1998) study. It is important that this type of question is interpreted correctly. These items only provide a discrete approximation of the underlying, latent variable of priority (Clason and Dormody, 1994: 32). The appropriate measure for such items is to note the count or proportions of responses in each category, as opposed to the oft used measure of central tendency, the mean (Clason and Dormody, 1994), because this notes the discrete nature of responses on Likert-type items.

93 The Chi-Square Test for Independence is the appropriate statistic for a count-based analysis of differences (Clason and Dormody, 1994: 33). However, chi-square tests could not be performed on the raw data, because the small respondent sample sizes (see Table 5.1) resulted in an unacceptable number of cells with expected frequencies of less than 5 across each item (Gravetter and Wallnau, 1992: 531). The general solution to this problem is to recode adjacent responses or to group similar items if that makes sense. Recoding adjacent responses into a dichotomous response retains meaning in this situation. Responses of Very Low and Low Priority were recoded as Low Priority, and High and Very High Priority were recoded as High Priority. Responses of Some Priority were ignored. This permitted
the samples for beliefs about current police priorities, from which it may be concluded that the non-police sample were acquainted generally with current police priorities for e-crime; although with the caveat that a larger sample should be used to confirm this.

Did the police sample tend to score the priority of any type of electronic crime either higher or lower than the private sectors? There was a weak negative correlation for “advance fee scams”. Some non-police respondents considered this a current High police priority, when police and the rest of the private sector did not ($\phi=-0.295$, $n=49$, $\alpha<0.05$).

Some private sector respondents believed police should consider digital piracy a high priority, when most police did not; considering it instead a civil issue for copyright owners ($\phi=-0.338$, $n=41$, $\alpha<0.05$). This was despite successful investigations by Victoria Police of digital piracy charged under obtaining property or financial advantage by deception (see Table 5.7). The belief was that “they’ve just given up on that, because it’s just everywhere and it’s too hard to police. You’ll get the occasional arrest for that sort of stuff, but that’s about it” (PS#11). Another investigator noted that for his colleagues in the entertainment media industry it is “very, very hard to try to get the calculation of Chi-Square statistics for one quarter of these items; the remaining items as to current and preferred priority still violated the assumption of size of expected frequencies.

$^{94}$ Answering this requires a measure of association rather than a test for differences. Given the recoding of responses as either Low or High and the nominal classification of respondents as police or not the Phi co-efficient was the appropriate measure of association to answer this question (Clason and Dormody, 1994: 33). Clason and Dormody (1994) note that to use Pearson’s correlation in this situation would be inappropriate, because it is sensitive to the choice of scale. That is, if this research were replicated using a different number of response categories, a different correlation score could be expected.
police interested in that sort of stuff. Unless there’s a quick and easy kill and it saves a litigation issue. You can’t get lawyers involved” (PS#15).

Also, some private sector respondents believed police should consider “theft of proprietary or confidential information” a high priority, when most police did not ($\phi=-0.349$, $n=44$, $\alpha<0.05$). The appropriate priority for this was contested amongst police respondents. Some argued that there simply is no legislative offence of “stealing information”. The case law cited by Victoria Police supports that one cannot “steal information”. In *Federal Commissioner of Taxation v United Aircraft Corporation* (1943) 68 CLR 525, Latham CJ ruled that, “I am unable to regard communication of information as constituting a transfer of property… Knowledge is valuable, but knowledge is neither real nor personal property”.95 A senior officer noted the importance of stealing information as a precursor and facilitator of fraud offences:

> Stealing information, I’m talking about: Internally, we have a lot of trouble with the LEAP checks and all that sort of stuff. That’s where I’m thinking of… In a number of our frauds, people are stealing information and creating

95 However, section 71 of the *Crimes Act 1958* (Vic) defines property that can be stolen to include intangible property. Intangible property includes “chooses in action” which includes for example money in a bank, shares and copyright (Encyclopaedic Australian Legal Dictionary). Further, although simple copying of data may not involve “permanent deprivation” of property as per the basic definition of theft in section 72(1), this is covered by section 73(12), “A person appropriating property belonging to another without meaning the other permanently to lose the thing itself is nevertheless to be regarded as having the intention of permanently depriving the other of it if his intention is to treat the thing as his own to dispose of regardless of the other’s rights”. This would seem to provide statutory basis for theft of (some) intellectual property. See Grabosky, Smith and Dempsey (2001: 61-2) for examples of theft of information from governments. Despite this, police still argued that property that may be stolen “includes intangible and tangible, but not data” (Police#4). See also, *contra*, Akindemowo (1999: 205-6).
the platform or the framework for crime… Whether they hack into the system or get a corrupt bank officer and steal confidential information – i.e. home loan accounts on people. You might go in and get yourself a loan for a couple of hundred thousand dollars; you’ll have all your passwords in there. All of a sudden, your name, date of birth and something else is used by a criminal to ring up, change the password and divert that money into an account and draw it out at the casino. That’s what I’m talking about, that’s our bread and butter (Police#14).

Within each group were there differences between beliefs about current priorities and preferred priorities for e-crime offences? While most police respondents believed that advance fee scams, unauthorised access to computers and denial of service attacks were currently low police priorities, many thought these should be high priorities (see Table App P.1). Gaining unauthorised access to computers was described as the “new untapped frontier of commercial advantage” (Police#19), but police also noted that when sometimes you had to undertake an investigation to determine if there was actually an offence committed, it becomes a drain on resources and a low priority quickly (Police#3).

The respondents agreed in general that the following e-crime offences should have high priorities: theft of electronic funds, credit card fraud, identity theft and fraud, dissemination of offensive content (eg child porn and racial hatred), cyberstalking, digital extortion, use of digital communications to plan offences, electronic money laundering or tax evasion, authoring computer viruses, illegal interception of digital information. Police priority for investigating computer virus authors was lessened by the capability of the community to respond on their own to threats. “It’s sort of middle ground, because generally there’s antivirus within hours that can be run up for it” (Police#10). Similarly with online auction fraud, “I’ve given [it] some priority,
but I think more responsibility needs to be played back on the auction houses rather than the police” (Police#2).

Likewise, the respondents agreed mostly that the following e-crime offences should have low police priorities: theft of telecommunication services, electronic vandalism including defaced websites, online defamation, illegal online gambling and spam. Police were quick to note that legislated offences for several of the types of crime did not fall within their jurisdiction:

You’ve got to remember that some of the things that you’re asking questions about here are Commonwealth related offences and not State. Therefore that’s going to be a very low in a State perspective (Police#4).

In particular it was argued by members of Victoria Police that theft of telecommunications services, defamation, digital piracy, illegal online gambling were commonwealth offences. It was also argued by a senior member that illegal interception of data was not an offence (except for members of Victoria Police acting without warrant under the Telecommunications (Interception) (State Provisions) Act 1988 Vic). The Surveillance Devices Act 1999 (Vic) does not actually prohibit the use of data surveillance devices by members of the public; it only prohibits law enforcement officers from unauthorised use of data surveillance devices. However, such data interception is prohibited under s247G of the Crimes Act 1958 (Vic) if that data were restricted by an access control system.

---

96 Under Victorian common law criminal proceedings can be launched for libel of sufficient seriousness. However this is particularly rare, “There’s criminal defamation which generally just doesn’t get used, we tend to refer people to a solicitor for a civil matter” (Police#3).
97 Defined in the Act as any device capable of use to record or monitor the input of information into or the output of information from a computer, but does not include an optical surveillance device. For example a keylogger device.
Priorities within the Computer Crime Squad have had to be reassessed since the tidal wave of work from Operation Lodden, but still lead with crimes against the person (Police#5). Within the Major Fraud Investigation Division there are formal criteria for assessing the priority of incidents, “but equally, I look at it and say if there are John Citizen-type victims we try and do those” (Police#14). “Nuisance” complainants receive less attention. “We try to look after the individual wherever possible, but not those who are continually complaining. Even if they are individuals” (Police#14). However, another member described a far more informal method of investigation allocation:

I come up here, I have a look at the allocation list and I say that looks interesting, I’ll take that one. That is completing bypassing the allocation system and although I get to do interesting investigations and I am certainly more enthusiastic because I’ve picked it, and they may get more work out of me in that respect, and it’s on the list—it’s made it to allocation—it’s still not what the allocation system was designed to work like. And I say… that’s just how it works. Sometimes jobs are “allocated”, but most of the time people come up and have a look see. “I don’t want that one, I don’t want that one. How about that one” (Police#7)?

The respondents in this study were united in expressing a general perception of police that to them the investigations of e-crime is “not as exciting as other stuff, and it’s complicated – you could spend two months looking at a job and get nowhere on it” (PS#11). Alternatively, police have a preference for investigating traditional crimes against the person. “We’ve been bought up on a diet of news which relates or revolves around violent criminal offences: where we hold the Homicide squad in high esteem in this state, I think, and in the police force generally” (Police#10). These preferences were thought to influence decisions about reported incidents.
I think there is a general reluctance to conduct [e-crime] investigations... people don’t turn their minds to this crime type. It gets re-prioritised out, it’s difficult to investigate, it’s difficult to get evidence, it’s difficult to put people before the courts. And, whether you talk commonwealth or state, when they have their meetings to decide which jobs they take on and which jobs they don’t, these go straight out the door… And if you want to talk at a state level, there's still the political things that drive the agenda, like burglaries in streets, cars getting broken into at railway stations, before they even get to the bigger ticket drug dealing, things like that (Police#19).

It was suggested that the low priority of e-crime incidents was related to a generational discomfort with information technology and computers. Unless an incident was novel it was likely to receive lower priority:

The first couple of instances of any emergent crime are always given some priority, just so that there is an understanding of what it is, what’s involved in resolving it and what some of the issues are. So, if you can ever get the first one of anything you’ll have a good shot of getting some resources thrown at it. Once it becomes a little bit more passé and more and more known that it’s going to be very difficult problem to fix the response changes. And I’ve seen that myself with a couple of hacking files that I’ve given off to police, and I sort of think, given a couple of years ago, “My God this is terrible: Russian mafia”. Now you do the same sorts of thing and “Why haven’t they got firewalls? Why haven’t they got virus protection? Why are they going to Kazaa? Why are they doing this?” I don’t know, nobody asks them to steal the money (PS#15).

This attitude was confirmed by police respondents about incidents even as serious as denial of service attacks. “Sometimes it’s a badly configured system. So we would put that back generally on the user” (Police#3). The
private sector expressed a deep dissatisfaction with this attitude of “responsibilisation”:

I think that to say just wholeheartedly: “Look you’ve got a hole in your system and you need to fix it; we’re not going to investigate it” is inappropriate. It’s got to be recognised that we can build all the systems that we like, but there are people out there that are trying to break it. And they’re breaking it because they make large amounts of money. My understanding is that after some recent arrests out of the UK and in Russia, they located an account in Latvia with something like 287 million dollars in it, which is supposed to be the proceeds of somebody phishing. Now, that’s a large thing… It has an impact on every person, because it results in higher fees or higher charges or higher insurance costs or whatever. So … whilst we are responsible for trying to protect our systems and put in processes and controls in place, there needs to be recognition that there are some very smart people out there that are trying to take it down. And when I say this, I’m talking probably within Victoria. I think the High Tech Crime Commission [sic], whilst it’s relatively new, does a good job. They’re probably under-resourced. I think that they do have some sort of understanding of what’s going on. But in the Victorian context, there’s an attitude of “it’s not really our problem, it’s your problem” (PS#11).

The companies spoken to in this study take their corporate responsibilities very seriously. One manager described the measures taken by her employer:

We put an incredible amount of resources in just in terms of looking at our code development. We put [a large number of] developers on to go through [our code] and they were retrained and they each took a section of code (PS#10).

In return, police complained that the private sector reprioritise incidents they reported:
So if we get a particular job from [credit card company], like we had a couple of years ago, and a bloke shoots through, then he comes back into the country and we’ve got him. Or we know where he is and want to go and get him and we want the [credit card] people to come and help us. They might have other priorities and do have other priorities. They say “Listen, we’ve got somebody more important than that at the moment, we can’t do it.” So that then becomes an issue to sort out (Police#14).

**Geography as influence on priority**

Interviewees were asked whether different priority should be given to incidents that involve multiple jurisdictions, such as if an offender or victim is located in another state or overseas. The general practice by State police forces for multi-jurisdiction incidents was described as follows:

Offences interstate: generally between the interstate forces, or at least at our level, we’ve got an agreement that whoever has the offender within their jurisdiction is in all likelihood the state where the matter will be pursued. Statements will be collected in relevant jurisdictions and forwarded, but they will do the charging in that state, simply because it is convenient and under-extraterritorial offences they can be prosecuted in any state. So it’s just logical (Police#4).

We will, the unofficial policy is, I don’t know how close it is to official, but if the victim lives in Victoria, then we’re are responsible for it. We get a lot of phone calls from people from Queensland, interstate, saying I’ve been ripped off on [auction site], and the person lives in [Victorian suburb]. We refer them to local police stations to make the report, and we believe that we can’t take interstate reports especially over the phone. We can’t take over the phone for that, so unless they are going to come down to Victoria and make their complaint, which they’re not, then it usually has to be done at their local; even though there’s extraterritorial provisions for offences. We can
investigate them, the way I do it is to have that person report it at their local police station, wherever they live, and what we do is that we refer people in Victoria the same way: off down to their police station, they investigate it, if the offender’s found to be interstate, then it’s boxed up, sent to their local police station interstate for further investigation. So we recommend that they do the same: Have their local police do it, send down it down to [Victorian police station] to interview the crook (Police#2).

At the AHTCC, criminality and impact was more important than geography:

If it’s fraud [then] dollar value. If it’s child abuse the amount of images or what are the images of, you know. I wouldn’t look at where it comes from (Police#19).

Even though a private sector company may be international this did not necessarily remove geographical boundaries. This IT administrator was separated from his global subsidiaries: “We’ve got a firewall that separates us from them: what happens on their side of the world happens on their side of the world” (PS#7).

If there’s an international component to it, the way things are currently set up, it becomes almost impossible to investigate it across international boundaries, because the mechanism just isn’t there for international cooperation on these things. So I think you can spend a lot of time, trying to investigate something that has an international aspect to it, and waste a whole lot of resources on that, where you might be better off applying those resources to things that are happening locally. And that’s just the reality of it (PS#4).

Although some respondents argued that there is not or should not be a priority difference based on the location of the offender, comments made by other respondents belie that in fact some offence types do receive lesser or greater priority based on geography.
I think that advance fee scams and the like, well, if they’re within Australia there will probably be a more conscious concern for the individual, but when they are offshore like the Nigerian email scams, then, because of international boundaries they will never ever get looked at. So they’re on a very low scale. It’s a matter of actually educating the public just to ignore them (Police#19).

When you look at international issues, unless you’ve got some very important high profile target that a number of countries with a lot of clout—vis-à-vis America—or someone who’s particularly interesting, your ability to actually get anything happening cross border is virtually impossible, I would say. But that needs to go from a state level, where we are, to a federal level and access the resources from that perspective (Police#10).

It may be that the evidence is located overseas and at that point justice has a dollar value:

We may well have the offender here, and we might have the victim here in this country, in this state. But all the evidence that we require to prove the offence is sitting in America, Russia, England, Canada or all of them. Now the cost of getting that evidence may well exceed the purpose in prosecuting. For instance, if you had a $50 dollar deception or something along those lines and it was going to cost you $20,000 to get the evidence to prosecute that $50 dollar deception, I’m tipping that’s going to be a very low priority job. And I’m tipping it may or may not even be pursued. That would need to be a decision that would be made down the track. So in that regard, yes, you would prioritise what was pursued and what wasn’t pursued in a timely fashion (Police#4).

It was suggested that Victoria Police would not fund travel overseas to follow up investigations (Police#7).
I guess we need to protect and show that we’re trying to do our best for our own victims. And if we can catch someone who is doing it, an offender locally, that makes it better. We see a result. Going overseas to bring back people or trying to assist overseas, it’s a very, very elongated process and most of the time it seems to be without result, because other police … in different jurisdictions overseas, they’ve got their own priorities as well. So I think everybody would say, “Let’s keep it local first, then extend out”. Unless it’s something against a government agency or something really big that was coming from overseas, obviously we'd have to be involved with it then (Police#17).

**Cost of investigations**

Consistently in my interviews with police for this study and in teaching officers during the e-crime investigations course, cost of an investigation was seen as the primary factor influencing the decision to launch e-crime investigations:

One of the first things we say is "How far can we take it? What’s it going to cost us?... Sorry, we can’t, we can’t afford it". And with this electronic crime those costs are very large. Whether it’s just people doing normal 282 checks,98 I mean they aren’t cheap for a start. And you may have to do three or 4 of them (Police#17).

Although the actual costs of e-crime investigations were not examined in this study, an example of the potential costs was AUS$27,000 for a single day to have a video-link to a witness in another country (Police#1). The potential for court costs to be awarded against police also influences decisions to investigate.

---

98 More commonly known as Call Charge Record checks, these are requests for information from telecommunications carriers under section 282 of the *Telecommunications Act 1997* (Cth).
I mean our job is so cost driven. A) The cost to actually run an operation B) The fear of costs awarded at courts if we should be unable to fulfil or substantiate the charges that we would bring against the person. And therefore we don’t have the luxury of other parts of the police force or maybe government instrumentalities that can launch prosecutions or take actions in court without fear of losing the case (Police#10).

Another respondent spoke of how risk aversion stopped inclusion of technical details in a media release to educate the public about preventing phishing:

And when we put those technical things in, it wasn't hard, but they thought that if we put that out in a media release people would come back and say “Look I did this, this and this: I’ve followed your instructions, I’ve just deleted my hard drive, and we’re going to sue you” sort of thing. Not that far, but that’s the sort of level of thinking (Police#17).

**Different goals and measures of success**

As suggested in previous research, the interviewees confirmed that different goals motivate police and private investigators of e-crime. For police, prosecution and conviction was cited uniformly as the benchmark standard. Equally, exonerating a suspect can be considered successful, although this gets lost within “No Offence Disclosed” results (Police#5). As outlined in Chapter Three, the overall goal of Victoria Police is reduction in the incidence of crime.

In corporate investigations success can mean prosecution of the offender or another sanction like dismissal (PS#18), but it focuses mainly upon cessation of the activity (PS#1) and avoiding a net financial loss (PS#16). Successful investigation can also mean convincing senior management of a need to
modify policies and having those modifications implemented (PS#12). For others, success is positive public relations; “success is sending the message that we’re going to find you. We’re looking for you, we’re partnering with law enforcement” (PS#8). For administrators who encounter younger e-crime offenders in schools success is “if they learn the damage they did, why they shouldn’t do it and to not do it again” (PS#6).

What do individual victims of electronic want? Those interviewed for this study indicated that first they wanted restitution of their losses (Victim of ATM theft, PS#5) and then they wanted the offenders stopped, so they could not victimise others.

“I wanted to get my money back. And secondly, if there was any way that this could be pursued I wanted it pursued, but I didn’t really know how to go about it... I know that’s probably not possible, because to a certain extent nobody knows who they are. They seem to be very mobile. They’re faceless people. I think it’d be very difficult, but the bottom line is, I’d like to see them put out of business. Somehow (Victim of Internet Banking Fraud, PS#3).

Given the different goals, investigators are working with different measures of success. Victoria Police annual reports focus upon the number of investigations conducted and resolved and number of prosecutions police handle and the cost of these (Victoria Police, 2004b: 6-7). Companies that employ private investigators manage to avoid annual reporting of actual losses or amounts recovered, focusing instead on descriptions of “risk management” processes. Behind closed doors, private investigators are measured in pure dollar terms:
A rival Australian bank has a fraud exposure of $222 million dollars a year. That is enormous business. Out of that, they lose $60 million. That means they’ve actually saved $160 or whatever it is, a year. That’s $180 million worth of fraud the police don’t have to investigate. But we don’t get congratulated for being that efficient. We got told that’s $60 million that you let slip through. I get really annoyed about that (PS#16).

Other firms that work for clients break down their investigation process into milestones that allow measurement of outputs as well as clarify expectations (PS#17).

The Australian High Tech Crime Centre reported use of more qualitative measures of success than state police services, although these could not be found reported in annual reports. As an example, calculation of “mitigated loss” was cited for phishing cases, based on how quickly phishing websites are taken down and knowledge of the funds such sites attracted previously over certain time periods (Police#21). These measures are used because of the difficulty in securing successful prosecutions in these types of cases:

And when you actually talk to the mules, are they always going to be charged? No, because they’ll produce 75,000 emails that they’ve got about the job that they signed up for and they’ll say, “Yeah, I thought it was too good to be true, but…” And you’re not going to get a conviction based on that. In reality, the mules are the people that you could arrest here. Essentially the crooks are overseas and they’re in regions where the law enforcement capacity is not the same or they’re not minded to be the same. So it’s very hard to actually get arrests (PS#11).
Obtaining evidence

Clearly obtaining evidence to prove an offence is central to a successful investigation when intending prosecution.

Is there any evidence? If there is any evidence, has it been collected and contained in a manner appropriate to put before a court? …We’ve had some red hot referrals where you go “This is going to be the greatest job ever” and there’s been no evidence. There’s been no login at the server and you know their ISP might have logged it, [but] it costs you two bucks extra a month so they won’t do it (Police#19).

Collecting, preserving and analysing digital evidence is a technical process relying on technical expertise and experience and specialist tools, similar to other forensic sciences.

Speaking technically for a little bit, you might come across a partition type, like I did called SafeBack. “What’s SafeBack? I don’t know what that is, never come across that before”. So you find out what SafeBack is. But when you used EnCase or the traditional software, it’s like, you don’t know what – like there is a partition there, but I can’t identify it, therefore there’s no data there. But I know there is data there, just because they didn’t recognise a partition header for that table at that time, meant that I can’t identify it, I can’t display the data to them. So I had to find out: I know there’s a partition on that drive, “What is it?” Found out what it is and you basically then have to go backwards and image the drive like we do normally, but restore it back onto that person’s PC and boot it up and then image it again. A live system – change the partition to a Windows value, so that we can then see it (Police#5).

Undertaking digital evidence analysis in aid of an investigation also relies upon having a complete picture of the incident so an analyst can identify
relevant information in a digital source and communicate that back to the investigating officer (Police#5). A lack of police intelligence was problematic when investigating other than the “low hanging fruit”:

We have found in doing our internal investigations, when we’re trying to find or sue somebody, you have to invest in human intelligence. It’s not just about knowing what the Internet means, it’s about somebody sitting in the chat rooms or on the IRC chat rooms, things like that, gathering intelligence, understanding the culture, understanding the way they’re moving, what they’re thinking, what they’re doing. You know, also being able to infiltrate some of the major hacking organisations. I mean, China is probably the most difficult to infiltrate and they are probably the most prolific of all countries in

<table>
<thead>
<tr>
<th>Key success factor</th>
<th>Frequency</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confession</td>
<td>112</td>
<td>52.6%</td>
</tr>
<tr>
<td>Seized evidence</td>
<td>26</td>
<td>12.2%</td>
</tr>
<tr>
<td>RCCR / CLI</td>
<td>12</td>
<td>5.6%</td>
</tr>
<tr>
<td>Victim testified</td>
<td>11</td>
<td>5.2%</td>
</tr>
<tr>
<td>Digital evidence analysis</td>
<td>10</td>
<td>4.7%</td>
</tr>
<tr>
<td>Incident was witnessed</td>
<td>9</td>
<td>4.2%</td>
</tr>
<tr>
<td>Retrieved property obtained</td>
<td>7</td>
<td>3.3%</td>
</tr>
<tr>
<td>Bank records</td>
<td>6</td>
<td>2.8%</td>
</tr>
<tr>
<td>Transaction evidence</td>
<td>4</td>
<td>1.9%</td>
</tr>
<tr>
<td>Cooperation by private sector investigators</td>
<td>3</td>
<td>1.4%</td>
</tr>
<tr>
<td>Exoneration of suspect</td>
<td>2</td>
<td>0.9%</td>
</tr>
<tr>
<td>Linked incident to other incidents</td>
<td>2</td>
<td>0.9%</td>
</tr>
<tr>
<td>Suspect returned from interstate</td>
<td>2</td>
<td>0.9%</td>
</tr>
<tr>
<td>Caught in the act</td>
<td>2</td>
<td>0.9%</td>
</tr>
<tr>
<td>Patrol car response</td>
<td>1</td>
<td>0.5%</td>
</tr>
<tr>
<td>Co-offender informed on defendant</td>
<td>1</td>
<td>0.5%</td>
</tr>
<tr>
<td>Lured offender via computer</td>
<td>1</td>
<td>0.5%</td>
</tr>
<tr>
<td>Police persistence</td>
<td>1</td>
<td>0.5%</td>
</tr>
<tr>
<td>Video evidence</td>
<td>1</td>
<td>0.5%</td>
</tr>
<tr>
<td><strong>Total</strong>*</td>
<td><strong>213</strong></td>
<td><strong>100.0%</strong></td>
</tr>
</tbody>
</table>


* Total exceeds 173 incidents, for which success factors were discernible, as some incidents involved multiple factors. No data was available in 192 incidents.
Table 6.3: Investigation difficulties identifiable from LEAP e-crime incident narratives

<table>
<thead>
<tr>
<th>Difficulty encountered</th>
<th>Frequency</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Evidentiary</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Suspect denied allegations</td>
<td>23</td>
<td>13.6%</td>
</tr>
<tr>
<td>Suspect made a 'No Comment' interview</td>
<td>17</td>
<td>10.1%</td>
</tr>
<tr>
<td>Offender located outside Victoria</td>
<td>13</td>
<td>7.7%</td>
</tr>
<tr>
<td>Insufficient evidence to proceed</td>
<td>12</td>
<td>7.1%</td>
</tr>
<tr>
<td>Inability to ID a suspect</td>
<td>7</td>
<td>4.1%</td>
</tr>
<tr>
<td>Offender location unknown</td>
<td>6</td>
<td>3.6%</td>
</tr>
<tr>
<td>Lost or tampered digital evidence</td>
<td>5</td>
<td>3.0%</td>
</tr>
<tr>
<td>Inability to refute suspect's claims</td>
<td>3</td>
<td>1.8%</td>
</tr>
<tr>
<td>Wrong suspect was identified</td>
<td>2</td>
<td>1.2%</td>
</tr>
<tr>
<td>Password protected files</td>
<td>1</td>
<td>0.6%</td>
</tr>
<tr>
<td>Unable to ID victim</td>
<td>1</td>
<td>0.6%</td>
</tr>
<tr>
<td>ATM cameras nil value</td>
<td>1</td>
<td>0.6%</td>
</tr>
<tr>
<td><strong>Delays</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Investigating member took leave</td>
<td>22</td>
<td>13.0%</td>
</tr>
<tr>
<td>Delay caused by external investigators</td>
<td>11</td>
<td>6.5%</td>
</tr>
<tr>
<td>Investigating member changed</td>
<td>4</td>
<td>2.4%</td>
</tr>
<tr>
<td>Company refused to provide information</td>
<td>3</td>
<td>1.8%</td>
</tr>
<tr>
<td>Suspect absent when warrant served</td>
<td>3</td>
<td>1.8%</td>
</tr>
<tr>
<td>Incorrect (old) forms used</td>
<td>2</td>
<td>1.2%</td>
</tr>
<tr>
<td>Member too busy with other cases</td>
<td>1</td>
<td>0.6%</td>
</tr>
<tr>
<td>ISP gave incorrect info</td>
<td>1</td>
<td>0.6%</td>
</tr>
<tr>
<td>Difficulty reading ISP Logs</td>
<td>1</td>
<td>0.6%</td>
</tr>
<tr>
<td><strong>Legislative or Policy</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Complaint was withdrawn</td>
<td>17</td>
<td>10.1%</td>
</tr>
<tr>
<td>ISP, bank or merchant must report else no offence disclosed</td>
<td>7</td>
<td>4.1%</td>
</tr>
<tr>
<td>Suspect had &quot;authority&quot; to act; offence N/A</td>
<td>1</td>
<td>0.6%</td>
</tr>
<tr>
<td><strong>Other</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Member unsure if incident criminal or civil</td>
<td>3</td>
<td>1.8%</td>
</tr>
<tr>
<td>Member refused CIU assistance</td>
<td>1</td>
<td>0.6%</td>
</tr>
<tr>
<td>Member lacked skills</td>
<td>1</td>
<td>0.6%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>169*</td>
<td>100.0%</td>
</tr>
</tbody>
</table>

* Total exceeds 137 incidents, for which investigative difficulties were discernible, as some incidents involved multiple factors.
hacking and malicious hacking. We found leads there but could go no further, because you sometimes have government sponsored hacking and malicious activities. So, if you can build up the human intelligence, if these agencies had that ability to tap into people in the underground, you can get a lot further in your investigation. It’s not all just knowing what IPs means and that. It’s knowing what’s really motivating these people and where to find these people. That’s the hardest part (PS#9).

Factors that led to the success of the investigation were identified in 47.4% of the stratified sample of e-crime incident narratives (n=173; see Table 6.2). For those police who are not technical specialists “if you get a confession it’s a great start” (Police#10). The LEAP incident data revealed that offenders confessed in half of the e-crime incidents for which there was data on success factors (n=112, 52.6%). The other most common success factors indicated in the narratives were that police had seized evidence of the offence (n=26, 12.2%), the results of Reverse Call Charge Record (RCCR) searches or Caller Line Identification (CLI) (n=11, 5.6%) or that the victim testified (n=11, 5.2%).

Difficulties in e-crime investigations were more easily identified from the incident narratives, most likely due to the nature of these narratives as progress reports to management (see Table 6.3). These difficulties did not always mean an offender was not processed for the offence. In many cases, the difficulty amounted to a delay in the investigation, such as in the 22 incidents (16.8%) where investigating members took leave during the investigation and the case was not resumed until they returned or it was reassigned. The average delay due to leave was 46 days (n=21; \( \bar{X}=45.7, \sigma=48.2 \)), the shortest five days and the longest was 165 days. In a few cases the police member was unable to access pertinent digital evidence, because it had been destroyed in the normal course of business, “Due to procedures of the complainant, no evidence can be gained. All avenues of investigation
exhausted”. Digital evidence was “lost” in five cases while in police custody, for example where unknown persons deleted text messages that were evidence of harassment via another mobile phone.

**Relationships between Australian police investigators**

Multi-jurisdictional investigations require a sensitivity to what is occurring in other states and an appreciation of the limitations of police powers, as explained by this detective speaking about his interactions with another state police service:

> We don’t want to compromise what they’re doing, because of the cross border issues. So we investigate in our state, but we don’t want to go storm trooping over there and speak to her without their assistance, because we can’t arrest in another state unless you’re a special constable. So when we go, we work with them or we execute a warrant with the local state police; actually we ask them to use their powers. Or if we have to arrest someone, we get them to arrest them and they facilitate it, bring them back to their place and we might ask the questions, but then we apply to their court to get that person extradited back to our state. So you have to use the powers of arrest and warrants in various states by the members of those states, because you’re just a guest in their state (Police#10).

Working with other police forces, both interstate and at the federal level, was described as problematic for state police. The bureaucracy involved, whether to have a warrant or arrest executed interstate or simply to conduct record checks, frustrated police (Police#8). Comments by the respondents about investigating e-crime highlighted the adversarial nature of relationships between state and federal investigators, reflective of O’Malley and Palmer’s (1996: 151-2) observations about the intense rivalry for “high policing” turf
between police and other regulatory agencies. In this case, it might even be called a tug of war over “l33t” policing.⁹⁹

There's been a history of non-cooperation in Australia. Federation was the worst thing that could ever happen. The states see the Commonwealth as just a cash cow and so they suck it dry for everything they can, and high tech crime is exactly the same. I think a lot of them pay it lip service and they don't like it. You know, even as we come in the perception is ‘tread all over everything and take all the good jobs’. And that's in all crime types. And I remember when we were going through setting up this Centre and probably some of our biggest sledges were even Victorian police. And a lot of it without basis. There's a stack of animosity (Police#19).

AHTCC personnel questioned why state police forces negotiate separately with private organisations on issues such as retention of data, instead of permitting the Centre to work on behalf of all Australian jurisdictions in a coordinated fashion (Police#19). AHTCC officers described having to convince state officers they were not from the Australian Federal Police to get assistance, “Sometimes we don’t succeed – quite often, we don’t succeed” (Police#18). It was argued that genuine state-federal cooperation only happened when there is a joint task force approach, giving common focus to the various agencies (Police#10).

Everyone’s very protective of their backyard I suppose and they don’t like disseminating information that could assist you in your investigation or vice versa (Police#6).

---

⁹⁹ Pronounced “leet” and meaning elite in leet speak, the language of the hacker underground.
Many Victorian police officers bemoaned the AHTCC. “Federal agencies quite often come up with reasons not to share information. We share with them, they don’t necessarily share with us” (Police#7).

I’ll label the High Tech Crime Centre as maybe the most guilty party, because I’ve got no idea what they can do and I’ve read their website and I’ve read all the information that we’ve got, which is just the website in relation to what they can do. I would assume there is an MoU between them and all the other police forces in Australia, or whether it’s Australasia I don’t know. But I’ve never seen it. I don’t know what they can do for me. I rung them up on a wing and a prayer and say, “Well this is what I’ve got, can you help?” Or email them, “Can you help?” and if they can, they can, if they can’t, well, there’s not much you can do (Police#6).

AHTCC members were naturally defensive of the work they do:

I don’t know what the answer is. We do completely different policing. What the AFP does in national policing—excluding ACT community policing—and what the states do is chalk and cheese. Can’t be compared. Different political priorities. Different everything. Well, we still do go out on the street. We still do search warrants, we still lock up people, we do all those techniques, but ours is very offshore, ours is very national. We’re very, well, without pissing in our own pockets, we’re a lot more broader thinkers than the states are, because they sort of come up through traffic and that’s all they think about (Police#19).

In latter interviews, some Victoria Police officers described improving relationships with the AHTCC, following a visit to CCS by the new AHTCC Director.

There’s been a void of information and we haven’t known [what they do]. And I think there was a huge notion that it’s a FedPol thing, that they’re
trying to take over every state, that they’re trying to push their ideas on us. And obviously you get resistance to that. That’s right, we didn’t know what they did and he’s cleared a lot of that up. And I hope that information will be forthcoming from him (Police#3).

This visit helped resolve expectations that the AHTCC were going to take over some of the state police workloads (Police#9).

They’ve actually got their deal together now and are becoming useful. At the start they just weren’t, they were promising everything and delivering nothing, whereas now we’re starting to see the results of people reporting there and then dishing out stuff; so [they are] available resources for us as well, in terms of if we need something done (Police#2).

However uncertainties remained outside of CCS and others reported a continued lack of feedback about incidents reported to the AHTCC (Police#13).

Of great importance to a partnership policing strategy, cooperative interactions between investigators relied on personal contacts:

I deal a lot with Customs, mainly because I know the guys there; we bounce ideas off each other… [another agency] not so much, because they’ve been fragmented, there’s been a lot of change and I’ve lost contact with a lot of the guys there… And people tend to say, “I know you, I’ll talk to you”. But if I don’t know you I’m probably a lot less likely to provide you with information (Police#3).

Difficulties were enhanced by the location of many federal agencies in Canberra.
You know they’re there, you know you need to use them, you get jobs from them, but you can’t ring them up or they can’t ring you up and say how about we go for a coffee or we’re going out for a drink tonight would you like to come along as a get together and you know just keep…keep relationships going. Can’t do it, because they’re not there (Police#5).

Mutual assistance requests through the Attorney General’s Office were considered labour intensive and time consuming (Police#4): “I’ve got to fill out a 9 page dot point … just to get a case worker assigned to it. So, it’s a lot of work. It can take 6 months” (Police#2).

More formal arrangements were viewed sceptically, as added bureaucracy might hinder information exchange more than assist it:

It’s not terribly satisfactory. I mean, we’ve looked a few times at putting something formal together or semi-formal together. We have a group in Victoria, the VDEG, the Victorian Digital Evidence Group. We get together and we discuss things… And there’s one in every State, but there’s no real formal connection between us. It’s been spoken about, but formalising it is kept at arms length, because it’s viewed [that] if it is formalised there won’t be that freedom of information that free flow of information (Police#3).

Both police and private investigators described relationships with overseas agencies as difficult: “We’ve sent stuff to Interpol before, but that’s a black hole, we never get to see that stuff again or hear about it or anything” (Police#2).

Trying to get a site pulled down in Korea can sometimes be a real drama. Getting a site pulled down in the US, sitting on a compromised computer is impossible… because they don’t care. It’s got nothing to do with the US so it’s not really their issue. You can send all the emails and the cease-and-desist letters you want to the IP providers and they don’t care. I think it’s because
the traffic consumes the bandwidth so they get fees. So they’re not worried about the customer’s compromised computer. But yeah, it can be a real drama trying to get those sites taken down (PS#11).

**Relationships between law enforcement and private sectors**

Interviewees were presented with information about Sarre and Prenzler’s (2000) models of police-private sector interaction and asked to characterise their own interactions. Police indicated that most private investigators with whom they interact were ex-police officers who have joined or head up private sector accountancy or investigation firms. “It’s just like we’re a small community of people in Australia” (Police#9). Ad hoc partnership was most often selected as representing the type of interactions between police and private sector personnel. This model was chosen by 54% (n=20) of interviewees, because they characterised their interaction as cooperative, but transient, and focused on individual incidents.

Banks, I think they’re a classic example: combined temporarily when needed based on mutual need for each other. You get a credit card sort of offence, a crook’s been using a magnetic card skimmer or something like that. They bend over backwards to help us, you know, and we press them for help and it’s a mutual thing while that case is lasting. You know if there’s no cases the communication there dries up for a while, till the next one comes along and it starts all over again. Not that we just don’t want to deal with them anymore or they don’t want to deal with us: just the need’s no longer there for the communication and it breaks down (Police#9).

In terms of working together, it only happens if something arises. Say for instance somebody’s had $2000 ripped out of their account. I have to contact

---

100 Thirty-seven respondents; four others made no clear response. Some respondents elected two models: ad hoc partnerships and another.
them and start up the relationship at that point. And once that’s finished, I won’t use that person again until I get another complaint. It’s very ad hoc and it may not be that same person, may be somebody else. And with them, if they have an issue they may report it. It will go to somebody down here. There’s no established movement of information or jobs or whatever (Police#1).

It’s not a partnership *per se* until they report the matter to us. And then it becomes this ad hoc partnership where temporarily we’re going to be mates and we’re pointing in the same direction. But when it’s over, we’ll go back to our separate directions (Police#6).

Flexibility was a major benefit of ad hoc partnerships (PS#12). The one ISP that replied to the study described it this way:

> We had a client whose laptop was stolen. But we found that the laptop was still using the owner’s internet service. So we contacted the police and we provided them logs of connection usage, which gives phone numbers. This enabled the police to locate the offender. No agreements, no pack drill, just getting on the job of solving the crime (ISP).

Outside of ad hoc partnership interactions, contact was described as fitting the supplementary services model (n=6, 16.2%); often due to the processes described above about private investigators undertaking preparatory investigations and handing off to police. As Button (2001: 109) noted there are few examples of police treating private counterparts as equals. “Police see us as ‘inferior’ and or interfering. When we put forward how to proceed there is contempt and accusations of interfering” (PS#21).

According to Stenning’s (1989) model, the relationships between police and private investigators in Victoria could be characterised as falling somewhere
between stages two (grudging recognition) and three (open hostility). To leave the police force and join a private firm was to change the relationship with their previous colleagues, who then considered that ex-members were “using” serving police officers.

[They] give the façade of wanting to help and all the rest of it, but they have other motivations, they have other masters now and that’s the dollar and so anyway they’ve obviously taken that incremental rise in money and you’ve got the little detectives down here working for this person who’s milking the system and doing quite well (Police#10).

Police respondents acted as moral superiors to private investigators, because they do not charge complainants for their investigation services:

I would say that the private investigators working with a motivation of making money — where they can account for a charge for every 6 minutes of their time, similar to an accountant or a barrister — milk the system for all it’s worth and charge the client, the corporation, large amounts of money. And every time they have an interaction with us — that the private provider of material or investigative services has an interaction with the police — they will bill their client for that privilege. And whether it’s supplying of information, phone calls, letters, notes, warrants, property, exhibits, meetings, you name it: there will probably be an exorbitant fee attached to it. A lot of big corporations really don’t mind, because they factor that into their thinking, but when you consider the length of time that some of our investigations take, you just feel that the corporation is being stung by the money-grubbing private provider (Police#10).

The work done by some larger private sector investigation firms was described as getting “bent over” (Police#19). It would be fair to state that these views, expressed in the confines of confidential interviews, would probably
not be expressed face-to-face. However, it seems these underlying feelings impact upon the relationships between the sectors and possibly influence policy, such as acceptance criteria described above.

Once police receive a case, they generally do not want to deal with “middle-men” private investigators; they want to go straight to the complainant victims (Police#10). They asked why they needed to update private investigators monthly or have meetings when they were in contact with the complainants. Unless police have an issue with submitted materials, they did not see a need for further interaction with private investigators at that point.

As was expected, there were some private sector investigators and police who had no cross-sector interaction (n=4, 10.8%).

In my situation, something comes to my attention, I’m bound by contractual obligations, policies, procedures to take certain steps. It’s not my job to ring police. And in fact if I ring police I could lose a contract. So I’m obliged to report it to the responsible authority… What they do with it is their responsibility (PS#18; also PS#6).

Several police respondents commented on the lessening of face-to-face contact with investigators in the private sector. For example, end-of-year liaison functions of the early 1990s when Major Fraud and Corporate Crime merged are no longer held (Police#12). This lack of contact may contribute to complaints that police lacked understanding of business operations and processes (PS#14; PS#21 above). One police respondent had had no interaction with private sector investigators, because

the victims paid to get the job imaged by an independent person, to get the job done quicker, and my understanding was that we were referred from my
bosses that “Well they’ve done the job; they can do it all for you, so basically we won’t touch it” (Police#13).

The interviewees rejected uniformly the Competing Forces model of interaction: “There’s no competition for market share” (PS#11). While the private sector may be competing, police are (supposedly) not. “We’re not competing for market share, because we investigate criminal not civil and they investigate civil and they can’t investigate criminal because we need to get involved” (Police#5). This highlights the legitimation crisis public police actually face, because private investigators are investigating crime and police are placed under a “quasi-market” pressure to meet performance indicators (Moore, 1990: 73).

Four respondents (10.8%) based their interactions with police on boundaries suggestive of the Property model:

If we’re the victim, have whatever you want. If we’re not the victim, give us a search warrant. But at the end of the day, it still gets to them. We’ve got to protect ourselves as well. We’re not just going to give out all this information (PS#16).

With Internet fraud, it’s not so much of an issue, because usually the banks have paid out, so we’re the victims and we’re reporting it (PS#11).

A few respondents thought the Division of Labour model best described their situation (n=3, 8.1%).

But what they’ll do and what we’ll do, there’s some reasonably clear boundaries on that. We can’t go storming into people’s houses and seizing their computers. I mean, we could if we got an appropriate court order, but we don’t see that as our role. We see that as their role. So yeah, there are boundaries there to who does what and what part they play (PS#11).
Others thought the boundaries were not clear enough:

I find sometimes they tend, the private enterprise people, tend to overstep their mark a bit, because they don’t have the legislative powers to do some of the things they think they can do. Or if they do, they really stretch it, to the point when they almost call themselves a police officer with whatever powers we have (Police#17).

The Joint Banking and Finance Sectors Investigation Team at the AHTCC was considered a “combined forces” model by each investigator there; it is discussed in detail in the next chapter. Only one investigator—excluding members of the Australian High Tech Crime Centre—considered that her company had reached a combined forces model of interaction with law enforcement (PS#9). The combined forces model was disputed generally on the basis that even though there may be a common objective towards crime reduction the focus of public police is on crime against the person, whereas these private investigators are concerned about financial, property crime (PS#11).

It was not expected that any interviewee in this study would disclose evidence of “unholy alliances” between police and private investigators in relation to e-crime investigation; and they did not. However, the Director, Police Integrity noted in his 2005 Annual Report, “convincing evidence” of “inappropriate associations between police and private investigators and the private security industry” arising from investigation of specific cases (OPI, June 2005: 23). Law enforcement respondents were uniform in their take on the Unholy Alliance model: police moonlighting and improper information sharing is a thing of the past, because of regulations.
I’d knock out the unholy alliance completely. I think it’s seen its day. In my 15 years of policing, it’s seen its day… There’s too many checks and balances in for people to be doing anything like that now (Police#19).

Private sector investigators affirmed this:

Probably seven to eight years ago, there probably would have been improper information sharing, but these days with the revisions of the Privacy Act and all that sort of stuff, the banks in particular are probably very reluctant to hand out information without actually knowing that you’ve got a warrant. That’s not to say that it wouldn’t happen, but it’s more likely to happen at a branch, where a policeman walks in and says “Oh, look, I need to do this” and talks to someone who doesn’t really know what they’re doing. In terms of e-crime, no, that’s out (PS#11).

Although the majority rejected the existence of unholy alliances, some interpreted current practices of some private investigators using personal relationships to get incidents investigated as unethical: “It’s almost like a soft form of corruption, isn’t it? You go to lunch and ‘Will you do my job?’ Instead of going through a tasking coordination process” (Police#14). There was disagreement within the private sector about the importance of personal relationships in the process of getting police investigations launched (PS#15):

It’s all relying on relationships, it’s the only way things work. If we want VicPol to do something, we don’t go to the fraud squad, we go to the divisional CIBs, and use relationships that we have with people that they’ve done something for us before and they know a bit about fraud and they’ve got a bit of a go-and-get-‘em attitude. “Can you do this for us” (PS#11)?

Others described this networking as a constraint that prevented collaboration with police: “staff currently rely upon networking, not clear guidelines and
contacts” (PS#22). One of the biggest problems described was inconsistency of response both in the private sector and within Victoria Police:

Getting people who don’t know what the go is, so you ring them and you get somebody who just has no idea… “Nope, we can’t do it”. So you find someone else in the office has done it two weeks ago, but they spoke to a different person. Stuff like that I find is inhibiting… and that’s the same everywhere. I mean I’m sure it has happened in this office as well with somebody has rung and said, “Yeah, we can do that” and then they come in and they get somebody who else who says, “Nah, we can’t do that”… [I find it happens] more here, because we investigate things that are so different to normal policing. Normal policing is drummed into you from day one, what you can and can’t do, such as crime scenes such as burglary such as theft, such as assault. So you know them back to front. Whereas here, especially with the new offences, there’s no guidance on it, there’s no rules, so everyone reads it differently, everyone classes it differently, everyone has different experiences in terms of computing so some things they know they can’t do, others can do it, but someone else in the office might not know that. So whereas if you’re in a division, just normal detective, you know that you can investigate a burglary, you know this, you know that. “We know where to get that information.” Whereas here, unless you ask everyone in the office every single question that you get asked, you’re not going to get that information (Police#2).

One suggestion from a respondent to address inconsistent responses within the CCS was a database of investigator skills (Police#2). However, this idea was kiboshed by another member in case it highlighted individual member’s deficiencies and became a source of conflict.

Police were also concerned that private investigators are not required by law to caution persons whom they interview, because they do not fall into the
category of investigating officials under Section 464 of the *Crimes Act* (Vic). Given the increasing numbers of private investigators undertaking interviews, legislative amendment was recommended. Police found that when cautions have not been administered properly in private sector interviews they had to repeat interviews or “double-dip”, during which suspects might change their stories, complicating a case, because it then became necessary to prove elements of the first interview in addition to the offence (Police#10). This also concerned private investigators, “There might be a suggestion that we could abuse the system by getting a private sector person to do the interview. Get a confession off the record and then use that” (PS#4).

**Privacy legislation and search warrants**

The “Privacy Act” — which referred collectively to the *Privacy Act 1988* (Cth) and the *Information Privacy Act 2000* (Vic) — was cited almost universally as the most problematic legislation affecting e-crime investigation efforts of both police and private investigators. Not necessarily because of the Acts themselves, but because organisations misunderstand or refused to agree about how the legislation permits them to assist police. Often it was “the lack of consistency in that response [that was] actually responsible for a reduction in effectiveness from our point of view” (Police#15). The Victorian Privacy Commissioner, Paul Chadwick, has a favourite saying in relation to these perceived problems that he has used in many public forums. He calls it “BOTPA. Blame it On The Privacy Act.”

It’s unfortunate that a lot of the people out there don’t have a real understanding of what the Act is saying. In fact they can release information, they feel they can’t, they start putting up fences… it’s certainly put up a lot of hurdles (Police#17).
We quite regularly have arguments with police on the phone about the fact that “No, you need to get a warrant”. And they try to rely on the Privacy Act, “Well the Privacy Act says you can give me this information for criminal purposes”, and so: “No, you go and get a warrant”. I mean, we’re quite aware of what we should and shouldn’t be giving, and I don’t want to be standing in front of my MD, explaining why we’ve stuffed up and why the Privacy Commissioner is knocking on the door… It hasn’t been tested yet, but no one wants to be the test case (PS#11).

Private investigators also felt that the privacy legislation prevents them from carrying out aspects of their work in relation to tracing accounts:

I think, certainly in respect to the Privacy Act, [private investigators] should be recognised as a quasi law enforcement body, within the Privacy Act, which they are not at the moment. So, we’re stopped basically from getting a lot of information, when we’re identifying a fraud. I mean, where we have identified there is a fraudulent process in a course of action, we can’t get any information from some of the government or semi-government bodies. Whereas, a law enforcement person can… I’ve got one job at the moment, for example, where I have somebody with a false identity has made claims. The best thing I can do is to put a stop on the membership and stop the claims going through. But I cannot find out who the member is, who has been doing this. They have a bank account, but I can’t go and ask the bank for identification of the member that’s paying the premiums even though we know the bank account number… And the bank can’t come and tell me. And there’s a fifty thousand dollar fine… So, I think there needs to be greater recognition to the people who are doing the right thing out in the private arena (PS#1).

Because some of the information then is in a partner or a spouse’s name, privacy legislation doesn’t allow me to close the account. Now, fair enough,
because I’d like that same protection myself. So there’s that degree of frustration (PS#15).

As another example, private investigators would be unable to effectively trace IP addresses of suspect computers:

If they’ve got an IP address, they’ll whack it into whois and that’s as far as they’re going to get. They’re not be able to resolve, you know, when it comes up to Telstra, they’re not going to get past that, so their avenues of enquiry are just going to dry up (Police#19).

Demands by financial institutions for warrants to produce records pertinent to criminal investigations frustrates police:

Why do we need a warrant that allows us to break enter and steal by day or by night at the [bank] to go and get the account statement records of Mrs Smith? I mean all we need is a streamlined process where either an officer of police or a Senior Sergeant of police can look at the circumstances of perhaps of a short report where the aspects of a person’s accounts is required, but the bank won’t release anything until they have something of a statutory nature that protects them (Police#10).

[A particular bank] won’t even disclose information until you execute the warrant. They’re saying we refuse to confirm or deny the existence of an account in that name. Which makes it difficult to get a warrant if you can’t confirm that the evidence for an indictable offence is at that location (Police#7).

101 Pronounced “who is”; refers to a tool for finding registration and contact details of an Internet domain name in various registry databases.
According to the respondents, banks are even requiring search warrants where police are able to show them that the identity involved is fraudulent (Police#15). Applications for search warrants need to be approved-in-principle in the first instance by an officer no lower than the rank of Senior Sergeant before going to a magistrate to have it issued (section 465, *Crimes Act 1958 Vic*). Respondents suggested that what is needed is a less onerous mechanism than a search warrant:

There needs to be something beneath a warrant, like a document of seizure authority or something where the police can simply go along, justify that to their superiors, rather than have to go to the court. And then the officer would sign that authority and then they’d go down to the bank give them a copy of that and the bank would then release the documents (Police#10).

Others suggested a “warrant card” system where no additional paperwork would be necessary (Police#7; Police#8).

For a bank, we give them what’s called a friendly warrant. So it is a warrant done by the court. A lot of the time you can just do it through what we call a 47, a form 47, letter of correspondence. We’ll send that off to them and they’ll do it. If it requires it to be used evidentially for a court, we’ll then obtain the warrant to have the proper materials extracted. Things are in place already, it’s just how quick we want the information. Maybe there could be some sort of legislation that says ‘When you do have a matter that police are investigating, a serious matter, the exchange of information should occur like this’. You know, you bypass that, because everything gets bogged down and the more things get bogged down the less they actually get investigated (Police#1).

---

102 Section 92(2) of the *Crimes Act* also permits an Inspector or above to approve a search of premises for stolen goods, if the suspect has been convicted for deception offences within the five preceding years.
For investigators in federal government agencies the process can be even more complicated:

First of all you’ve got to get your affidavit together, which can be quite lengthy and detailed. Then you’ve got to coordinate that with the availability of the federal police, and if they’re not available, you can use Victoria police to execute the warrant. So you’re talking a couple of weeks, I suppose. It could be a couple of weeks or longer, and your federal warrant only stays alive for about seven days, so you’ve got to make sure that the police are available within seven days of its issue. Otherwise, you’ve just got to go and get another one (Police#15).

Police may take private sector personnel with them to assist in searches of premises under section 342(1) of the *Crimes Act 1958* (Vic): “A search warrant authorises any member of the police force, with such assistants as he or she thinks necessary, to enter and search the premises to which the warrant relates, and anything in those premises”. Persons assisting police may also use reasonable force to carry out the search.

Private investigators understand the delays caused by the search warrant process:

Money can move from account to account to account – you don’t know where the money has gone until you’ve got the first set of accounts. And then you say “Oh, I’ve got to go to a second bank to get that” and go through the whole search warrant application process just to get on to the second bank. And then you find it’s gone to a third account. So they’re caught up in red tape and it slows the whole process down (PS#4).
Private investigators are more restricted than police when it comes to search and seizure, because they do not have access to criminal search warrants. Private investigators saw collaboration with police as an entrée to investigative avenues such as search warrants (PS#14). Private investigators also raised the possibility of advising clients to report to police in an attempt to sidestep privacy legislation. Their solicitors could file for third party discovery against the police to obtain the documents that were seized for a criminal case and use them in a civil proceeding.

I don’t think the system would cope too well with police going out, getting documentation with a search warrant, routine application to the court for third party discovery, because it’s easier, abusing the process. They [police and courts] wouldn’t be that happy (PS#4).

**Technical resources**

Members of the Computer Crime Squad felt generally that they had sufficient technical resources (Police#2). Only in the area of decrypting encrypted files did the Computer Crime Squad express an interest in acquiring access to additional hardware:

Infrastructure in that regard would be, it would be great if we could incorporate ten thousand PCs on a network and utilise 10% of all their processing power for our own goals of breaking encryption (Police#4).

However, other police felt that the centralisation of technical resources for e-crime investigation compromised their own investigation efforts.

We can’t even get EnCase\textsuperscript{103} here, because it’s so expensive. I know Computer Crime have got it. For them to have it, that’s fine. But then for you

---

\textsuperscript{103} Industry standard in commercial forensic computing software.
to go and use it, you have to go up to their office. And I might have a hard drive that’s 80GB, and the keyword selection search and the target word search encompasses 40,000 hits. So I have to use their system to look through all the EnCase files and that can take days. So what am I meant to do? Whereas, I could sit here with a copy of EnCase on the system here and go through it at my leisure when I get a spare hour and eventually get through it over time. But the other way’s too difficult, and so we don’t do it… We have to refine the keyword search. It has to be so refined down that it has to be words that would only be 95% particular to that incident. Which eliminates us broadening out the investigation or looking at the fringes of it. We have to actually just identify that particular bit and we miss everything else. So, it’s basically you’re in a dark room, you’ve got a dart and a dartboard on one side. They turn the light off and you fire at it. That’s how we do it. Sometimes it hits the bullseye, sometimes it doesn’t. But that’s because we don’t have the money to resource (Police#1).

Another police officer reported going outside Victoria Police to conduct digital evidence analysis using the resources of a third party investigation firm hired by the complainant company to avoid delays with the Computer Crime Squad (Police#8). There was concern that doing so might “taint” the evidence, however the investigation exonerated the suspect. “Look it was refreshing and it was a unique experience from my point of view in that you’ve got a company who employ the services of the police, ultimately the lawyers billed the company. They didn’t bill Victoria Police” (Police#8).

Several police respondents complained about having to input the same information about their investigations repeatedly into many non-integrated police databases (Police#15).

I would say that an investigator at the Fraud squad would spend 35-40% of their time repetitively entering the same information on all the systems...It’s
an absolute ridiculous and frustrating situation, which seems to be getting worse rather than better. I don’t have a brilliant computer mind, but with my limited knowledge I don’t see what would be so difficult to have one system that is used across the board by every department or station, is user friendly and once an entry is created it’s simply updated and retrieved by any person having authority (Police#15).

First, officers are required to keep an official diary, but many also keep a day book. All incidents that come to MFID are recorded in ASISCaseManager, where they are updated throughout the life of the investigation. There is also the StationBooks system. The same information has to be entered and updated into LEAP on a monthly basis and also into the Crime Department system called APOD (Action, Plan and Operation database) that is used to report to the Assistant Commissioner of Crime. MFID members also input data into an in-house system called TAYSIS, which was created by one of the MFID members, because it provides easy cross-referencing of investigation information about exhibits and people. It assists investigators by collating this data into brief of evidence forms for court, saving lots of time. Despite the availability of information in these systems, officers complained about having to reproduce summaries to report to their superiors. Email constitutes another “database” that is not centralised for information sharing within the police (Police#10). This segregation of information fuels turf tussles within the organisation.

We’ve got all these little stand alone intelligence sections, units, organisations, all keeping their own little bits of data, not sharing it as you would hope to do. Saying "Oh, no you can’t have that. Or we’ve got this little bit, but we can’t tell you everything." And that to me is foolish (Police#15).
Feedback to complainants

A common complaint amongst private sector respondents was the lack of feedback from police about the progress of e-crime cases. In some instances, they reported receiving no feedback at all:

It’s really difficult, because with any investigation—even the stuff that we as an organisation refer to police or give them any information to assist them with an investigation—we may never get any feedback. So we may never know if someone ever had been arrested or prosecuted for a particular action (PS#16).

We completed a full investigation of company systems, employing data forensic experts. When referred to police along with all contained evidence police have NOT replied any results of investigation. Employee has become suspect not only of police but of company efforts (PS#21, emphasis in original).

Forfeiture of “tainted property” and victim compensation

Information technology used in the course of an e-crime incident, such as home computers, might be considered “tainted property”\textsuperscript{104} that could be forfeited following conviction (see especially, Smith, 2004b). Members of the Criminal Proceeds Squad (CPS) were interviewed to discuss this, however explained that they are not involved with minor forfeitures. They indicated that members of Victoria Police were also often mistaken about what the CPS does and does not do to assist investigators. “In doing compensation jobs our

\textsuperscript{104} Defined in the section 3(1)(a) of the Confiscation Act 1997 as “property that was used, or was intended by the defendant to be used in, or in connection with, the commission of the offence”. Schedules 1 and 2 of the Act list offences for which forfeiture may be sought.
role is pretty much just to restrain the assets and then after conviction it falls back to the victim to get their own solicitor and pursue it civilly” (Police#11). CPS requires in excess of a $10,000 loss and a victim who will apply for a compensation order before CPS can apply for a restraining order under the Confiscation Act 1997 (Vic). Most e-crime incidents of this nature involve companies or financial institutions and financial loss. Forfeiture of company computers was generally not appropriate in such incidents.

For other offences, such as possession of digital child pornography, interviewees suggested police investigators should be applying routinely to the courts for the forfeiture of computers as “tainted property” once the computer has been analysed for evidence and an offender convicted. However, forfeiture of computer is particularly rare in Australia (Smith, 2004b). In incidents where losses have gone overseas assets are unlikely to be restrained, because as one respondent put it, “No one’s going to listen to the Confiscation Act from Victoria. Do you know what I mean?” (Police#11). Similarly, although Victoria Police has the authority to investigate digital music piracy proscribed under federal copyright offences, these are not scheduled under the Confiscation Act and they cannot restrain property for these offences (Police#12).

**Training and accreditation of investigators**

Private sector investigators, especially those who had previously been police officers, questioned whether public police had superior training in terms of e-crime investigation (PS#11) as suggested by Sarre and Prenzler’s supplementary service model. There was consensus that there was a lack of training available for both police and private sector investigators of e-crime incidents. Police were particularly unhappy with the level of training, “you’ve
got people here that, let’s face it: they’re just not qualified. It’s embarrassing” (Police#1). “All of our cases have involved some electronic aspect and we really should have received at least some lectures on that basis” (Police#7).

The main issues surrounding training were the lack of funding to provide training outside CCS and to junior private investigators, despite the expectation that these people now investigate most e-crime incidents; lack of available cross-platform training in operating systems such as Apple Macintosh and Linux (Police#5) and the cancellation of courses. It was noted that Victoria Police courses like the Economic Crimes Course had been discontinued (Police#8).

So, there’s an expectation pushed down on detectives or uniform members to investigate what are still quite cutting edge crimes, without – they haven’t been given the training. They don’t have the skills to do it. But there’s an expectation that they will do it. In fact, straight out, they’ve got to do it, because if they don’t do it, no one’s going to do it, which causes a lot of frustration (Police#9).

Talking about the lack of training for his employees, one investigator lamented:

What training do you give them so that they feel confident that they’re not doing the wrong thing? … And it’s alright to say “Well, at the lower level you’re going to learn on the job and learn as you go and it’s experience and you’ll get it”, but you’ve got to have some training for them to feel empowered enough to be able to say “No, I’m not going to give you that information”. I’m not always in the office for them to refer back to, so they’ve got to have a good grounding on what they can and can’t do, and what avenues that they should be following. There is nothing around at the moment (PS#11).
Additionally within Victoria Police, there was a complaint that maintaining qualifications was not sufficiently recognised and remunerated. Members of the Computer Crime Squad spend a lot of time maintaining their qualifications with the latest forensic software, knowledge about computer systems and training others. Lack of training was inevitably linked to budgetary constraints:

I think funding is the biggest problem. Training for VicPol does seem to take a lower priority even though they may say it doesn’t. But I mean they got a budget and the place has got to fitted be out properly with vehicles and equipment and that sort of stuff...wages, whatever. There’s priorities of the core business (Police#17).

Others blamed fragmented training efforts:

Training is the bugbear of everyone. Everyone you talk to generally says “No, there’s never enough training. There’s no training, there’s no training, there’s no training”. Yet, everyone’s having the crack at doing their own, half assed thing. There’s no national coordination with training. It’s a joke. Absolute joke. I don’t know how many times I’ve spoken to people and said “If you’ve got a great idea, think nationally, we’ll support it. We don’t have a mandate on good ideas, think national”. People won’t. And what VicPol are doing with you guys\textsuperscript{105} is probably a classic example of the isolation of the training. If it’s a great idea, why not roll it out nationally (Police#19)?

Inevitably, training is sought in reaction to specific crime trends, such as credit card skimming, which required card vendors to train police.

\textsuperscript{105} Refers to Graduate Certificate in E-Crime Investigation.
We had no one within Victoria Police who was trained in anything in relation to credit card skimming. Not how to download a skimmer. Didn’t know how encoders worked. Didn’t know about the computer programs that were used. We asked for assistance from private industry, financial institutions in relation to reading the credit cards, providing us advice on how things work, because prior to that had no idea. None whatsoever (Police#6).

Linked to training is the issue of accreditation. Until recently, computer analysis was not considered a forensic science. As forensic computing aims to become a recognised forensic science, it will be necessary to accredit investigators and laboratories. Police want their own officers accredited independently to boost their standing in court as expert witnesses. Accreditation for private investigators is “only done, essentially, to freeze out the mavericks on the side” (Police#14). Generally, private investigators were in favour of professionalising their industry to keep people from simply hanging out a shingle as happens in many areas of IT.

Role and workload of the Computer Crime Squad

There was a debate within Victoria Police about whether the Computer Crime squad should only be a support squad providing forensic computing support to other investigators or whether it should undertake more e-crime investigations. Linked to this was the question of whether CCS should be staffed by detectives or analysts.

Computer Crime want to hang onto their … image that they’re a high profile, highly skilled, “staffed by detectives” [unit], but in effect, because the word investigation has been taken out of their description—they’re now Computer Crime Squad and not Computer Crime Investigation Squad anymore. So as a result they put up a great argument to say “Well, we need to have detectives there to analyse this data and do this work and they need to have a certain
level of qualification and they have to be skilled or trained at Detective Training School”. But Detective Training School doesn’t teach them anything about computers, it might teach them some investigative process or things to consider, steps to consider but basically most of those guys are self taught or they come with computer backgrounds way before they joined with the police force…. My argument is that you don’t need to have detectives in those positions. You might have someone to review the stuff later on, but a lot of that is just a service industry: they crunch the numbers, they go where you go, you analyse it. You get a few analysts and a few people to crunch it, I don’t see that they need, I don’t see that Computer Crime needs to have detectives (Police#10).

The issue in part arose because CCS rarely runs investigations themselves, despite the provision of their Charter to run proactive and reactive investigations (Police#2; Police#9; Police#13). This was largely due to the forensic workload arising from large child pornography operations like Auxin. Members of the squad were divided about whether the squad should conduct more investigations, as some members were reportedly content to undertake digital evidence analysis (Police#2). The Computer Crime Squad does not have the facility to take incident reports directly from complainants who walk in off the street, although some would like to (Police#2). However, CCS member respondents were united in expressing the importance of the lateral thinking skills of detectives to successful digital evidence analysis.

Understaffing, backlogged cases and other demands on their time disgruntled CCS members. The decline in jobs undertaken by CCS in 2004/05 reflected that CCS was discouraging members from bringing in evidence analysis jobs to them, which they would be unable to complete at their current manpower (Police#4). In addition to their forensic workload, members often found themselves responding to requests for “training” or lectures, including many
requests from prosecutors, magistrates and schools (Police#13). The inability
to refer e-crime child pornography incidents was one of the major frustrations
of CCS members: “One of the unfortunate positions [is] that we can’t push
analysis to CIUs or down, every other squad can push stuff out. We can’t,
it’s… the buck stops here” (Police#9). Operation Lodden had affected the
psychological wellbeing of officers at CCS for whom child pornography
analysis became a staple diet. “Oh, that's a massive drain. I mean it's crap to
look at. The whole idea of it is awful. And unfortunately it’s got to the point
that there's no way around it. There's nothing you can do it’s, I mean because
we predominately do child porn cases. That’s all we do” (Police#3).

Inadequate staffing

Uniformly respondents reported that there are insufficient skilled
investigators to complete all the tasks involved in investigating rising levels of
e-crime.

Where something is required of us, whether it be an unauthorised access or
something like that, there is a real, an unsaid thing in the office where if I was
to go and say “Look I’ve just taken a phone call from a company in St Kilda
road that is saying that someone is accessing their system.” There is no way
known I would be authorised to go and do that job. Not a hope in hell. It’d be
“time to go and ring a private company and get them to look at the system”
whatever it might be and it just wouldn’t happen… At this point with our
current workload even a 100% increase in our strength would be absorbed
very quickly (Police#3).

A job out there for a major company that has been a victim of an e-crime: one
person from here is not going to do the trick. And at the moment that’s maybe
all we can spare, maybe… Having no investigative capability is personally
not on. It should be happening and we should have the ability to send three
or four blokes out to a major corporation who have been hacked or denied service or whatever, and have the expertise and the ability and the resources to be able to investigate it. But we don’t (Police#2).

However, it was noted that tapping into younger members’ skills is constrained within an organisation like a police force, because of the hierarchy of ranks and qualifications:

But because it’s a rank based job, if you’re not at the right rank to get the job you’re not going to pick necessarily the right person to do the job, because they’re not necessarily within the rank structure or have a qualification like Detective. You might get someone who’s a connie who’s just joined the job out at Footscray, who if he was put on a task to assist with something electronic he might be leaps and bounds ahead of people who, say, are here in this office at the moment (Police#10).

**Headhunting and retention of police officers**

Fears about the headhunting of law enforcement personnel working in the area of e-crime are well founded. In a high profile example, Alastair MacGibbon, the original director of the AHTCC was headhunted into the private sector by the auction site eBay just a year after the Centre opened. Others commented:

I think whoever goes into High Tech Crime’s going to get poached, unless they actually start realising that’s a likelihood. Because whoever is the head of High Tech Crime is going to network and if they’re seen to be doing a good job there’s going to be job offers for them. And some of those job offers will be three or four times what they’re on now (PS#11).
This headhunting is seen as impacting on the effectiveness of an organisation like the AHTCC.

You’ve got the transition while they work out who’s going to be the new boss. Then the new boss comes in, and you’ve got to go through that ‘what experience do they have?’ and you’ve got to go through that rebuilding of the relationship to him. We probably have more contact with the lower levels – but again, they would be getting job offers, I’ve got no doubt. Anything like that, of course, has impact on the relationship. And then the new person comes in, you’ve got to think about do they actually know what they’re talking about? Are they a talking head? How long are they going to be there? Are they going to change the focus? What do they see as priorities and all that sort of stuff? What are they going to do? And you’ve got to work through all those issues (PS#11).

Some argue that those headhunted to the private sector are not “lost” to public police and this should be considered a relocation of investigative resources. However, headhunting is a major concern of the Computer Crime Squad, because their core business is not investigation, but forensic analysis. To lose a CCS member to the private sector does mean a net loss for Victoria Police. One of the factors influencing headhunting into private investigation is pigeon holing within Victoria Police.

You have to have been in the chair for a period of time before you’re able to develop an expertise and then you cease to be marketable in other areas. For instance as a policemen, which is what I am, I would struggle now to go and get a job doing general police work because I haven’t done it in so long. So I become pigeon holed A) through my own intention, because that’s the avenue I want to go down, but B) because I’ve let everything slide. And everyone’s the same out there (Police#9).
Another influence on headhunting the quality of work that can be expected outside of a police force, as commented by a private investigator who had recently been headhunted by another firm:

I’m really lucky that I’m working in an organisation that’s way at the top of the tree. And I’m spoiled rotten and where I’m going, I’m going to be spoiled even further, because people aren’t going to be able to afford to hire me to do junk. I can only be hired to do significant work. I’m never going to have to put up with doing crap (PS#16).

Recently, five members of the Computer Crime Squad were authorised by Victoria Police to set up a private business to provide digital evidence analysis and data recovery to the small to medium enterprise (SME) business market.

I don't think they [Victoria Police] were happy with it. It took us six months to get the approval from all the bosses. They’re obviously concerned that a) we’d use their equipment and time to do the work, and I think, although it never hit paper, that they’re concerned that five of the squad are going to leave and that’s half the strength here gone in one swoop. And I can understand their concerns in relation to that, but it's part of an ongoing dispute that people are having with management—and its not the actual management here per se, but the police command in general—in relation to career advancement and recognition of skills and so forth. In term of the private world, they just offer too much money, and everyone’s got their price. Now, life here is good, in terms of ... we work hard, but we don't work arvo's, weekends, nightshifts, we're not doing overtime all the time, we get good equipment, nice office. So we can't complain, but when it comes to crunch you hit a ceiling in your career and you want to go somewhere else or you want to advance, because I know myself I've got another X odd years before I retire and I'm not going to sit here for X years doing what I'm doing.
And that was part of our reasoning for starting this company and we’d identified all these problems with Vic Command and said “We want change. We like it here, we want to stay, but you guys are going have to do something”. And we were basically told, “If you don’t like something, leave and we’ll get someone else to fill your spot and we’ll train them”. So, I thought well, do you want a better income? Start your own company. If we leave we leave. If we don’t: we’re happy, like I said, we’re all happy here. We like it, but we need something else to occupy our minds I guess (Police#2).

Unlike days gone by of unauthorised moonlighting this venture was sanctioned. The private forensic work undertaken by police who work at this company allows them to experience IT systems they normally have little exposure to at Victoria Police, learn those systems quickly and bring the knowledge back to Victoria Police (Police#3). Although this initiative raises several issues about potential conflicts of interest for Victoria Police, these had been addressed in negotiation with Victoria Police:

It’s company policy for us not to do criminal [investigations], because obviously it’s a conflict of interest for us straight up, and that’s something we tell clients straight off the bat “if it’s criminal, we’re not even going to start”. If we start a job, a civil job, and all of a sudden we look at it and it’s going to become criminal, we’ll step away and either hand it to somebody else and say to the client “sorry, we can’t be involved in this anymore”… If it becomes a criminal matter, we would probably refer them to their local police or to the Major Fraud group or whoever is going to handle it. If the job ended up coming back to this squad, there are other members here who can handle it and it would be in consultation with the boss and obviously it’s something we want to have happen, but because any job we take on we look through thoroughly to start with and if there is any aspect of criminality at all we won’t touch it. It’s just company policy (Police#2).
Backlog of work and investigation delays

Large-scale coordinated raids, such as that of Operation Lodden in Victoria to combat online child pornography, exacerbated a backlog in the forensic examination of computers seized in such raids. “You talk to any of the computer crime teams that do the forensic work, 18 month back logs is the norm” (Police#19).¹⁰⁶ Police explain delays and backlogs in terms of the priority of incoming e-crime incidents, especially those conducted entirely via email such as auction fraud.

¹⁰⁶ The extra time investigations take may have subsequent impact on accused persons, especially those who are innocent. However, it should be noted that in Australia there is no general right to a ‘speedy trial’ at the common law independent to the right to a fair trial (Jago v District Court of New South Wales (1989) 168 CLR 23, ¶13, Brennan J.). To recognise such a right would necessitate a remedy for its abuse, such as permanent stay of an investigation or indictment. That would undermine the right of the State to have a matter investigated and tried at court, by imposing arbitrary time constraints on investigations. The means to test such a breach would be untenable:

Such an enquiry would encompass an examination of the level of resources made available by the executive government for the detection, investigation and prosecution of criminal offences and a critical review of their utilisation in the particular case. It would encompass the effect of delay upon the life and interests of the accused in the particular case. And it would end with an assessment of reasonableness from the viewpoint not only of the accused but of the public whose interests the enforcement of the criminal law is intended to protect and, especially, of any victim of the crime. The elements for consideration are so diffuse that they can hardly be the constituents of a common law right (Jago v District Court of New South Wales (1989) 168 CLR 23, ¶16, Brennan J.).
We need to act on it quickly, to get information, but having said that, you identify a person, you do a warrant, you take his PC and it becomes a low priority for the moment, because everything else goes above that (Police#5).

Similarly, members of MFID complained about cases taking a long time to get through the allocation phase (Police#7). Commonly when CCS requests assistance from ISPs or banks it is on behalf of another investigating member. However, one respondent reported reducing the lag between receiving requested information when it related to an investigation carried out by CCS members; ostensibly because of the closer relationships between CCS members and private sector staff (Police#2).

Delays caused by investigators taking leave during investigations, as evidenced in the closed case LEAP data (see Table 6.3 above), might not prevent successful investigations, but certainly affect complainant and private investigator views of police investigations. Police expressed concern about the impact of leave:

I mean 9 weeks annual leave that’s more than two months of the year you’re not here. Long service leave, I’ve got about 9 months long service leave if I wanted to take it. Carer’s leave, that’s changed now because it used to be your sick leave, you could only access to that with a sick certificate but now with carer’s leave they’ve changed the label on it so that people are now taking their sick leave that they’ve accumulated and I’ve got [hundreds of] days over X years. So if my wife gets sick or a family member gets sick I can take my leave off. All I do is provide a [statutory declaration] or a certificate from the doctor and I’m just out of circulation, I’m gone (Police#10).

Accrued leave was reported as a key factor that permitted members of the Computer Crime Squad time to form and run their own civil forensic computing and data-recovery company.
Chapter conclusions

The interviews and LEAP data revealed many factors originating both outside and within Victoria Police that affect the investigation of e-crime in Victoria. First, the interviews revealed differences between the sectors and within police as to the nature, scope and boundaries of “e-crime”, suggesting the need for continued education and clarity when discussing this phenomenon. Technological advances have assisted the detection of e-crime in general, although some products, such as unlimited broadband packages may hide unauthorised access incidents from end-users.

This study provides support for the importance and working of factors identified by Chan (2000) as driving forces in decisions to report or not report e-crime. For example, the influence of IT knowledge might be bi-directional depending on whose IT knowledge is at issue. Less IT literate managers were described as under-reporting when knowledgeable IT administrators would have reported if it had been their decision. Whether an offender was internal to a company might discourage reporting, dependent upon the relationship of decision makers to the offender. Or it might encourage reporting, because of the ability to nominate a suspect.

However, this study also highlights the importance of police influence on reporting behaviours. Within Victoria Police, reporting to an officer who is skilled and willing to undertake an investigation is the first major hurdle for complainants. Avoiding investigators who feel that victims “deserved” their victimisation is another hurdle. Middle management officers have also been forced to devise policies that discourage reporting and or recording of incidents and encourage referral of incidents to other jurisdictions. Prioritisation has been used to “stall” investigations and discourage further
reporting; incidents might not be accepted unless accompanied by evidence packages; extraterritoriality provisions are generally overlooked in favour of referring incidents to the jurisdiction in which offenders reside; incidents might be declared civil and not criminal; narrow definitions of victim are applied to certain offences and reports not accepted from victims who are redefined as “witnesses”. These initiatives and policies have been instituted as matters of cost, practicality and under the rhetoric of “responsibilisation” of the private sector. Other rationales that led support for these policies included dissatisfaction with the bureaucracy of investigation, police frustrations with “lazy” members of the Force and a desire to prevent corporations from taking advantage of Victoria Police.

Victoria Police was described as reacting defensively to the high costs of e-crime investigations, fear of costs that might be awarded against them at court and headhunting of their officers. This reaction has been exacerbated by the increasing incidence and complexity of e-crime incidents that require costly investigation processes such as digital evidence analysis, which is only provided by the thirteen-man Computer Crime Squad.

The Computer Crime Squad affects police investigation of e-crime in Victoria intimately through its provision of advice to officers in the five regions. The ubiquitous involvement of information technology in modern crime and the lack of clear boundaries in the law enforcement definitions of e-crime and “computer crime” have placed strain on the Victoria Police Computer Crime Squad and its members. Almost any crime might be considered e-crime and directed to their door, including perjury the least obvious of offences (see Figures 5.7, 5.8 & 5.9). To help address the workload and negotiate their fiscal constraints, Victoria Police officers had taken to interpreting criminal
legislation in ways that reduce recording and investigation and subsequent reporting of incidents by victims.

Redefining incidents in this way does not help harmonise definitions and understanding of what constitutes electronic crime (Electronic Crime Steering Committee, ACPR, 2001: 10). Nor does it assist the development of strategic intelligence about crime trends, which is key to a preventative strategy, nor assist crime analysts attempting to identify links between incidents for investigation, because incident data are not recorded.

The value of personal information to criminal enterprise is unquestioned. Obtaining personal and other information is often the precursor to many serious frauds, such as identity theft. It is an area of loss of great importance to business and individuals alike. Whether “theft of information” can be pursued through criminal prosecution is debated by police, even though the Crimes Act 1958 (Vic) is suggestive that it might be. It is not a legality that police wish changed. Police would face an even worse fiscal crisis if they had to investigate theft of intellectual property.

The model computer offences, as introduced by the Crimes (Property Damage and Computer Offences) Act 2003 (Vic), have thus far had little impact. In what appears a catch-22, the complexity of the offences and lack of completed prosecutions had led to argument over the applicability of these offences to different types of incidents, which led to forestalling of investigations.

These actions are understandable in the context of economic managerialism, post-Keynesian policing and the need to establish favourable case law. The Australasian e-crime strategy is guided by a principle that “prevention is better than cure” (Electronic Crime Steering Committee, ACPR, 2001: 5). Responsibilisation should impact upon prevention efforts positively, however
should not exclude policing when prevention is unsuccessful. Some practices highlighted by this research suggest that a certain level of e-crime offender is systematically ignored by both law enforcement and the private sector.

It is not clear which came first, but key corporations have acted to externalise costs of assisting police by targeting their reporting to local CIUs and decreasing the frequency of this by reference to privacy legislation and demanding search warrants. Technological advances have permitted Internet Service Providers to offer products, such as unlimited broadband that have the perhaps unintended consequences of hiding unauthorised access incidents. Of importance to partnership efforts, private investigation firms face similar constraints to police when investigating multi-jurisdictional incidents. Engagement of a multi-national investigation firm was not described as a panacea to jurisdictional or geographical issues.

A common theme that emerged from the interviews was an increasing breakdown in communication between police and major stakeholders in e-crime investigation, such as private investigators and financial institutions and Internet Service Providers. The issues raised by the interviewees suggest that thus far there has been little success in achieving synergy between police and private investigators (Covey, 1989: 263). The interviewees painted an adversarial picture between state and federal police and private investigators, peppered by working together on an ad hoc basis to investigate individual incidents. This presents a significant hurdle to a partnership policing strategy for e-crime. Briefings from other agencies, such as the AHTCC Director’s visit to Victoria Police, have started to pave the way for better state and federal interaction.

The findings in relation to acceptance criteria and recording of incidents suggest strongly the need for policy change within Victoria Police to institute
a strict *prima facie* model of report recording so as to give credence to the Key Performance criteria under *The Way Ahead Strategic Plan 2003–2008* and avoid conflation of inputs (the recording of crime) with outcomes (reduction in crime) and encourage development of shared goals between police and the private sectors. If Victoria Police wants to gather a clearer picture of fraud and e-crime occurring in Victoria, it should first implement a streamlined reporting process and require members to officially record all reports, because it is clear current methods contribute to the dark figure of e-crime.

Large-scale operations, such as Operation Auxin have turned the profile of the workload of Computer Crime Squad upside-down and child pornography cases now predominate. Consequently, does the role of the Squad need to change to better meet the needs of Victoria Police and the community? Should the functions of complex e-crime investigation and routine digital evidence analysis be separated? Should the Victoria Police Computer Crime Squad be staffed by detective level investigators or unsworn analysts? The private company formed by members of the Computer Crime Squad is an example of synergistic thinking within Victoria Police to retain their detectives. It meets the needs of the parties involved: increased variety for CCS detectives and hence greater satisfaction in their careers; for Victoria Police it has thus far avoided headhunting of their members and provides a lateral avenue of training and organisational knowledge acquisition.

The next chapter examines the respondents’ reactions to the strategy of partnership policing that aims to improve interactions between police and the private sectors.
Chapter 7: Responses to investigative partnership policing of e-crime

In light of the current context of e-crime investigation in Victoria, highlighted in the previous two chapters, this chapter explores respondents’ views about strategies of partnership policing as they might apply to e-crime investigation. The previous chapter demonstrated that the majority of investigators, police or otherwise, remain constrained by resources and geography and indicated strained relationships between them.

In this chapter, three different examples of Australian attempts at investigative partnerships in the field of e-crime investigation, detailed in Chapter Four, are used to highlight issues relating to investigative partnership policing and the investigators’ responses to possible police-private sector configurations:

- a joint taskforce and secondment model as exemplified successfully by the Joint Banking and Finance Sector Investigation Team of the Australian High Tech Crime Centre (AHTCC);
- partnership through industry bodies, as seen in an attempt by the private sector to form a new industry association with police called the E-Crime and Forensic Technology Association of Australia (EFTA); and
- one-to-one commercial relationships as explored in preliminary discussions between a forensic investigation firm and the Computer Crime Squad of Victoria Police.

POLSEC is also examined as a possible generic framework for partnership. Interviewees discussed with whom police should partner and how, their concerns about partnership policing and regulation of partnerships including their responses to the elements of Sarre and Prenzler’s (2000) proposed
Regulated Intersections Model of police-security interaction and the state government proposal for a Victorian Fraud Information and Reporting Centre (VFIRC).

Shared meanings of partnership?

Chapter Three outlined the meaning of partnership policing according to the Victoria Police *The Way Ahead Strategic Plan 2003–2008* (Victoria Police, 2003a) and the meaning of partnership according to the Victoria Police Manual (Victoria Police, 2005a). As discussed in Chapter Six, e-crime investigative “partnerships” described by the respondents and evidenced in the LEAP data were ad hoc, bringing together participants only for the duration of a single investigation or were informal relationships between investigators. At the time, respondents indicated that Victoria Police did not have any memoranda of understanding with private sector organisations in relation to e-crime investigation (Police#4). At a federal level, investigative partnerships have also been ad hoc in nature.\(^{107}\) In many cases, “partnership” would not describe correctly the relationships between police and those they contacted in the private sector during investigations. What did “working in partnership” mean to the police and private investigators who have been asked to develop working partnerships?

For the majority of interviewees working in partnership meant “information sharing”, whether this was information on suspects, investigation methodologies or business processes and technologies. “And it means that

\(^{107}\) For example, in 2001 the Australian Federal Police, Microsoft and a Brisbane-based private investigation firm Trade Mark Investigation Service (TMIS) conducted a partnered investigation of copyright offences in the software industry (Lawler, 2001: 40).
you have a confidence in that movement of information, that it won’t be used for any other purposes other than what was originally intended” (Police#1).

Few respondents identified partnership as “working together to achieve a common goal” (Police#17; Police#13; PS#14). Victoria Police members were involved in non-investigative relationships with the private sector relating to e-crime information sharing. For example, individual police officers were variously members of international organisations that they considered “partnerships”, such as the International Association of Computer Investigative Specialists (IACIS) and the High Tech Crime Consortium (HTCC). This involved participation in email lists. Police also attended local chapter meetings or conferences of professional bodies for investigators, such as those of the International Association of Financial Crime Investigators (IAFCI) and the Australian Institute of Professional Investigators (AIPI). Victoria Police was also involved in “training partnerships” with tertiary institutions, such as with Melbourne University Private,108 La Trobe University and Holmesglen TAFE. Victoria Police also pursues research partnerships, whereby they offer research topics of interest to research students (Police#4). While these are not partnerships involving investigation of incidents, the respondents’ discussed their key role in facilitating interaction between the sectors in the day-to-day context of investigation.

Often partnership was discussed in terms of facilitating the respective, routine work of police or private investigators:

> It’s making life easier for each other. And disclosing avenues of information that either go to prove or disprove the facts in issue. And at the moment, we face brick walls in the private sector, because we can’t get access to the information. Where if working in partnership were that, we would get the

---

108 Later with the University of Melbourne as Melbourne University Private merged with it.
information and we would be able to say one way or the other if we had any points of proof. And whether we’re going to be wasting their time by going forward with the brief or not (PS#1).

The respondents’ concerns were mainly about responding to the inefficiencies of existing investigative practices and workloads discussed in Chapter Six. For example, cooperating with police investigations without causing delays or difficulties was seen as “partnership” (Police#6):

I think working in partnership means having the police … working closely with [a company] to train the loss assessors so that they’re not wasting the police time and coming down for frivolous matters. When they do grab someone… there’s sufficient evidence. That’s a partnership. That there’s training there, there’s the education. They’re helping each other out (PS#18).

This focus on routine work contrasted partnership initiatives that target specific forms of offending, like the JBFSIT focus upon phishing and the Virtual Global Taskforce focus upon online child sex offending. Pursuing parallel goals of criminal and civil prosecutions at the same time also constituted partnership (Police#5). For those investigators who saw themselves in a supplementary services position to public police, partnership involved police exercising control over investigations but outsourcing investigative activities, as in this example of referral:

We took an assignment so far then reported it to police, so that we could get access to warrant-based information. Then the police took over the matter, and now have assigned us to do the work. Assigning us, in other words, telling the party, “This is the information, but we haven’t got the resources ourselves to do that”; so asking us to do that (PS#15).
This is a clear example of Flemming and Rhodes’ (2005) “network state” characterised by issues of diplomacy, trust and reciprocity. Participating in interviews of suspects to confirm or refute technical aspects of an organisation’s business was an example of partnership behaviour (PS#1). Others thought partnership should entail police contracting investigators in to alleviate understaffing:

I’d seriously consider it if I was approached to go and work for Computer Crime or for the state Forensic Science laboratory… They say, “Right, we want—you’re trained—we want you to come in on a contract basis, we’re going to train you just as though a junior police member would have come in”… I’d be quite prepared to do that on a contract basis. I can understand the reasons why the police wouldn’t want to do that. Legalities, training, responsibility, retaining knowledge. But they can do that through contracts. I think they have to have a shift in their attitude towards the way they do things (PS#18).

Partnership meant acting ethically to build relationships “without that going into anything that’s inappropriate. And I suppose in the broader sense when you’re involving police in it, it goes into public interest type issues that some of the common interest is a matter of public interest as well” (PS#14).

Partnership for police also meant sharing blame and reducing costs:

Amongst other things, it means sharing out the responsibility for blame if it goes bad. Partnerships mean trying to widen your resources without paying for them. So if we’ve got 10,000 police officers and we can partner with someone else, maybe we can do more work. Partnership means, in the right circumstances, freeing up the information, although there are obviously issues, legislative blockages with that. But that’s what you’re trying to do: you’re trying to get information from one area to another. Trying to get an
understanding and appreciation of both sides, of all the organisations (Police#14).

While some in the private sector recognised the need to share “deficits”:

Partnership is about $1 + 1 = 3$. So I mean there has [sic] to be benefits flowing in both directions to both people and also the deficits as well. And that’s a true partnership… and sometimes I would see that you might have to go into deficit before you get into benefit in the long run in some particular cases (PS#17).

Others were not interested in sharing the liabilities of responsibility, such as costs awarded in unfavourable court decisions: “I’d be out of business, I’d be broke in a week with all the costs awarded against me. So not interested in it. I’m willing to help the police and I’m willing to work towards that, but, no I don’t want to be prosecuting” (PS#18).

From the private sector perspective, partnership meant taking a longer-term view of reciprocity or “payback” (PS#4). In the short term the private sector would make money and in the longer term the community and police would benefit from faster resolution of investigations. “So it’s a win-win-win situation between the consultant, the victim and the state in terms of speedy resolution and crime suppression” (PS#4).

However, working in partnership is complicated by the underlying roles and relationships that people and organisations have with police:

I don’t really know what working in partnership is. And I don’t know what the police expect out of a partnership. At the end of the day, we’re a victim, they’re a service provider. They’re either going to be able to provide the service or not (PS#11).
Police disliked empty rhetoric and posturing about partnerships:

[Partnership is] a dual will to actually do something not just the window dressing. It’s not just a matter of walking into big business, because it’s easy to go to a big business like [the telcos] and say “We want to work together” and they go “Yeah, yeah, we want to work together” and go to Company X and say “We want to work together” and the CEO of Company X is a really nice guy. I’ve got a lot of time for him. He’ll trot out at the next conference and say “I’m working with police.” He’s not doing jack. We’re talking about an awful lot of things, we talk about it till the cows come home, but not a great deal is getting achieved in a lot of instances (Police#19).

Police were critical of “partnerships” they have with other regulatory agencies that appeared to hinder rather than assist investigations:

We have so-called partnerships between us and [a regulatory agency] and getting information out of [that agency] is just ridiculous. It’s like getting blood from a stone. We had a matter that was reported to us by [that agency], where me and my Sergeant went to meet him, was us two and about five solicitors from [the agency] and they’re saying “We want to report this matter to you”. And I said “Well, who’s the defendant?” “Well, we can’t tell you.” “What have they done?” “Well, we’ve done a warrant and we’ve found this information.” “Well, can you tell me about it?” “Can’t tell you.” And I said “Well, when you work out whether you can tell us, then we’ll come back, because I can’t apply for a warrant, because I don’t know anything and you won’t tell me, even though we have an MoU in process” and they go “Well you can write to us to request it.” And I go “Well I don’t know what I’m going to request, because you won’t tell me”… And I just went “Well, you all go back and have a meeting and when you work out that you’re the people reporting it to us and you can provide us the evidence, then we’ll come back”. And that took months and months of too-ing and fro-ing. So, it’s all
right to have a partnership, an MoU, but it’s got to work. I would assume that
the definition of partnership is to make things easier not to hinder (Police#6).

Given the often-separate goals of police and private investigators and the
difficulties discussed in Chapter Six, interviewees were asked whether
partnerships were necessary to perform their work. Could not law
enforcement do it by themselves with warrants, just making the paperwork
easier? Police thought not. “But that’d be just like going around with a stick in
your hand saying give up or get clobbered sort of thing. And that doesn’t
work” (Police#17). Partnerships were considered “absolutely necessary” to
improve the current situation: “It’s like the old transformation process, I mean
that anything that feeds on itself is doomed to failure. You’re going to
disappear in ever decreasing circles. You have to have input from other
sources” (PS#1). Partnership was warranted to address skill levels:

Yeah, I think we do [need partnerships], because it’s obvious that not
everybody’s going to be skilled in everything, I mean you can’t teach a police
investigator from Computer Crime... how to operate Linux and be a Linux
guru in one course. I mean these things take years of experience, years of
playing with, years of technical knowledge, you know setting up systems,
utilising systems and just, you know, hacking... They may come across a job
where it’s hacking a big server but they don’t have the experience to
investigate it. Are you going to rely on the systems administrator that may be
the crook (Police#13)?

Survey respondents expressed their views on policing partnerships for e-
crime investigation by indicating their level of agreement with statements
about them (see Table 7.1). These respondents were clear in their support for
partnerships that extended beyond single incidents and disagreed that
partnership would engender corruption. Survey respondents agreed
generally that partnerships should be formalised through codes of conduct, contracts or laws (see Table 7.1). With the partnership policing strategy, the idea of partnership is beginning to take on more formal characteristics for police:

Partnership, it has a bit of a different connotation than it used to have. I think nowadays, you know I think I would use... a professional relationship with more formal process... I think when we talk about partnerships with Melbourne University Private and Victoria Police there’s a signed document, ... this is almost an extension of a memorandum of understanding, it’s a formal process... So when people say, we’ll talk about partnerships, now to me I immediately think about the formalised process (Police#9).

Table 7.1: Ranking of agreement with statements about partnership policing of e-crime

<table>
<thead>
<tr>
<th>Rank</th>
<th>Statement</th>
<th>N</th>
<th>Mean</th>
<th>Std. Deviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1st</td>
<td>partnerships should extend beyond a particular incident (ie, be long-term)</td>
<td>27</td>
<td>1.74</td>
<td>0.98</td>
</tr>
<tr>
<td>3rd</td>
<td>partnerships with police are necessary to combat e-crime effectively</td>
<td>26</td>
<td>1.88</td>
<td>1.14</td>
</tr>
<tr>
<td>4th</td>
<td>effective partnerships need regular meetings</td>
<td>27</td>
<td>1.96</td>
<td>1.02</td>
</tr>
<tr>
<td>5th</td>
<td>partnerships with police should be formalised (eg, codes of conduct, contracts or laws)</td>
<td>27</td>
<td>2.07</td>
<td>1.04</td>
</tr>
<tr>
<td>6th</td>
<td>joint investigations by public and private police need to be regulated by new legislation</td>
<td>27</td>
<td>2.22</td>
<td>1.05</td>
</tr>
<tr>
<td>14th</td>
<td>partnerships will encourage corruption</td>
<td>27</td>
<td>3.70</td>
<td>1.03</td>
</tr>
</tbody>
</table>

* Calculated from responses on a five item Likert scale; lower means indicate greater agreement. Table does not display non-partnership policing items.

Having a standard process of interaction (Police#2) or working with formal recognition, perhaps via a memorandum of understanding, indicated partnership for police (Police#5).
When they talk about partnership policing they talk about partnership policing as if it’s a, a process of just two people agreeing on their own saying “All right let’s do this together”, but the reality is to develop a partnership, a formal partnership there’s a lot more to it… really the strategic directions are aimed so that the man on the street can understand it, but the man on the street is not entering into partnerships (Police#9).

It might be the very expectation that partnership means a “formal” partnership that might preclude their widespread use in state policing:

Yeah, well let’s face it, this is what happens—and you can get right back to your first question about [the definition of] e-crime—when people use labels and then define the label: you can’t then use what you thought of it before, you’re now restricted to what it means…Now I could be wrong they mightn’t use the term partnership formally but I am pretty sure that the partnership is the documentation and it’s a formalised process and you know you can’t use it to say it’s an informal relationship (Police#9).

Senior police were acutely aware of the politics of “partnership policing” and outlined reasons why it is unlikely that “partnerships” will eventuate in Victoria.

I don’t believe at all that we’ll be having that close a partnership. The “partnership” is almost a misnomer – it’s the relationship that we have. Relationships with people. We won’t call it partnership because that infers 50/50. Not on your life, because VicPol doesn’t really want to get into 50/50 relationships with people, because you lose control. And when you lose control you become exposed. I just think it’s a risk assessment process. Why lose control if you don’t have to? What are we going to get? Are we going to get money for it? Are you selling off half a company? You’re not. What you’re trying to do is, just by relationships, build a better way to combat the crime; either by investigating it or preventing it. It’s not trying to make a
group of part time police officers or an auxiliary police force or something like that. It’s almost an appreciation of another group – have another group – whatever it is. And say “Listen: we can help each other. Our biggest issue is to assist the community of Victoria. You have some specific expertise in that area and you can assist – and should assist – because you also have a responsibility to the community” (Police#14).

In many cases, the partnerships envisaged by state police respondents represent Deering and Murphy’s (2003) “command and control” model of partnership. “The partnerships we’re trying to form [are] so that we can see if we can actually control some of the resources out there. And when we can’t control the partnership, we don’t generally want it” (Police#14). Police even considered “coercive powers” a possibility to facilitate “partnership”:

I think it’s important that the coal-face people get together – not so much the head of one department meets with the head of another department up in Canberra and they do some cocktails somewhere at some get-together and that’s deemed to be a partnership. I think you need coal-face partnerships. The people on the ground doing the work have got to be able to get on the phone and speak to someone that’s in an organisation, and say “Look, can you give us a hand?” You know, with coercive powers or something if necessary (Police#15).

A senior police officer confirmed the way partnership policing differs from community policing:

Community policing, we’ll sit down at the community safety committees. And the community will sit down and say “We think our priority in Williamstown is people going up and down the streets in noisy cars or spray-painting at the railway station or not feeling safe at home.” And VicPol might say – and the community might be represented by a number of different organisations and VicPol might only be one – and the community
might say “We think this is our priority, and we should put the resources there” and VicPol say “Hold your horses, it’s not ours. We have political masters as well and we want you to go somewhere else.” So VicPol is trying to gather up all those potential partnerships and point them the way VicPol wants to go (Police#14).

The strategy of partnership policing might be considered “police policing” rather than community policing (Police#14).

**With whom should law enforcement partner?**

Key to partnership policing is the appropriate selection of one’s partners. Both police and private sector organisations are constrained by resources as to the number of organisations they could effectively partner. In the United States alone there are tens of thousands of police forces at the various levels of policing. While police forces are less numerous in Australia there are still seven state and territory police forces, the Australian Federal Police and other regulatory bodies that companies with national or international points of presence might wish to engage. From the police perspective there are over three million businesses in Australia in June 2004 (ABS, 2004). For law enforcement the question is also with which organisations can we partner without introducing bias or abuse into their service role as protectors of the community?

What if you get someone in there who’s a bit ruthless and you don’t like the way they talk about you? And you sit there and listen to them and you say “Why should we deal with this person, because we don’t feel they portray us or portray themselves in a professional light”? If you’re already tied in to the partnership you can’t walk out on it. And maybe the tail will wag the dog and VicPol will no longer be independent (Police#14).
Partner selection needs to be targeted carefully. The investigators interviewed for this study nominated the banking and other financial services industries, such as superannuation funds and insurance providers, as the most important industries to partner in relation to e-crime investigation, especially as repositories of digital evidence related to financial e-crime. Telecommunications carriers (PS#4), Internet service providers (Police#13) and accounting firms (Police#5) were also considered key. Partnership with telecommunications carriers was considered important to reduce the cost of e-crime investigations and reduce delays with requests for assistance (Police#9). Academic partnerships were considered important for research and community education (Police#13). Police should also be able to form partnerships with other investigators “who are accredited by reason of experience and so on. They should also be able to partner with individual corporations who have their own in-house investigative capability” (PS#4). Police reported partnering with software developers to gain access to software:

We do, well it’s probably more of a leech partnership really; we try to partnership [sic] with software developers who develop particular types of software or any software in general, because it doesn’t really matter. It may have, you may have no interest in a piece of software today, but tomorrow you need it because you’re doing an analysis which relates to something that is opened by, used by, created by that particular piece of software and you’ll need to either install it or examine it or pull it apart and see how it’s working (Police#4).
This officer stated that under the federal *Copyright Act 1968*, police were entitled to use software “for the purposes of investigation and prosecution” without breaching copyright.¹⁰⁹

But, that’s ok to say you can use it, but you’ve got to get it. So it’s always good to have a partnership with some of the providers of the more common software. So that if and when a new version comes out, there are no issues with them either providing you a free copy of it or allowing you use of it during a particular investigation and providing it to you for that. And most of them are quite happy to do that (Police#4).

However, companies need to be comfortable that “we’re not going to take a particular piece of software or information that’s supplied to us by company A and skip it out to company B” (Police#21).

Potential e-crime investigation partners for state police fall into four categories (see Table 7.2). As suggested above, in a partnership policing strategy for e-crime the police are not seeking to form partnerships with the “man on the street” (Police#9). Repeat victims and the sources of digital evidence were the partners police sought most. Relationships with private investigators in third party firms were, as seen in Chapter Six, those of “middle-men”. Police need cooperation with once-off victims during an investigation, but did not see ongoing relationships as important, when effort could be focused on repeat victims and infrastructure organisations. The status of potential partner companies is complicated when they may be both victims and “third party” sources of digital evidence, such as banks.

¹⁰⁹ A wholesale exemption could not be located and clearly does not extend to routine police work or else Victoria Police would not need to license software at all, other officers would not complain about lack of access to forensic software, nor would there be allegations of software piracy from software providers (see, Shiel, 14 August 2004).
Table 7.2: Potential private sector-police partners for e-crime investigation

<table>
<thead>
<tr>
<th>Who?</th>
<th>Onetime victims</th>
<th>Repeat victims</th>
<th>Infrastructure providers, sources of digital evidence</th>
<th>Third party investigation service provider</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>May be any victim company, any industry</td>
<td>Financial institutions, merchants, ISPs etc</td>
<td>ISPs, telcos, financial institutions, other IT service providers</td>
<td>Accounting or investigation firms, etc</td>
</tr>
<tr>
<td>Type of personnel</td>
<td>IT personnel, managers</td>
<td>In house investigators, IT security personnel</td>
<td>In house investigators, IT security personnel, general staff</td>
<td>Contract investigators, forensic accountants</td>
</tr>
<tr>
<td>Need for partnership</td>
<td>Ad hoc, depending on incident and victim capability</td>
<td>Greatest need, to address ongoing crime problem</td>
<td>To reduce costs associated with law enforcement cooperation, address crime facilitators</td>
<td>To improve services to clients; reduce costs; generate business</td>
</tr>
</tbody>
</table>

There was concern about partnering with individual organisations:

We’re the government, we’re not in the business of picking winners by sort of saying, “Oh, we’re just going to side up with Company X”. And that's why I’ve always preferred dealing with industry sector bodies, like the Australian Banker’s Association, Internet Industry Association… CUSCAL where they represent 162 credit unions, for example, rather than picking a credit union (Police#19).

VicPol can’t have a partnership with private companies… Like politics, you’re trying to gather as many people with individual links. So if VicPol has a capacity to service X number of conduits, you want the maximum number of people on them (Police#14).

The joint investigation team at the AHTCC addressed problems of one-to-many relationships:
It’s a one-stop shop. If they partner with us, they partner with Australian law enforcement. And they can deliver the assistance that they offer to all jurisdictions by coming to the AHTCC. That’s not to say that they don’t have interaction in the jurisdictions, because they do, a lot of them. But in terms of the strategic stuff, it’s best placed here. They think and so do we…[For police] it’s not about bums on seats, it’s about how can we operate effectively but as leanly as we possibly can? Because otherwise you find yourself in a situation like the US do, where every time they have a taskforce, there’s five hundred people sitting there with their own databases. It’s not about size and it’s not about how many, it’s about how effective and efficient you can be, that’s what we need I think (Police#21).

As discussed in Chapter Six, Victorian police identified their relationships with financial institutions as ad hoc partnerships. They also noted that some banks were distancing themselves from police:

We do have partnerships developed with the banks, but I’d say they’re backing away from those partnerships at the moment, becoming less and less available to us. Making our jobs harder…I’d say it’s our increasing demand. So as fraud gets bigger and we’re increasingly asking for more and more, they’re saying, “Well, we get nothing out of this. Really the fraud group does very little for us, what are we doing this for? Ok, well, we have to by legislation comply with these requests. How can we make that more difficult?” Not that they would ever use that word in a discussion, but how do we reduce the amount of man-hours we put into complying with these requests? A lot of these man-hours are taken up on telephone conversations about accounts. A lot of them are taken up replying to emails, which was a great way of doing investigations between bank officers. Gone. So just fax off to somewhere, they will allocate the request to the appropriate person who doesn’t have the level of authority or investigative skills to do anything but comply with the request (Police#7).
Other hurdles for police include reluctance in the private sectors for competitors and different industries to work together. One private sector investigator in the financial sector noted:

Telcos probably have a different focus, so I don’t know that we’re ever going to actually work in partnership. Though it may very well be the same crooks, or the same organised crime people that are doing it. But I doubt we would ever work in partnership. It would be an ad hoc relationship, where you say, “This has happened today”. And that would probably come out at a police based forum where you sit down and say, “Well, this is a fraud trend and this is a fraud trend and this is a fraud trend” (PS#11).

There was a perception among the private sector that graduation from courses, such as the Graduate Certificate in E-Crime Investigation, should provide an entrée to working in partnership with police:

I think police… need to look at what’s out there. What’s available to them, and this was a prime example, where you’ve got people who’ve done a course, you can evaluate that ok, they all pass say, “But geez, I wouldn’t let him touch a computer. But I’d let him. Well, he might be really good on a team. I don’t think he’d do the job properly, because he’s got no morals”. And you can look at that group and go, “Yeah, yeah, no”. With a lot of that key selection criteria. And I think the police really need to look at that course and make use of the people that are on it (PS#18).

While ex-police officers turned private investigators are potential partners, they should not be exempted from probity checks if opting to work to police:

Were their work practices ethical and auditable and all the rest of it since then? Has their behaviour been exemplary since they left the police force? Was it in fact exemplary when they were in the police force is another
question. So, no, sorry guys, you’ve moved on, your circumstances have changed, nothing stands still and put it this way, it’s as much for your protection as ours (PS#13).

There was some concern that multi-national corporate partners might influence local police priorities:

If it’s market driven, then our partnerships will be one of consumer and supplier in the end, because even though Australia, I think, has led on many occasions in the area of investigations online and what have you it has to maintain its level of economy… Now if these are multi-national organisations, I’m saying, it can drive a bit too much of the way our police work, rather than determining what’s appropriate for our local environment (PS#12).

Why did organisations and private investigators want to partner with law enforcement? Third party investigation firms wanted to generate business for their companies and overcome investigation barriers. Organisations that were suffering loss wanted to mitigate that loss and risk and be seen as doing so: “The bank as a business needs to be seen as doing something” (Police#16). Among interviewees of this study, reducing e-crime and promoting safer communities was not just another “cause” to which their corporations wished to attach their logo. Police commented “We’re wanting people to come in and assist for reasons unrelated to money; they’re only coming to us because of money” (Police#14). Investigators not employed by large firms were drawn more to the potential benefits to their reputation through association with police:

It’s very difficult to explain. A lot of reasons I would like to do it. I look at it – it’d pay well; but what I’m doing pays well. But yeah, it’s an area that I’m interested in. I would get great satisfaction out of collecting the evidence that
put some child-molesting pervert in jail for twenty years. That’d put a real big
smile on my face when I went home to my kids at night. Things like that,
that’s probably a greater motivation than the money (PS#18).

I wouldn’t mind being able to say, particularly to myself, “Hey, I work with
the police” and that would give me a lot of self-confidence, but they don’t
know me. I’ve got to be realistic. They don’t call on me, because they don’t
know me. I haven’t worked in the trenches along side them or along side
their buddies. They have no way of knowing whether I can stand the heat in
battle. And so you can’t blame them (PS#13).

Police note that “police-officer-wannabes” think more positively of police
(Nalla and Hummer, 1999: 39) and Rigakos in his ethnographic study of a
private security firm described this “wannabe” subculture (Rigakos, 2004:
126). It clearly exists in the private investigation field also.

Besides confirming the qualifications of potential partners the benefit of
partnering must be clear, “You don’t engage just for the sake of having a
partnership: There’s got to be some benefit out of it” (Police#20). Selection
also involves ethical decision making as described by one police
respondent:110

It’s almost a moral dilemma. Do we sit down and say “We won’t partnership
with this person, because we don’t believe they are of good character or we
don’t believe they’d behave ethically, they’d charge too much.” Haven’t got
to that stage yet, but they’re the issues I’d be thinking of. Straightaway, I’d be
saying, “Well, we don’t – who makes the call that we don’t like this particular
company? Or who controls it but doesn’t head it? What if it’s controlled by
someone who might have links to criminal aspects? How long are they a

110 Marx (1987: n.2) noted this complexity when one branch of the US Justice Department
partnered IBM, while another sought prosecution for antitrust violations.
criminal for? Are they someone who committed a child sex offence when they were 20, like a teacher, and someone who was 16 and now 20 years down the track they’re heading something else? Do we deal with them? Does it mean that we got to do probity checks on everybody before we do it?” I can’t answer it (Police#14).

Others noted the potential hypocrisy in making such judgments:

Who are we to say we don’t think your corporate governance is good enough to go into partnership with? Based on what’s going on everyday in the newspaper? Who are we to say we’re not getting in bed with you, because one of your directors was charged with fraud? …At the end of the day, we can’t go out and lecture to someone about corporate governance and to be seen as hypocritical. So it’s a two-sided thing. We can’t go into partnership because your corporate governance is crap and you as a private sector person go “Well we can’t go into partnership with you because your governance is RS”.... And my knowledge of what’s going on is the same knowledge that they’ve got, because they’re reading it in the paper. So it’s a two way street when it comes to partnerships and governance (Police#6).

Police respondents generally opposed partnering those who conduct criminal defence work as a moral criterion:

I don’t want a partnership with Company X who does defence work, because their aim is “I don’t give a rats, I don’t care whether I believe the person or not. Hey I’m making a profit, a lot of money, therefore that’s why I am doing it”. I say “Well, here I am prosecuting that person, because they are a piece of crap, they do need to go to jail, they need to have some punishment, yet you’re fighting with me and then two years down the track you want to jump on board with me because you reckon what I’m doing is a great thing, but you’re still doing defence work?” So like, we don’t work that way, because there are certain ethics that need to be followed and it’s like you can’t make
the money doing the bad thing, what I consider a bad thing, because you know this person is a piece of crap, but you’re going to get ten grand off him. However you want to jump on board with some of these prosecution cases, because you want to be seen as combating the crime as well (Police#5).

At the first meeting between Victoria Police and the investigation firm to discuss a possible partnership, the very first “hurdle” related to whether the company undertook criminal defence work. It did not and so the discussions continued. The firm formed by CCS members had also chosen not to undertake defence work.

We don’t do defence work at all, that’s just a moral thing that we all decided on. We don’t agree with it, so we’re not going to do it… And we know that investigators are usually bang on the money and it’s just a moral thing we all decided that that’s not what we want to do. And at the moment, we can’t do it (Police#2).

Despite all this, senior police argued that the fundamental question of whether Victoria Police should conduct investigative partnerships has yet to be answered. There was a danger of entering into investigative partnerships before Victoria Police was ready for them:

Not unlike the partnerships with universities, where we might get in and have a partnership with one university and the university may make money out of it and then on the side there might be another partnership with a similar course going on with another institution and you’ve got the same problem: then you’ve probably exposed yourself to the threat of legal actions and it becomes messy. We’ve got to come to grips. In principle, are we going to allow outsiders to do investigations? When that decision’s made, then we go setting the criteria. Not the other way around, I believe (Police#14).
Responses to a *Regulated Intersections* model

Interviewees were asked to comment on the normative model proposed by Sarre and Prenzler (2000), their *Regulated Intersections* model (see pp. 84-91). Support for a model of limited and regulated interaction between police and private investigators was divided evenly between the respondents, but did not reflect a police versus private investigator split (For n=15; against n=15; noncommittal n=5; missing n=6). There were divisions within each group. Those against regulation argued:

Part of this stuff is a good will exercise. If you make it more difficult for us to do it or if it’s regulated, I think you’re going to make private industry less likely to engage. I don’t know why you’d want to do that (PS#10)?

Formal regulation through an oversight body seemed completely at odds with the notion of working in partnership:

Unless it’s voluntary and unless people self-regulate, I just don’t think it works... And it creates an inflexible environment for people to actually do their business. It creates a suspicion and also a distrust of, in my case law enforcement, because they’re then scared they’re going to break the regulation and be penalised for it. And so they’re constantly concerned with compliance as opposed to doing the right thing and being good corporate citizens. I don’t agree with regulation and being careful how closely you interact. You just need to do it with maturity. And a lot of times that just comes down to the people you’ve got working in the places that you do... that’s why you’ve got the core values of the organisation. And you adhere to them. That’s why we’re regulated from within with the professional standards type people... My opinion is that as little regulation as you can

---

111 Chapter Six reports the respondents’ views about the current nature of interactions according to Sarre and Prenzler’s descriptive models of interaction.
possibly get away with is the best model, because [then] people are there at
the table because they want to be and not because they’re forced to be
(Police#21).

Limited interaction would also be counter-productive to addressing e-crime
the likes of phishing: “the crime type that we’re looking at here is different
because it’s constant, ongoing and involves the same institutions. So we need
to have that ongoing relationship” (Police#18). Perception about regulation
already impedes e-crime investigation, as discussed in Chapter Six:

The perception that organisations can’t give the police information causes us
dramas even when they can actually give it. If you put in regulation to say
that you’ve got to have particular, for example, court orders to obtain
information it does make it very difficult and time-consuming to do things
(Police#18).

Most respondents did not see the need for additional regulation in the area of
police-private investigator interactions. “To a large extent it already is
regulated, because you’ve got to have search warrants, there’s got to be a
criminal offence, what we can and can’t release is essentially regulated under
the Privacy Act. So, there’s already a lot of regulation there” (PS#11). There are
also the Evidence Act 1958, Crimes Act 1958, Magistrates’ Court Act 1989, Police
Regulation Act 1958 and associated regulations, policies and procedures
(Police#6) and the Confiscation Act (Police#11) that regulate interactions.112 The
formation of partnerships would not avert the myriad regulations already
directing police-security interactions: “Just because we’re in a partnership
doesn’t make the information you gather admissible” (Police#6). As one
investigator from a multinational company put it:

112 See also Sarre and Prenzler (2005).
If we were just to hand over the intelligence we gathered during an investigation to certain countries, they couldn’t use it for evidence, they’d just have to just maybe use it for intelligence purposes. We work with [police] to understand what this information means, how it can be useful to them and then we also have our people and our legal department in different places… we’ll try to do some of the due diligence for them on the legal side of things and say, “based on your country’s laws we can do this or this information would be good as evidence.” So, we know resources are limited and we try to use our resources wisely and try to help them as well. We try to do our homework (PS#8).

Victoria police officers also considered that the interaction was regulated already, because “we are telling them what we want” (Police#14). Another noted that if the intention was to prevent police methodologies and knowledge passing to the private sector, then one need consider that most private investigators investigating e-crime in Victoria are already ex-members (Police#4). Private investigators of e-crime were distinguished from other “private security” industry personnel like security guards and crowd controllers. Respondents believed investigators needed less regulation arguing they interact less with people:

I understand it for security guards and the like where they’re interacting, they’re bouncing heads at the front doors of pubs and wearing their numbers and you know all the issues that come from people interacting with people. But out in the market place but this is closed shop, it’s sort of remote, it’s electronic, it’s information gathering, it’s intelligence gathering, it’s putting together a full brief and all the other material that goes along with it, computer records and the like and then using analysts to crunch that and make meaningful predictions or meaningful estimates as to how the funds have actually been moved (Police#10).
This did not consider that investigators interview and interact with people as a main aspect of their work, just as police do.

Regulated interaction would add an unwelcome bureaucratic layer according to police who hypothesised what would develop:

So, I need forensic accounting, I don’t just ring [company] and say can you come down here and do this job? I’ve got to put in a report attached to what I require, goes through a senior sergeant for yes, it’s required for this investigation. Goes up to probably though the Super to probably to a public service person within the Victoria Police force, but an unsworn member who has to allocate certain number of quotes to auditors to get the work done. That’s right. Ok, so hands off. It then comes back down. And you’re going to chuck on a terrible bureaucratic layer that will delay things and there’s always the risk of it won’t happen, even when you really need it, because of perceptions based on how reports are written. Or that investigation or that victim at the time. Or they can pay for it themselves (Police#7).

Limited interactions would still need to allow contact during an investigation:

Once that system’s up and running I would really love to be able to speak to an auditor and ask them a question, while my investigation’s on the run. Alright, we’ve used you a few times, I got to know that auditor, I want to be able to give him a phone call and say look I got this issue coming up, can you just give us a hand? Go out there for a one hour meeting. He doesn’t charge me for it. And it helps my investigation move forward (Police#7).

Private investigators did not support a requirement for presentation of evidence packages with reports of crime, discussed earlier in Chapter Six, because of the additional costs that would place on their organisations:
Should there be standards? No. They’ve talked about a model of “We expect a brief that comes to us to be like this”, only qualified people can do this—this is the fraud squad—and then we will investigate it. But to do that you would need to have … access to criminal records. And you’d need to have access because, what do you know about the person you’re going to knock on the door of to interview? In any sort of thing like that there has to be a bit of give and take and you can’t expect there to be an exact standard. That’s one of the misunderstandings I think the Major Fraud Group has. They see the word “bank”, and they think we’re all the same. [This financial institution] is a very small entity… Our resources compared to the resources of [X] are a lot smaller. So we don’t have the ability to go and do all this sort of stuff to the same level that they do. I don’t know that type of model’s going to work. It has to be a relationship thing. It’s how you develop that relationship and how you manage that relationship is how you’ll react. We might come and say “We’ve got this huge fraud, we’re not sure, we know this, this, this and this, can you help us?” Whereas, if it was a [another company], they might say “Well, you go away and either get someone in to look at it”, or “You’ve got enough experienced investigators yourself to be able to do something about it”…If they go down the line and say “Only certain practitioners can investigate it to our standard” the cost to your [accounting firms] and that sort of stuff, who would be the certified practitioners, is pretty big… they can cost five grand a day for one person. Now if it takes them twenty days to investigate a fraud that might be a hundred thousand dollars, there’s 10% of what you’ve just lost you’ve got to add on top of it. Now, the courts to date haven’t been terribly good about going “Well, you now owe that [company] 1.1 million dollars”. They tend to go “Well, you owe the [company] 1 million dollars”. So, there’s an immediate on-cost (PS#11).

If such a standard was introduced it should be for corporations and not individuals. “If a little old lady is defrauded of half a million dollars, the
police should investigate it. They shouldn’t say, ‘Oh, you go and do it yourself and come back and see us’” (PS#11).

Police stated that any formal investigative partnership with the private sector would occur under the auspices of a memorandum of understanding, “but the MOU is almost like a contract. We call it an MOU, but essentially: someone puts their foot out of line, we can pull out of it” (Police#14). If partnership takes on a contractual form, then it is likely that they will become standardised as a customary format. Crawford (2005) argues that contracts are not real options, because by the process of standardisation the original ideal of negotiated agreement is lost. With the agreement already in black and white, there is only the choice of whether to accept or refuse it. There is a lack of bargaining power to adapt the standard “contract”. Crawford (2005) calls this liberal intent with an illiberal outcome.

Support for regulation was based on weeding out undesirables:

I firmly believe that private sector investigators should be regulated. I don’t disagree with that at all, we have far too many …in the past there have been far too many charlatans in the field. I think that there needs to be a greater formal cooperation between law enforcement and recognised private investigators. Life is very difficult for private investigators who are doing the right thing out in the field to source information and to source cooperation (PS#1).

It would also reduce innuendo about corruption (PS#1) and to manage risks of unintended outcomes:

When the police – when they eventually get around, if they do, to referring victims of crime to us to vet and to screen and what have you – eventually, there will be a case that goes wrong for whatever reason. So the person gets
charged money and they don’t think it was good value for money and they go to the police. I think we’ve got to minimise that and we minimise that by only putting accredited people onto the list who can really do the work (PS#4).

Police considered extra regulation would be required if investigations became corrupt. Examples of private investigation that concerned them included offering to let offenders pay back money with no other repercussions or offering money for information during an investigation. Whether investigative partnerships with police should be publicised or not was raised by a respondent. He argued that working in partnership with police must not be publicised as a matter of investigative and personal security:

You would have to say, “Look you can’t advertise that you’re on our panel. You will keep your mouth shut”… because you can be caught. Well, first thing is you wouldn’t want the crime syndicates to know who is working with the police, because an individual is only an individual at the end of the day. And I may be watching too many American movies, but I’m sure that even in Australia there would be cases where an individual inadvertently says that they do something, the wrong ears hear it… So I think that it’s very important for the wellbeing of all concerned that they’re never allowed to articulate that. I think that’s very essential for the wellbeing of everybody and the security of the police (PS#13).

It was a concern echoed by POLSEC (7 Mar 2006, personal communication) and committee members observe a Code of Ethics and sign a non-disclosure agreement (NDA) (see Appendix D: POLSEC partnership documents). Under the NDA, police may suspend or terminate committee membership for disclosure of sensitive or confidential information and instigate inquiries or investigation. Few other respondents were circumspect about entering partnerships that would receive public attention:
Taking it from our perspective, [my organisation is] striving to be in the top one hundred in the world, it’s reputation is quite important and it would probably be unlikely to engage the police in a partnership, unless there was clearly possibility of improving [our work] or including a profile in [assisting policing]… You would only form the partnership in a discreet way (PS#12).

Generally, respondents considered the ability to advertise partnership with law enforcement as a key benefit of entering such an arrangement:

Companies need to, for success, we need to show positive. We need to show what we’re doing, because there’s so much negative that’s in the press without your doing. I think the success is sending the message that we’re going to find you. We’re looking for you, we’re partnering with law enforcement (PS#8).

Awareness is an incredibly useful fraud prevention tool. And there’s no reason to keep these sorts of partnerships [quiet]… in fact you should celebrate it. We see some real value in working together. There is no competitive advantage in somebody losing money through fraud. So all of us, all of the banks, are all sitting down together around a table with the police, with Tax, with this, with that. We’re not going there to try to pinpoint people or breach privacy or anything like that. We’re trying to protect every person’s money…There’s something to celebrate in that (PS#16).

Instead it is law enforcement that is held back from publicising incidents (Police#17). Police are loath to release statements to the media about investigations until a prosecution is finalised with no further appeals and this is less helpful for victim organisations. Law enforcement wants victims of e-crime to identify themselves to the public on their own accord and state that they have prosecuted offenders successfully.
Those who supported regulation of interaction between police and private investigators generally offered qualified support depending on what form of regulation might be imposed. For example, management, perhaps even similar to an informer model, might be favoured, however additional legislation was not (Police#5). Existing bureaucracy could be put to use for partnerships (Police#8). However, it needed to be flexible and permit crisis responses (PS#13). Standard forensic computing processes and procedures would provide a form of regulation stipulating that “at any stage you can be criticised, ‘No this is how I did it. This is what industry standard dictates. I have the same standards, so do you.’ … It’s not managed by any one person, but it’s: this is my job, this is your job” (Police#5).

Additional regulation should facilitate the process rather than wrap it further in bureaucracy, such as a ‘request for information notice’:

We should be able to serve some sort of notice on a business [other than a search warrant] that gives them comfort that they can actually hand things over to us. Most people want to help out, most individuals in organisations want to help, but they’ll have their own corporate rules and regulations (Police#15).

Accreditation might not prove problematic despite current objections:

Banks are all jumping up and down saying ‘No, we’re never going to wear [accreditation]’, but banks have all got somebody who is going to be accredited to the right people, because we’ve all got the same skills. So, somebody will get accredited, every brief that will go to the police will go to this person, they’ll probably check it, sign it off and say this brief is up to scratch or it isn’t (PS#16).
Overall, it was believed by some that regulation of investigative partnerships would be “reactive”:

> It’s really going to have to be like everything. Going to have to put your foot in the water, see what it’s like, what happens, what’s the downside of it. Then start fixing it up. It’s all very well to say “We’ll set up a rule, someone has to be accredited” and all that and a huge infrastructure – who polices the bloody thing? Who regulates it (Police#14)?

Contrary to Sarre and Prenzler’s (2000) suggestion that licensing of private investigators occur through an independent third body, investigators in this study preferred accreditation by police:

> I think it has to be accreditation by the police themselves, because they have to be comfortable with the person that they’re working with and if they think that person has contacts that he may be passing information on to, who shouldn’t be getting that information, then they’ve got to have the right of veto (PS#1).

However, there is uneven regulation of those who undertake e-crime investigation in Victoria, on the basis of whether they work for multiple clients or a single client (their employer). Many investigators have claimed exemption from licensing by virtue of section 4(h) of the *Private Security Act 2004* (Vic), which exempts personnel who conduct their inquiry work on behalf of an employer that is not a private security business (AIPI Victorian Secretary, 22 Feb 2006, personal communication).113

---

113 This is a continuation of an exemption in place since 1966. While “private security business” is not defined in the Act, it can be inferred from section 14 that this refers to “the business of providing the services of other persons to carry on any one or more activities... acting as an investigator”. Arguably this means offering for external hire, which institutions such as banks do not.
In fact, accreditation of private investigators by the Ethical Standards Department of Victoria Police was seen as “the ultimate in terms of no vested interests, in getting a background on people” (PS#1).\(^{114}\) Support was not common for this:

> I would think, why would I need to have an ethical tick to be working in my industry when I didn’t need that to become a member of the police force? Why should the standard be higher now that I’ve decided to leave the police force than when I was in it (PS#16)?

### Additional powers for private sector investigators?

Prenzler and King (2002: 5) documented calls from the private security industry for additional police-like powers in other Australian states, with all but one of their respondents arguing that licensing should entail greater access to government-held and some privately-held information. The Australian Institute of Private Detectives propose greater access to police information, arguing that for private detectives to not have access to the same information as police under privacy legislation is to undermine the right to a fair trial (AIPD, 2005). Two senior Victorian private investigators who participated in this study also called for reform to search warrant powers that would assist their investigative practice:

> What we’d like to see as a change is: we’ve got the right to go down to the police and say we believe this is a [criminal] matter and we’d like a warrant. The police look at it and they say ok. It’s not reported formally. So it’s not like

\(^{114}\) As a partnership initiative, there is an understanding within the main POLSEC committee not to discuss licensing issues and these are referred to LSD (POLSEC, Victoria Police, 24 Feb 2006, personal communication).
we’ve gone and made a complaint to the police… The police come along and they take us down the magistrate, he sees us, who we are and we say to the magistrate, we believe if we examine this information it may lead to us being able to prove a wrong-doing and the magistrate says, “Yeah you’ve got your warrant”. That would aid a lot of investigation and cut down a shit load of police time, plus the cost back to the client and it’s still not having us becoming pseudo police. We simply have authorised access (PS#15).

The proposal called for a dedicated “desk” or other oversight mechanism by which private police would apply for these warrants or information as contact through individuals member could breed corruption (PS#15). Of twenty-seven survey respondents, two thirds agreed or somewhat agreed that private police should have greater access to police intelligence and information (n=18). Forty-eight percent believed they need greater powers to investigate e-crime and should be able to apply for warrants to conduct searches (n=13). Most interviewees opposed additional powers for private investigators (n=18, 64.3%); although some would support access to criminal records and habitation checks if police demanded briefs of evidence (PS#11; PS#16). Prenzler and King (2002: 6) suggest that these “proposals are worth considering in terms both of the interests of justice and to reduce the demand for illicit information”. The benefit of this suggestion to the public interest and public police is not clear. Such a mechanism would likely increase police workloads as they escorted private investigators to magistrates and more incidents came to police attention, whether reported officially or not.

Law enforcement respondents were cautious about taking such a route:

All that is doing is setting up a mini-police force. Other than one that is State regulated and not regulated under any other legislative body or review panel. I would say that’s probably a dangerous way to go down the hill… If there was that issue a simple solution from a policing perspective or from the State government perspective if they wanted to amalgamate these groups would
be induct them into the Force, swell the numbers in the area, have a business liaison section which would go out and provide the service and advice and direction to business (Police#4).

I think once you open up those doors you’re really starting to open up the corruption issue... You start releasing information like that it’s going to be abused. Most police forces try to keep the way they do the business within the protocols, and there's legislation within that to ensure that officers do their job properly without stepping over the mark. You let it go outside, it just opens too many doors (Police#17).

Those investigators who called for additional powers were not saying they wanted to involve police earlier in investigations:

I don’t think there’s any need to involve them until we make a conscious decision that we have sufficient points of proof to supply them with a brief. I think we’d be wasting their time …We ring up and say, “We’d like to come down and discuss this job with you, what do you think I should do?” And really what I’m saying to them is: “I don’t know what my role is, that my professional qualifications are not really good enough, I need to be told what to do” (PS#1).

The issue was not competence, but facilitation. “Saying you’ve got to do the investigation, give us the tools to do it” (PS#16). The need was recognised by some police, especially in terms of activities such as tracing IP addresses:

I think there should be recognition that the people out there need the information just as much as the police and their job relies on that information and they, you know, it may be necessarily [they] can’t go to the police or it’s not a police matter there. Why should their task just hit a brick wall because, or they’ve then [got to] go the next degree and get out, take out court orders and things like that to get it? However, I don’t see it as a one way street. I
don’t think that they should just be given all these additional powers without some sort of responsibility placed on them to have those powers as well. Again they’re dealing with people’s personal information, they should, you know obviously have to deal with it correctly and not be able to misuse the power … there has to be restrictions on it as well (Police#9).

Extending search powers might be acceptable if would alleviate the work backlog for Victoria Police. “Yeah, you can go in and seize a computer, image and give it back” (Police#6). Private industry can already apply for Anton Piller orders to conduct searches, although these are limited compared to police search powers.

I would rather see the power go to an ISP investigator to enable him to gather more evidence to hand to the police to make their job easier…I certainly wouldn’t like to see private industry doing raids. It’s too easy to step over the mark… It’d be better if the private sector was gathering more information and getting it together better for the police and saying to the police “Hey look here’s these 37 people that we’ve detected, they’re running their own little chat room on our Internet service and they’ve downloaded all these images. Here are the log files, here’s a copy of all the images. Here’s the chat room, here’s their IPs. Here’s their phone numbers, their addresses and here’s all the evidence” and the coppers go “Yep, well let’s go see the magistrate, let’s get the warrant and go kick in the door and seize all the stuff. That’s then a police matter.” Ok. That’s going to save the police thousands and thousands of dollars. It’s going to be easier for the police and easier for the ISP. And it puts more of a sense of responsibility on the ISP and I think that you would find that the Internet in Australia would be cleaned up dramatically (PS#18).

Police suggested that private investigators should be able to purchase information from government agencies (Police#10):
Now, my argument has always been that the Victorian government is in possession of information, things such as car registration details, licence details, individual’s photographs on their licences and criminal histories. Now, if a person is a licensed private inquiry agent and passed all their appropriate courses and so forth, if they were to sign a contract with the state government to say that they wanted access to this information for legitimate purposes, being … investigation of criminal offences, the investigation of civil matters where it is necessary to determine the whereabouts of the individual or something – they’d just list all the categories and then each time a private inquiry agent wants a car registration he just fills out a form: “Car rego number required for… determine ownership or whereabouts of X, Y Z,” and then at the bottom of it, it says “I’m doing this in full knowledge that if I do this for any other purpose than specified, I’m guilty of an offence – two years in jail, or $1000 fine” and signs it. Send it through, the government would earn $70 or something each time it happens, this guy gets the information, he provides it to the law firm that’s trying to determine whatever they are trying to determine (Police#15).

Regulation of such a scheme would rely upon hefty penalties according to this respondent. Equally, this respondent was in favour of police paying the private sector for provision of information for criminal investigations. Other police argued that public police requests for information should be fee free (Police#10).

Most private investigators believed their industry should not be granted additional powers: “Police should accept what they are assigned rather than do nothing or consider private organisation powers. Real relationships, formally accredited and acknowledged are a consideration” (PS#21). Decisions about granting additional investigative powers to private industry
need to consider the broader balance of law enforcement and crime prevention:

You don’t need police powers to be proactive. That’s where the private sector should be heading. I totally believe that and if you give them police powers all you’re doing is pushing them down the wrong direction. I think you keep resources pointing in the right direction, police do policing and make the private sector have to deal with the police if they need policing or find a niche and that’s to be proactive rather than reactive (PS#17).

As an example of this, security industry members do not receive any police powers through involvement with POLSEC.

**Responses to partnership mechanisms**

The remainder of the chapter draws upon the three case studies and discusses the respondents’ responses to public-private investigative partnership configurations that Australian police have or might pursue in relation to e-crime investigation.

**Joint investigation teams and secondment of investigators**

The Joint Banking and Finance Sector Investigation Team (JBFSIT) of the AHTCC is an active public-private partnership based on secondment of bank investigators to law enforcement (see Table 2.3, pg 34). The formation of the team was recalled thus:

First phishing scam: April 2003. Fake Commonwealth Bank site, we went to Sydney, we locked this bloke up, charged him with money laundering. New South Wales DPP dropped the charges because there was no evidence, which was the correct thing to do, and then the floodgates were open. So we’re saying to the banks “We can’t do this without you. You’re going to cop a
whole lot of losses” and they said “That's cool, you know, we’ll risk manage it”. And in the end they couldn't. It's one of those things: it gets to a threshold. Ad nauseam meetings, two steps forward, one step back, and in the end, till we get to them saying “the Joint Team”: a genuine public-private partnership, where policing doesn't have the resources nor the expertise, nor anything else and the bank account sector can’t do it by themselves: working together. And that’s how you see it today (Police#19).

An AFP agent who reports to the Director of Operations heads the JBFSIT. There is no specific government funding for the JBFSIT. Funding is drawn from the $1.7 million annual federal funding allocated to the AFP to fund the AHTCC. State police agencies and corporations meet the secondment costs of their members (Senate Legal and Constitutional Legislation Committee, 2005). The JBFSIT public-private partnership is formalised through Memoranda of Understanding between the AHTCC and each external organisation. Secondment agreements formalise an individual’s secondment. These MoUs and agreements focus upon reporting structures, information sharing and privacy. They were not available for review in this study.

Here, in this one team, the bank staff are actually brought in as contractors to the Australian Federal Police. They get a security clearance, so they’re actually subject to the AFP disciplinary requirements.115 They’re managed here in that even though they’re a bank employee, they become privy to information that they normally wouldn’t see. They use that information to do their job, but they don’t pass it back to their bank (Police#18).

---

115 Although hosted administratively by the AFP, the AHTCC is a separate organisation (Police#18).
Bank secondees signed secrecy agreements and are criminally liable if they breach their responsibilities (Police#20).\textsuperscript{116}

So we actually give them access to our criminal investigation case management system. So they can see criminal history information; only what’s in our system, the AFP system, which isn’t a great deal since most crimes are state based. So they don’t see people’s main criminal histories, which are maintained by the states. But they’re privy to any information that the AFP might hold, unless it’s bound at a higher level (Police#20).

Unlike Hoogenboom’s (1991) analysis that characterised the “old boy network” and moonlighting as a unidirectional dispersal of police culture into the private sector, secondment of private investigators into police forces offers a means for bi-directional learning and practice. A major success of the JBFSIT has been overcoming under-reporting of incidents to law enforcement by the banking sector:

Before we had bank secondees here, we had agreements with all of the major banks that they would actually supply us with the information that they’re supplying us now. Before we got people physically in the door that just didn’t happen. We’d occasionally get bits of stuff, but I think if they’re disclosing losses and they can’t see what’s happening with it—they’ve got no input into the control of it—there’s that real reluctance, because they don’t want that to be disclosed publicly (Police#18).

This strategy of secondment is a clear example of Bradenburger and Nalebuff’s (1996 cited in Geis and Geis, 2001: 18-19) “co-opetition” where the five major banks competing in the Australian banking sector work together to address problems of phishing so as to encourage and defend the growth of

\textsuperscript{116} Police secondees were sworn in as special members of the federal police giving them Australia-wide jurisdiction for Commonwealth offences (Police#18).
the Internet banking market. The initiative creates an intersection of public, private and police interests. The procedures put in place encourage that cooperative work:

What we’ve been doing to collate [information from the banks], we’ve set up a separate database that we’ve put that information in. So each bank secondee only has access to their own bank. They don’t have free access to the other banks. So each bank secondee then inputs the data from their systems that we need into our central database that they all have access to. And then from there we go forward (Police#18).

When establishing the joint team, restricting police access to bank information was a greater concern than secondees releasing police information. “So that we don’t see it in the first place, because the banks can’t do anything to us to stop us from misusing it” (Police#20).

In the JBFSIT, bank and police secondees assemble target packages on suspects deemed worthy of prosecution that are then forwarded to the most appropriate jurisdiction, often a state police force, for prosecution. That work is reactive, based on referrals from the banking and information technology sectors, AusCERT and state police. However, there are plans to introduce proactive education of bank and police investigators. The investigations are mostly office-based, interrogating the banks’ systems, working up patterns and finding the information needed to target suspects (Police#18).

And we might have, for a particular job there might be a lot of victims from one particular bank, the staff from all of the banks will contact victims to get statements. So we share the load around. It’s not “it’s your bank’s customer so it’s your problem” (Police#18).
Occasionally, team members travel interstate to serve search warrants and interview suspects and witnesses, accompanied by local state police. Police still “call the shots” in these joint investigations, because “if it’s a police matter, it’s a police matter” (Police#20).

At the time of this limited case study, the AHTCC and the JBFSIT have had few high profile prosecutions (Police#19). On his departure to the private sector one year after the AHTCC opened, the previous Director, Alastair MacGibbon explained this:

We have three or four people before the courts in relation to Cybercrime offences — and they are still before the courts. Part of that is because this is new ground for a range of people. It’s new ground for us, the prosecutors, the defence and for the court system itself… In relation to the lack of high profile cases, you need to cut your teeth and develop a reputation of being helpful to industry and taking on complaints. We’ve started doing that, but this is a long, long road… With proactive policing you will often fail as well, because you can look at a person or group with an expectation you will find them doing something and they may not be doing it at that time. [IT related policing] is prone to a success rate that is not as high as other industries. But I’m comfortable with how we have gone with investigations. (Bajkowski, 2004: ¶ 18, 22, 24).

The AHTCC does not produce an annual report that is available publicly. Internally, monthly fraud figures are compiled by the JBFSIT. These figures are aggregated to avoid highlighting the performance or otherwise of any individual partner bank. Success is also measured through coupling of qualitative and quantitative indicators, such as disruption of criminal enterprises and estimations of mitigated loss versus investigation costs:
That you may not be able to release publicly, because it wouldn’t make any sense, but certainly to the powers that be, and to our political masters we can demonstrate that this was identified… Classic example is this: a phishing site comes out on the Internet and … we are able now to take that Internet site down in a matter of hours using our contacts, in AusCERT and things like that. If the AHTCC hadn’t developed that type of methodology and that website was up for three weeks… On the law of averages, if we average out what these things actually realise in terms of profit, this is how much we’ve stopped, because we took it down in two hours, we didn’t leave it there for three weeks (AHTCC#6).

Successful prosecutions are slowly making their way into the public domain, such as that of teenage hacker, Stephen “Susboy” Sussich. During routine maintenance, Webcentral staff detected an intruder on one of their servers. The AHTCC analysed the hard drive of the compromised computer. The unauthorised user had been storing and distributing copyrighted movie and music files and scanning for other vulnerable computers. They traced the IP address to a Melbourne home from which the connections had been made. A search warrant was executed at Stephen Sussich’s residence on Wednesday the 28th of September 2005 at 7:05am. He and his family were in bed and the computer he used was switched off (AHTCC, 2006). Preliminary analysis of the home computer found evidence sufficient to seize it and arrest Sussich. That hard drive was analysed by the Melbourne AFP Computer Forensics Team. When interviewed, Sussich made admissions about his unauthorised access of the Webcentral server. He was charged and bailed (AHTCC, 2006). Sussich pleaded guilty in the Melbourne Magistrates Court to two counts of unauthorised modification of data to cause impairment. He was convicted and fined $2000 and order to pay $3000 compensation (Butcher, 14 Feb 2006).
Recently, the JBFSIT team also participated in a worldwide operation that closed down 1400 phishing sites, including thirteen sites based in Australia (Keelty, 2005). The JBFSIT includes in its successes recent moves by Australia’s major banks to impose daily, monetary limits on Internet banking transactions to reduce the rewards from phishing. Most recently, following investigation by the JBFSIT, a Victorian man was charged with using a telecommunications network with intention to commit a serious offence, which carries a 10-year prison sentence. He was alleged to have used a botnet to attack Australian Internet relay chat servers (The Age, 22 Mar 2006).

The physical presence of investigators from across Australia was considered a key factor in the success of the team:

There is the obvious benefit of you’re talking to people from other jurisdictions face to face rather than over the phone and things do happen – things can be organised to happen a lot quicker. Because if I ring another state police force and ask them to do something, it doesn’t happen as quickly as if someone who works for that police force rings them and asks them to do it. So if I want something done in Tasmania, for example, I can ask the Tasmania Police secondee to organise it and it will happen far quicker than if I try to organise it myself (Police#18).

While bank secondees do not possess police powers during their secondments, they felt more power to achieve results and receive feedback about that:

It’s one of the main functions of us to coordinate the investigations. We may work a target up, as such, and refer that off to the appropriate State police. And it does seem to hold a bit more… like I’ve sent a couple off recently, and had phone calls about them saying, like could you just give me a bit more
information? That’s more than what I was getting when I was in the bank. As in, they’re going to do something with it... Tends to have a bit more credibility coming from here than coming from the bank...It’s great here, because we can coordinate one investigation here; we’ve got the main banks here. If we need to share information, we’ve got it all. I don’t know, it just seems like I feel I’m a lot more confident when I send out my briefs and my whatnot from here, than I did when I sent it at the bank, because most of the time, like I said, because as much information as I gave out when I was at the bank it never got any feedback. Wouldn’t have a clue if that person was arrested or prosecuted. And there were a few incidences where they actually had people. They had apprehended people... but we never heard anything (Police#16).

Increased networking through personal relationships was a benefit for police secondees also:

This [is a] new environment for me, but I came here to learn and to make those meetings with people, those friendships even and working relationships with other people. And that has started to happen for me. I know now [that] I can now go to certain people and say “Hey, I need this, this and this” and I talk to them on the phone and they go “Yeah, yeah, yeah, send us the official bit of paperwork through” and you know it’d get actioned, rather than just putting something out there and not knowing who is at the other end of it, send you back something and you think “Oh, it’s not quite what I wanted”. So, yeah, I think that’s important (Police#17).

In terms of Sarre and Prenzler’s models of interaction, the members of the JBFSIT were united in describing the joint team as a Combined Forces model, with sectors combined permanently and symbiotically at executive and operational levels. Despite this, the JBFSIT might not represent permanent symbiosis between the sectors.
Where the police are here for two years, some of the banks only signed up for initial periods of three months, which has been extended on a three-month by three-month basis. Some have signed up for a year and then at the end of the year they’ll look at whether they’ll renew or not... There’s not the long-term commitment from the banks that there is from the police services. But that doesn’t mean to say that there won’t be, it’s just that they haven’t given [that commitment] up front (Police#18).

An investigator in Melbourne, whose company had seconded an investigator with the joint team in Canberra, was quite firm in noting that his investigator would be involved in the team only as long as it served the purposes of his company (PS#19). In this manner, private sector partners construct power within the partnership through the underlying “threat” to withdraw their support and resources. It was recognised that the constituency of the team was not permanent:

There is no perfect blueprint for doing something like this. This will change tomorrow. They’ll introduce a particular security instrument that blows phishing out of the water and the next day there’ll be something different. And it’ll be something to do with the stock exchange. So we’ll have the stock exchange in here... And I think that, I think that it’s – how do you explain it without sounding too corny – it’s the relationships. It’s not a business model. It’s the relationships that make it work and I think that once people realise that this model it’s not intended to threaten anybody, it’s not intended to act as a common police service, far from it: it’s basically meant as a centre of excellence that provides assistance and coordination and training and all sorts of things to the jurisdictions. I think that that’s the key... And it may very well be in the future, and it will be in the future, that for a particular investigation we’ll bring someone on, we’ll sign them up under a secondment
agreement and then once the job’s done, they’ll go back to their organisation (Police#21).

It is the aim of the AHTCC that as e-crime evolves, investigation of different forms of offending should be “pushed down” to state forces (Police#20). If the AHTCC is doing the same thing in ten years time it would have “failed miserably” (Police#20).

The architects of the Joint Banking and Finance Sector Investigation Team have built the trust between partners that Flemming and Rhodes (2002: 195) consider the central mechanism of networks. It was argued that investigative partnerships in other countries have yet to move beyond rhetoric:

They say “Oh, we’ve got a seat there for the bank person to sit, but they don’t sit there”… It’s only on a needs basis…By having the five banks seconded here, it’s just never been done anywhere in the world… I don’t think people realise now how hard a work it was, the meetings we went to that went nowhere. And then we got the support from the card companies, the credit unions (Police#19).

It is clear that the team capitalised upon shared values and norms and negotiated the divergent organisational cultures (Flemming and Rhodes, 2002: 195). Cautionary lessons from the JBFSIT initiative include not over promising “partnership” or results:

I think we may have even fallen into a number of times the trap of over promising, under delivering. So that would be the thing I’d be most wary of. Saying “Yeah, we can take on your investigation” or going to conferences, and I’ve done a lot of speaking at a lot of conferences, some big ones and we’ve said “Yeah, we want to work with industry”. And so they hear that and they
ring up and say "We’ve got this job" and we knock it back, that’s not good (Police#19).

Defining the boundaries of the team’s work was also important:

We really need to put a fairly strict definition on what is high tech crime so we can say that it falls outside that; it’s somebody else’s responsibility (Police#18).

Despite its successes as a model, the JBFSIT should not be seen as the only team capable or responsible for addressing high tech crime:

And again my view of the high tech crime world is that the AHTCC doesn’t have a mandate on high tech crime. The broader AFP or anyone can deal with high tech crimes. And so many times I see it, people see any type of nexus to high tech crime and they’ll palm it: they’ll refer it to us straight away. And then we’ll pump it straight out the door (Police#19).

While secondment into police was proving successful in the JBFSIT, it was suggested that law enforcement should also second officers to work with anti-virus manufacturers and software designers to learn more about the technical aspects of malicious code, advise on the design of software and establish liaison with those industries (Police#17). Private investigators wanted police to come and see how industry functions:

What we’re doing very much now is that when we’re having these criticisms levelled at us, we’re inviting the police to come in and spend some time with us and see what we stop. Understand the size of our business and understand that we generate X billion dollars a year in profit and we do that because we’re doing a whole lot really well (PS#16).
However, police remain reticent due to potential headhunting as discussed in Chapter Six. Likewise concerns were raised about the bureaucratic hurdles for police to undertake short term visits to private sector organisations, such as attendance at the execution of a civil Mareva injunction to learn about private investigation or business processes (PS#17).

Most respondents favoured secondment of private investigators into Victoria Police. Some investigators did not because they did not generate sufficient referral of work, the complexities of their own conflict of interest checking and because they might have to pull out if clients withdrew permission (PS#14, 15). The benefits of seconding private investigators into police forces included access to and explanations of company records. Nevertheless, police respondents believed that previous secondments of corporate investigators to Victoria Police were merely goodwill exercises:

The access is limited. In fact, there’s an email we had come out that said “This person will not have access to this, this, this, this and this; and you’re not to ask them blah blah blah.” In other words, it’s purely a superficial arrangement... There isn’t really any exchange of information. It’s more just to say, “We like you, you can like us” (Police#1).

For secondments to be worthwhile, “you really need to make an assessment as to whether or not those agencies need to be seated in the Centre or whether we can use the resources that they can bring to bear when we need to” (Police#21). Secondments of less than three months to Victoria Police were not considered worthwhile:

A secondment for a month in here [the Computer Crime Squad] is absolutely pointless. A secondment for two months is almost just breaking even. A secondment for three months, it’s worthwhile. So, we won’t entertain a
secondment under three months for obvious reasons. Your first six weeks—
first four weeks—it’s just a pain. It’s a real drain. Next two weeks it’s not so
bad, you’re getting some return, but there’s still a lot of going backwards,
then the next four weeks, it’s ok, it’s only a review of what’s being done. After
that they’re pretty much, it’s just a question when there’s an issue. Box on,
and then let’s just see how you’re going and just do a weekly check. So it’s a
bit like RAM, there’s a point of diminishing return. But in reverse (Police#4).

We have temporary people, but to some extent when you get someone in and
their offer says temporary—it might be for three months— it sort of balances
up to almost a negative. Because yes, it’s great, you can have them here, they
can start to do some things, but they can’t do a lot. It actually takes from
someone else and you’ve got to go and train them and mentor them and assist
them. So it’s almost a drain some times (Police#3).

Other concerns were raised about secondments relating to issues of
confidentiality, worker’s compensation and because secondees would have to
become unsworn members of the police force. This was seen as problematic,
because people without the power to arrest simply might not meet the needs
of police in terms of resourcing (Police#14). Serving “two masters” might also
conflict with police needs, for instance if the private employer wanted reports
on particular investigations and it was not the right time for police to release
that information.

Another option might be lateral entry into the police force (Police#5). A lateral
entrant member could be distinguished from sworn generalist police as a
sworn specialist member. Those coming in laterally could have restrictions on
lateral movement within the police force once they’d joined, perhaps unless
they went back to complete the “beat” policing of new recruits. Previous
commissioners have opposed creating two tiers within public policing of
generalist police and “more highly skilled police member[s] who would perform more complex investigative functions” (Comrie, 1995 cited in Davids and Hancock, 1998: 52-3). Lateral entry as an unsworn member is more likely.

**Partnership through industry bodies**

Another option for police would be to “partner” with industry associations. Normally this would involve police formalising ties with existing organisations as in POLSEC. The E-Crime and Forensic Technology Association of Australia represented a different initiative, where Victoria Police members and the private sector attempted to develop an industry association from the ground up. The founding members of EFTA aimed to “develop and promote the EFTA as the premier organisation of professional computer forensic investigators in Australasia through professional cooperation and communication between public and private bodies” (EFTA, 2004a; see *Appendix R: EFTA Mission and objectives*).

EFTA proposed to accredit “EFTA Accredited Specialists” according to their area of investigative specialisation. An accreditation committee would be convened to research and establish this process. Accreditation, according to the rules of association, would be based upon “relevant work experience, education and training or industry certification” (EFTA, 2004b). As a method of raising industry standards, members would need to earn “points” towards their accreditation through “provision of work experience to non-related Associate Members or Members within the year preceding the application date for membership renewal” (EFTA, 2004b: 7a). To maintain accreditation, members would also need to complete twenty-five hours of training or education each year. It was agreed that industry would be consulted before attempting to impose this accreditation scheme.
I think the concept was to get a group of people who are actually doing a bunch, who are actually practising computer forensics or those sorts of associated things and make sure that when they do that they are accredited or that they are doing it to a certain standard. And at the same time to have a group where information and methods and knowledge can be shared. It’s a fantastic concept (Police#3).

EFTA would play an important role, as some police had raised concerns that other associations, such as the Australian Institute of Professional Investigators (AIPI) might not appropriately accredit members (Police#14).

I think this is a good thing, because there is no real association which sets down some ground rules or regulations. I think having police involved in part of that process may be a good thing, because hopefully they’ll bring commonsense to the fore and you’ll end up with some good internal regulations in relation to qualification achievement or in – what am I thinking? – I’m thinking like your Standing Orders, your methodology, your practices and procedures: that are endorsed. And that could be a good thing (Police#4).

Linked to accreditation was the key aim to “establish a standard of professional conduct incorporated in a code of ethics to uphold the trust given to our profession” (EFTA, 2004a).

There is no code of conduct, code of ethics, nothing. There is informally, as in, this is what Victoria Police do and the big companies do it, because they’re all ex-coppers from Computer Crime Squad. So that’s a code of ethics that’s probably adopted from Victoria Police and they’ve carried it on, because that’s who they are. People outside that, don’t have that. They have that in some respects, but it’s not something that they abide by. It’s something that they may use, but “Oh well, if I overstep that that’s nothing to do with me,
it’s not governed, so it doesn’t matter.” So what we want to do is have a group membership. If you want to be a member of this association and you want to be a part of it, you want the recognition and you want all this gratitude, I suppose then this is what you must do. It’s not punishable by anything other than, you can’t bring our organisation or association into disgrace because you went outside those boundaries, because we’ll just kick you out. And if you refer to us, when it comes back to it “He was referred” say, “No, this was why he was excluded from the organisation” (Police#5).

Over and above rescinding memberships as the most severe sanction (Sarre, 1998: 101), EFTA proposed fines up to AUS$500 for members who breached the association’s rules or Code of Conduct and to publish a register of disciplined members (EFTA, 2004b: s10).

The benefit of EFTA to business was expected to be long term strengthening of individual businesses and the industry through a supportive infrastructure and profile raising, similar to ideals of the open source software industry that benefits communities above a single provider (PS#17). EFTA members hoped to promote forensic computing as a process rather than a knowledge of software tools (PS#17). EFTA was to have a practical investigative output:

It’s going to be about getting guys out on jobs with us you know and in some ways it’s not going to be a lot of benefit to us, but you know it will be in the long run, because to have more people doing it is going to open the marketplace. But traditionally what you’ll find in my experience…is that people look at this environment (it has happened to me before in a couple of situations, where I go, “Wow there’s a big market here let’s go, let’s be really greedy”) and what actually happens by doing that they actually strangle it to death and nothing happens… Whereas if you can be like this and you can have heaps of people out there doing work that means that it is only going to promote [the industry] with people and there’s going to be more and more
work. So it’s going to be like being an electrician at the moment: it doesn’t matter whether you’re useless, there’s that much work out there you’ve just got to hang yourself up a shingle and you know get your A grade licence and you’ll get work (PS#17).

EFTA was seen as an opportunity to cross the police-private sector boundaries. For police, EFTA would be characteristic of a forum in the community policing tradition. “Everyone is representing their own entity officially, because it’s managed officially by those boundaries and yet unofficially we’re going to sit there and have a chat” (Police#5).

Recognition of their professionalism was a key motivator for police interested in EFTA, similar to their motives for undertaking tertiary qualifications:

I go to court, I’m President of EFTA [for example]: “Oh, ok”. And in the industry, “Wow”. You being Joe Blow: “What does that mean?”, but industry is like “Wow!” And that’s what you want: “Ok, he does have ethics, he does have a Code of Practice. He does take his position seriously, because he’s a member and only this core group of people can be a member of that organisation” (Police#5).

From observing the committee meetings and speaking informally with members it become clear that a reason underlying the formation of EFTA was recognition that police will choose with whom they will partner and as individual, private operators these investigators might not get a “look in” otherwise. For police who were unhappy with their current positions, EFTA was seen as an opportunity to move on from police work:

I’d love to … suddenly go, kabomb, like my head’s spinning because suddenly I have to go now part-time with Victoria Police because EFTA is doing this thing and I have to devote time and [am] getting paid to do it and
whatever, because this is what I have to do to maintain it and it’s now a new job of mine that’s part-time. I’d love to do that (Police#5)!

However, it soon became apparent that EFTA was not developing as envisaged:

It doesn't really seem cohesive as something at the moment. It's very difficult to get people interested or involved in it. I know, I tried there at one of our meetings to get people involved and got no response at all. Quite depressing (Police#3).

The EFTA committee met for the first five months of 2005 and arranged social drinks twice for interested people. However, the committee had difficulties collecting membership dues from prospective members. At the fifth monthly meeting in May 2005, the committee members discussed a federal initiative that had been announced that would develop IT Security Skill Accreditation for the forensic computing industry and duplicate the key aim EFTA was trying to achieve (LeMay, 14 March 2005). EFTA had missed the deadline to tender for the contract to conduct the research into such a scheme. The discussion that night signalled a clear end to EFTA’s efforts and that was the last committee meeting held. In September 2005, the media reported that industry “did not identify a compelling need” for certification (LeMay, 27 September 2005).

In May 2005, EFTA exhibited more characteristics of “failed partnerships” than successful ones (Wilcox, 2000; see Figure 3.2). It had leapt from the second phase of partnership—frustration—directly to failure. One of the clearest reasons that EFTA did not succeed is that there are already many professional and industry bodies such as the Australian Computer Society and the Australian Institute of Professional Investigators that cater to a broad
range of industry professionals. Most investigators, as mentioned above, are already members of established associations. The private sector believed there was need to centralise the “hotchpotch” of various professional associations, corporate bodies, committees and sub-committees (PS#1). Some committee members hesitated to affiliate with larger organisations in case EFTA’s aims and objectives were quashed by the goals of an affiliate. It even invoked secrecy about its aims. As a small organisation EFTA would add to the number of organisations instead of reduce it. Others were disappointed by this and hoped the group would welcome association with larger industry bodies as a means of growth:

If you had a bigger association who’s doing exactly the same thing, as we’ve found out, open-minded people go, “Hey, they, this other association may have thousands of members, we have six or ten or twelve. They want to do what we want to do, why reinvent the wheel if they have all this power?” and they’re suddenly going to go bang and snowball the whole thing. We’ll jump on top and ride the wave with them… It’s hard to know, because you don’t know what’s going to happen, but we might be a chapter off that, that we’re affiliated and we use their affiliation, but we still have a little group here, but still run with these guys. But with the IT industry and the forensic industry, because they’re so dissimilar in that respect that might be a “Ah EFTA that’s, you’ll be under our umbrella, but you have those guys and these guys have industry standards for them and we’ll try to cross-pollinate because these guys want to move to forensics”. And work in both fields. And that’s the way you use it to your advantage. Hopefully it works out something like that (Police#5).

---

117 It was only at the penultimate committee meeting in May 2005 that the “in-confidence” status was removed from the association’s Mission statement (EFTA minutes, 12 May 2005).
At the time of writing, no such “cross-pollination” had occurred, although the Internet Security Interest Group (ISIG) had offered affiliation (personal communication).118 EFTA “is very bogged down. Yeah, I think it needs to be an open environment, rather than, I think it could tend to become a club sort of thing” (Police#3).

Some private investigators thought police should not partner with industry bodies, because it would create a conflict of interest in terms of investigating members where industry bodies work to protect the interests of their members first and foremost (PS#1, PS#2):

[Police] shouldn’t associate with professional bodies except to give them advice, but certainly not to have them participate in any policy formulating type committees. Where professional associations and bodies are concerned I sometimes like to pull the military trick of a pre-emptive strike at times, because that’s the only way that you get them out of the way, before the person has an understanding of what is happening to him. And bearing in mind that these are pretty difficult ones where you get in with the person and the very first thing you’re doing to the person is saying, “Good afternoon” and giving them a formal caution. Because that’s how you want the matter treated (PS#1).

Although not an industry body per se, in terms of e-crime AusCERT has been perceived as the most successful at liaising between its members and law enforcement.

I think they sit really well because they’re at the University of Queensland, they’re not government and they’re not private, so they have no, I’m not saying they don’t have any motives, but they sit well in the middle ground.

---

118 ISIG changed its name in 2006 to the Australian Information Security Association (ASIA) to reflect the professional standing of the organisation.
And a lot of people can trust them, because if you’re a private sector company you want to subscribe and you’ll think “Well, they’re not for profit, so they’re not trying to screw me over for money, for example, yet they’re not the government so I can trust them” (Police#19).

However, collectives avoid the difficulties associated with partnering with a single organisation, such as claims of endorsement of products or services or special relationships (Police#13). Even so, interest in participating with some of these groups lessened if there was a lack of control by police. The Australian Bankers Association was a case in point, where police described having limited contact because they couldn’t control the direction of it, describing police participation in that forum as “really almost watching” (Police#14). Even more established industry organisations like the AIPI were unlikely to achieve partnership with Victoria Police according to senior police due to the small size of the industry: “It’s a market they would love to develop. And I can understand that. Do I think it’s going to happen quickly? No, because they haven’t got enough grunt. Chief Commissioner’s not going to listen to 80 people” (Police#14).

Private investigators also had their own reasons for joining industry bodies related to practical benefits to their work:

The real reason we would be members of IAFCI is simply because it gives us access to people across the world. We get a membership directory and we know if I’ve got another bank, say, one of those Nigerian scams… And we were then able to use the IAFCI register to contact someone at [an overseas bank] and say “We’re aware of this, one of our customers is thinking about sending money: what’s the story” (PS#11)?

Forums such as conferences, round-tables and regular meetings were the main mechanisms used for information sharing. Face-to-face forums were
preferred over email communications. Some respondents complained that there are already too many discussion forums, which need better structure (PS#11). In general, the main benefit of industry forums to investigators was sharing ideas about operational investigative methodologies (PS#16):

Someone will come up and say, “We’re also checking the browser string to see if our customer’s browser string is the same as the browser string on the IP address that’s accessing it”. They might use Internet Explorer and the crooks are using Mozilla. We’ll go away and look and that and say, “Well, can we add that into our reports or whatever” (PS#11).

Police utilise such forums to advise industry of current and emerging trends. Industry forums have their limitations: “Well, you can’t really communicate about individual incidents. You can talk about fraud trends, but you can’t get into specific incidents” (PS#11). A major problem related to forums run by industry associations is the cost of membership. As an example, the major Australian banks withdrew their membership of IAFCI due to perceived low return for the membership fees (PS#16). They subsequently introduced another informal forum for bank investigators only and without memberships. “We probably had to have ten members in IAFCI. And at US$200 a pop it started to get really expensive. If I had ten members in this, cost me nothing, cost me a plate of sandwiches when we have the meeting. So it works well” (PS#16).

**Commercial investigative partnerships**

When members of Victoria Police and an investigation firm met in early 2005 to discuss “partnership”, the investigation firm was straightforward in stating that it was looking for a commercial advantage from an association with Victoria Police. Having passed the first hurdle as to whether it undertook
criminal defence work the firm was asked about headhunting of police members to work at the firm as a second hurdle. It was put to the company representatives that Victoria Police would seek assurances that they would not entice members of the Computer Crime Squad away to work in the private sector, should a working relationship follow. The representatives assured those present that was not their intention as they were a small firm.

At the meetings, neither party expressed clear goals or a project for a potential partnership. Recall that lack of a clear goal for a partnership is one of the key indicators it will not eventuate or will fail (see Table 3.2).119 Nor were these discussions coordinated by the partnership structure developed earlier by POLSEC; no mention of POLSEC was made. One officer described the problem police often have with negotiating partnership: “It’s never what can they give us. We know what they can give us. The hardest point is what can we give them” (Police#1).

Some interviewees held optimistic beliefs as to what work the private sector could undertake for police in relation to e-crime investigation: “it can be any work at all for the police as long as the person doing the work has suitable qualifications [and] experience commensurate to the job” (PS#18). For example, might private operators conduct the initial collection and preservation of digital evidence known as forensic imaging? Respondents to this study suggested there might be a place for outsourcing this: “if they reduced their fees to a reasonable rate, it probably would happen, you know” (Police#5).

119 However, this is common for the introductory, exploratory stages of a partnership and may only have represented the early stages of negotiation (EDuce Ltd and GFA Consulting, nd).
If we have an organisation outside our organisation who is seen as independent who can come in and do the imaging and all that sort of thing, then yeah by all means. Because in the end of the day, Computer crime blokes are trained investigators, like I am, and what do they do? They image computers. They don’t investigate. They send jobs down to us saying investigate this and you say, “Well you’re the experts. You please investigate it.” And they go, “Well, we can’t, because we’re imaging disks or imaging hard drives.” So, if there is something out there who is able to provide that assistance who passes through the governance checks and is willing to work in partnership with the police, then yeah, there’s a place for them (Police#6).

Others did not support outsourcing of imaging:

I don’t agree with outsourcing that type of police work. So many times I’ve seen fraud investigations outsourced, because no one can do it and it comes back and the rules of evidence haven’t been applied and then the whole thing falls out. And all you end up doing then is cleaning up the case. [Forensic computing] is the same, unless they can meet a particular standard I don’t think it should occur (Police#21).

Some years ago, private investigators and Victoria Police explored the idea of police providing paid opinions about the merit of a criminal case:

There was some talk about MFID working with private industry in a moneymaking exercise, which was: corporations and private enterprises would submit complaints for opinion. So they would say “We’ve got an employee, we think he’s taken this, here’s the data we’ve got. Can you have a look at it, give us an opinion” and they would pay us… It didn’t fly, because if the opinion was incorrect we were liable (Police#1).

Police were clear that Victorian law prevented private investigators from assisting with computerised child pornography cases (Police#5).
An alternate public-private partnership project might harness the unused computing power of IT hardware owned by private organisations or individuals in the community to decrypt suspects’ encrypted files. This might be either a commercial arrangement with a private organisation or non-commercial with the community like the Search for Extra-Terrestrial Intelligence (SETI) project.

If you’re only passing the key, there’s no problems. And a lot of it depends on the file type. There’s some you can and some you can’t, because you’ve got to pass the whole file to do it. If you’ve got to pass the whole file and you believe it contains something like child porn, well then suddenly, you’re distributing child pornography. Can’t do it (Police#4).

**Referral of investigations**

“Referral of investigations when police resources are insufficient” (PS#14) was an advantage private investigators expected from working collaboratively with police. Others in the study also requested that police “assist with information on other alternatives if the specific situation does not appear to apply to them” (PS#13). Referral might involve either transfer of incidents considered civil, outsourcing of an investigative activity, such as initial assessment, collection and preservation of digital evidence discussed above or referral of an entire criminal investigation which would then be referred back to police after investigation accompanied by an evidence package. Respondent investigators described instances where police already referred criminal cases back to their companies, once matters had been reported officially (PS#14; PS#15).

---

120 The US Secret Service already harnesses over four thousand computers within its agency to run its “Distributed Networking Attack” program to decrypt data for investigation purposes (Krebs, 28 March 2005).
When they met with Victoria Police to discuss a possible commercial partnership for investigating e-crime, the representatives of the forensic investigation firm asked about the possibility of referring appropriate cases or complainants that Victoria Police had decided for some reason not to investigate. Although “referral networks” were supported in the Victoria Police Way Ahead strategy this suggestion was declined immediately. It was argued by police that referral to private providers was problematic as a matter of equity. A list of all private sector investigation service providers would need to be provided to a complainant and no such list of the whole industry existed. It was further suggested that even the mere ordering of a list of providers could prove contentious. Recall also that Victoria Police had suffered the “Windows 95” scandal involving kickbacks for referrals, discussed in Chapter Three. Victoria Police does not even refer suspects when they request legal representation. They offer the telephone directory, whereupon the suspect can make their own selection.

**The proposed VFIRC**

Interviewees were asked to respond to the proposal of the Victorian Parliamentary committee inquiry into Fraud and E-Commerce for a VFIRC (see Chapter Two). The response from the private sector was to say the least, mixed:

> Well, I’m not going to report one offence 28 times. That’s just stupid. Already we report to High Tech Crime and AusCERT. If it’s card fraud, we report it also to [the credit card company], as part of our fraud statistics. We report stuff to the Australian Payments Clearing Association... For someone to say “All financial crime in Victoria you must report to me”, well, no sorry, I report it all over the place. If I think—and we make selections, we make decisions about what we’re going to report and what we’re not going to
report—we might have one cheque fraud or one internet banking fraud where it’s a one-off, totally unrelated to anything else; it’s a thousand bucks. We’re not going to spend money trying to investigate it. We’ll keep records on file and see if a pattern comes up, but why would we want to report that to an already overloaded system? You’ve got to be rational about the whole thing (PS#11).

A related concern was that if a business is registered in Victoria, but undertakes its business also in other states and an incident occurs in another state, would they be required to report it in Victoria as well as the state in which it was to be investigated (PS#11)? The proposal was also opposed on the grounds it would diminish relationships between police and private investigators: “Based on our experience, that’s just another level of ‘in-between’ the direct contact. And I think the direct contact has proved to be just so valuable” (PS#2). It would also add delays by adding an additional level of initial assessment (PS#1). Others preferred a national reporting centre to “marry up” the disparate Australian states (PS#13).

Those who supported the proposal saw the usefulness of a mechanism that directed reported e-crime incidents to the appropriate agency (PS#18). The proposed VFIRC could mirror the public-private partnership of the JBFSIT and provide effective coordination of reported incidents (PS#16). It was best that such a centre not be hosted in the private sector, as commercial rivalry already prevents investigators referring publicly to surveys written by competing firms (PS#16). Others preferred an avenue for hands-on participation of the private sector: “We would see the private sector being more involved in assisting the police in the investigation of this kind of thing” (PS#4). Despite supporting the necessity of mandatory reporting, fierce opposition was predicted from the banking industry as the VFIRC would
initially harm reputations: “why has the crime rate spiked 200%, what have banks been hiding” (PS#16)? IT administrators preferred a system that mirrored reporting to AusCERT:

AusCERT provided that level of trust, where it could go beyond security and be able to openly discuss issues that were affecting me… I felt like I wasn’t threatened that this could blow out into reputation issues. And I could maintain the control I needed in my own space without feeling that if I reported something that there would be a loss of control. And I suppose that’s part of the reason why the police were not included in a lot of this, because I thought the information wouldn’t be as easily coming. I wouldn’t be able to share as openly and honestly. The possibility of losing control as well, if there was a crime that needed to be identified or traced or what have you and then [police were] interrupting the working space or business processes (PS#12).

This IT administrator felt that cooperation with police was complicated beyond worthwhile benefits, due to his perceptions about overlapping, conflicting state and federal police systems:

Cooperation has to be demonstrated and I suppose what was appealing about AusCERT was that there was, it was homogenised in its mission and there were no overlapping agendas there. Whereas with the police, I certainly feel like there is an overlap… If there are politics that come into the technical environment, then it gets awfully confusing and trust is difficult to place in that (PS#12).

Law enforcement respondents viewed the proposal favourably, especially if it would provide centralised cross-referencing of offender modi operandi and other intelligence (Police#15):
I think it’s important, definitely important, especially with e-crime being extraterritorial, international. You could be chasing one bloke on [an auction site] for 400 bucks, but there’s another copper in NSW or another copper in Victoria whose been chasing him for $10 000 of [auction site] frauds and you don’t know anything about it. If it’s all collated in one spot then you can say “Ah, Joe Bloggs from [auction site] has done 15 different frauds” or 20 000 frauds and then it gets sent to the Fraud squad. So that file gets sent to the fraud squad, or sent to local CIU if it’s only a small amount (Police#2).

Police supported a VFIRC that would create a true intelligence capability in support of proactive investigations: “that intelligence capability would allow us to move off in the right direction and to determine what the right direction is” (Police#7).

**Private donations or sponsorship of public policing**

In the AHTCC’s Joint Banking and Finance Sector Investigation Team, the major Australian banks sponsor the investigation of “phishing” offences by seconding their investigators there while paying their wages:

I think we should be able to do that. And in fact we have been able to do that. We’ve done it. And not only in terms of assets with the banks, but in terms of [financial] contributions. And the way we get around that—not the way we get around it—the way we justify and do it ethically is we undertake a contract and we articulate certain things and the contract is pretty detailed. No expectations that there’ll be preferential treatment or that sort of stuff, no conditions on how the money’s spent. Other than to know where it was spent, for what purpose. That’s it. And then it’s put into a trust account and once it’s expended and it’s spent, then we report through the board. And articulate. And ordinarily, what we try and use it for is things like capacity building, equipment, you know the really benign stuff that. So we don’t sort of say for example, industry X who is an ISP provided $20,000 and we paid
for the salary of the investigator who was investigating an offence that was committed against the company X. That wouldn’t be very wise. So we usually spend that kind of money on… our training budget and things of that nature (Police#21).

However, Victoria Police policy prohibits as unacceptable donations or sponsorship where Victoria Police directly or indirectly regulates the donor or sponsor’s industry, specifically including the security industry (Victoria Police, 2005a: 205-5: s4.1) or if there is a potential or perceived conflict of interest. Generous overtures of financial support have been made in the past knowing that Victoria Police would not be able to accept those contributions:

They can be very willing to give us lots of resources, when they know that we won’t take some of them, being the donations and sponsorship stuff. We can’t go to them and say, “Give us $100,000 and we’ll go and hire an extra detective”, because if we did that it comes out in public domain saying, “This is ridiculous – you’re working for the banks and you’re not working for the individual” (Police#14).

Another police officer argued that if sponsorship of investigations were permitted in Victoria it would need to apply to both prosecution and defence efforts:

Or if it is available, or if you are allowed to do it, then it’s not ad hoc, it’s across the board. If the defence start to say well, “We want you to go and do

---

121 For example, the existence of other regulatory or contractual relationships between the prospective donor and the recipient may render sponsorship suspect (Grabosky, 2001: 10). Funding has thus far not been an issue for POLSEC as support has been arranged without funding or separate government funding (POLSEC, Victoria Police, 7 Mar 2006, personal communication).
this and we’re willing to pay for you to do the ISP traces” then off you go.
Can’t be just one way. Can’t be victim related without being defence related
(Police#6).

Chapter conclusions

Despite police powers to obtain information coercively via search warrants,
partnership style relationships with the private sector are considered essential
in Victoria for investigating e-crime. Good relationships grease the wheels of
efficient justice. However, Victoria Police has yet to decide whether formal
investigative partnerships with private investigators are appropriate. It is
impossible to separate issues of investigative efficiency from questions of
probity and it seems Victoria Police is waiting to see how partnership policing
turns out in other forms, like educational partnerships, before committing
itself to investigative partnerships.

In particular, this chapter highlights the very different philosophies driving
attempts at investigative partnership. Underlying partnership policing is
police desire for change in the behaviour of the private sector: secure your
companies, report incidents affecting you, facilitate law enforcement
investigations in a timely manner. Demands for change were two-way: the
private sector wanted faster results, better feedback and commercial
opportunities. To most working in partnership meant sharing information;
although how bi-directional that sharing would be is debatable. Reflecting
Sarre’s (1997: 76) observations that police are loath to share “their” work,
many police and private investigators respectively spoke of partnership as
others facilitating their own investigations; assisting a partner was only a
secondary, less important concern. It might be the very expectations of what it
means to work in partnership that might preclude their widespread use in
state policing. For police, it included sharing costs and responsibility; for the
private sector, in-sourcing, outsourcing and referral of investigations. Considerations of legalities, lack of trust and need for investigation secrecy (LeBeuf, 2001: ¶29) also affect the desire and ability of police to share information with private sector investigators. These discussions about partnership reveal further the dynamics of potential partnership interactions: police generally hold the upper hand. They pick and veto their potential investigative partners. Potential partners are unlikely to include those who conduct or assist any criminal defence work or who headhunt police members. In efforts that take off like the JBFSIT, or even progress marginally in the case of EFTA, the private sector wields the power to withdraw cooperation. Arguably, neither sector has yet mastered an economy of scale in terms of investigative partnership at state policing level due to the decentralised operations of both public policing and private sector industries.

Investigative partnership is further complicated by the victim or third party status of potential partners. Victims expect police to provide service; witnesses expect recompense for assistance. “There’s always going to be that dispute as to why should we pay for that? We need it or it’s their job” (Police#13). Depending upon whether the private sector is a victim or whether they are asked for assistance by law enforcement can turn the tables on this issue and so it is recognised as a powerful bargaining chip by repeat victims like banks.

Sarre and Prenzler (2000: 106) advise maintaining a “respectable distance” between the two sectors. Most private investigators were clear they did not want to be police; likewise most police held themselves above private investigators. Support for formal regulation of investigative partnerships was divided amongst respondents. Most concerns were that formalised, regulated partnership would hinder cooperation and information exchange rather than
encourage it; a suggestion supported by the experiences of the Royal Canadian Mounted Police (LeBeuf, 2001). While almost two thirds of survey respondents supported granting private investigators additional investigatory powers to assist e-crime investigation, almost all interviewees demurred.

Inconsistency in the current regulation of private investigators poses problems in terms of accountability mechanisms and a level playing field. E-crime investigators in Victoria may or may not require licensing by Victoria Police depending upon their employment situation even though they may undertake effectively the same or very similar inquiry work and thus some escape these oversight mechanisms (see section 4(h) Private Security Act 2004 Vic). Regulation of the industry by police might also negate opportunities for funding of partnership activities by private investigation firms. This provides additional support for Sarre and Prenzler’s (2000: 106) argument that a third party should license private security.

The EFTA and POLSEC initiatives provide important lessons for partnership attempts. Both highlight the fragmentation of the private security industry and partnership efforts and the ease with which initiatives that do not include all stakeholders can be overtaken by other agendas or higher authorities. Likewise, POLSEC teaches that broad frameworks can be implemented narrowly and miss opportunities. Truly cooperative initiatives may be overcome by regulatory ones as demonstrated here.

The strength of the secondment model of the JBFSIT is in the collaboration of partners that would otherwise be in competition and in the central coordination of efforts aimed at the specific task of policing phishing. Despite the borderless nature of e-crime, policing efforts are enhanced by the physical location of police and private investigators together. Investigative partnership efforts within Victoria to tackle e-crime must complement the efforts of the
AHTCC and the JBFSIT and not duplicate effort unnecessarily. The “one-stop-shop” characteristics of the AHTCC make it an attractive partner to the private sector and state police forces will need to capitalise on that. As it is the aim of the AHTCC to push down e-crime as it evolves to state forces, state police forces should prepare for that eventual push down of incidents. That might involve creating environments conducive to private investigator secondment to joint investigation teams.

This study indicates that there is no one-size-fits-all solution in relation to e-crime investigation and police will have to pursue investigative partnership at different levels according to the risks and benefits involved. POLSEC exhibits some qualities of a generalist framework for police-private security partnership. POLSEC’s information sharing protocols and secure system represent resources other police should be able to access and if need be customise to avoid reinventing the wheel. However, POLSEC seems to have failed to attract the attention of others within Victoria Police as a generalist framework for constructing partnerships. Currently, there is no provision for squads like CCS to be part of POLSEC initiatives.

The next chapter synthesises what we now know about the investigation of e-crime in Victoria and responses to the partnership policing strategy to model a set of normative guidelines for state police forces that decide to proceed with e-crime investigative partnerships.
Discussion and conclusions

Chapter 8: Instituting public-private investigative partnership policing of e-crime

The previous three chapters report the results of research undertaken to examine the contexts under which partnerships between public and private police for investigating e-crime could be beneficial to both parties, while adhering to public interests. To achieve this it was necessary to learn more about the emergent phenomena of e-crime policing and the significance of investigative partnership to this. The anonymous, online pilot survey was less successful than expected, generating few responses. E-crime victims, perhaps naturally, preferred to telephone or meet in person to discuss their experiences. Interviews with police and private investigators provided the richest data for this research, detailing a myriad of routine factors that influence the successful investigation of e-crime. Analysis of police incident records provided insights into the nature of e-crime reported to police in Victoria, Australia and the organisational responses of police to these types of crime. Caution must attend interpretation of the incident analyses, because only cleared cases could be inspected, the quality of LEAP records was inconsistent and, as reports of their own performance, police might have downplayed the private sector role. Future research should examine both solved and unsolved incidents and should analyse briefs of evidence that contain more consistent detail. The research was flexible in its approach and took advantage of opportunities to observe, albeit briefly, three case studies of investigative partnership that developed midway through the research.

In light of the conclusions drawn in previous chapters, this chapter proceeds first to evaluate Sarre and Prenzler’s (2000) *Regulated Intersections* model on the basis of how well its policies fit the existing regulatory character
surrounding police and private investigator relationships in Victoria. Next, based on this analysis and the formal standards for public and private policing outlined in Chapter Three, reforms to local mechanisms that impact upon policing of e-crime in Victoria are suggested. Regardless of whether the decision to pursue formal investigative partnerships has been made, these proposals should be considered in light of the ad hoc partnerships described in this study. Following this, the lessons from this research are operationalised as practical guidelines for police officers and policymakers and discussed as applied to seven forms of investigative partnership. Final conclusions are drawn at the end of the chapter.

**Evaluating the *Regulated Intersections* model**

Does the *Regulated Intersections* model proposed by Sarre and Prenzler (2000) fit the existing regulatory character attending interactions between police and private investigators in Victoria? Figure 8.1 summarises the regulatory character as evidenced in the research data. Comparison of Figure 8.1 with Figure 3.4 (see pg.68) reveals that in most respects *Regulated Intersections* reflects the current regulatory character for police and private investigator interaction. However, a discrepancy and tension exists in relation to the concept of a “level playing field” as that relates to investigators following the same standards and thus competing equally for public police resources. Both private investigators and police desired institutionalisation of professionalism in the security industry on the grounds of excluding “mavericks”: from the industry entirely or from legitimate interaction with police. Simultaneously, investigators currently exempt from licensing argued against the “level playing field” of a licensing framework.
Figure 8.1: Regulatory character surrounding police and private investigator interaction in Victoria

<table>
<thead>
<tr>
<th>Social norms</th>
<th>Social norms</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collectives (objective)</td>
<td>Collectives (objective)</td>
</tr>
<tr>
<td>Social ordering (Perspective)</td>
<td>Social ordering (Perspective)</td>
</tr>
<tr>
<td><strong>Type of authority</strong></td>
<td><strong>Type of authority</strong></td>
</tr>
<tr>
<td>Social norms</td>
<td>Social norms</td>
</tr>
<tr>
<td>Social norms</td>
<td>Social norms</td>
</tr>
<tr>
<td>Ideology of “responsible communities” and “professional police” working in partnership. Trust is foregrounded. Separate roles of police and private investigators emphasised. Police occupy senior, leadership position.</td>
<td>Law acts as a mechanism to protect public interests, promote professionalism and exclude “mavericks”. Partial licensing of investigators reflects predominance of market interests over public interests.</td>
</tr>
<tr>
<td>Individuals mouth rhetoric of “partnership”, but action covers spectrum of responses according to Stenning’s (1989) stages of interaction. Calls to partnership focus on own routine activities, and “police policing” (see pg. 283). Potential for overt conflict as individuals attempt to impose or avoid responsibilities.</td>
<td>Conflicting use of either personal relationships or bureaucracy and legalism. Laws interpreted legalistically by individual police to smooth over constraints on public policing provisions and by corporations to claim access to services. Personal relationships or victim status used by private investigators to access policing.</td>
</tr>
</tbody>
</table>

As seen in Chapter Seven, the respondents opposed regulation that “limited” cooperation as foregrounding suspicion and distrust instead of trust (see Cherney, 1997). This highlights that the weakness of Regulated Intersections as a normative model is that it lacks ambition to exploit fully the benefits that could accrue from ongoing, mutually beneficial relationships that prioritise and preserve public interests. A combined forces model, also regulated closely to maintain an appropriate balance between public and private provision of policing, but not limiting the potential for virtuous cooperation should be the final goal of a society that values security for all. The Regulated Intersections model thus represents a “middle-range” normative theory—to
adapt Merton’s (1967) term—that, if the element of limiting cooperation is removed, provides the means to work incrementally towards an acceptable combined forces model through “do and review” and “radically new” style partnership policing (see Table 3.1, pg. 69).

**Reforms to promote successful policing of e-crime in Victoria**

**An hierarchical taxonomy of e-crime terminology**

Chapter Two traced the development of terminology used to describe crimes facilitated by or committed against computers and other digital technologies. However, terminology has not been used consistently within academia or law enforcement and is particularly broad and open-ended. Often terms are described as “interchangeable”. Consequently, this thesis asked whether the ambiguous definition of “electronic crime” assists or hinders public and private policing of these types of incidents.

Interviews with police and private investigators indicated the definition or lack of using definitions has led to some miscommunication between police and private investigators, relating mostly to what is considered “e-crime” or not (see pg. 180). Investigators also expressed concern that the terminology does not distinguish investigative specialisations. The definition of e-crime did not establish boundaries for police, which could impact on appropriate targeting of police resources and referral and acceptance criteria, such as whether a specialist squad should investigate an incident. The literature also noted the difficulty of quantifying crime where method is needed to identify incidents (Krone, 2005a: 2).

Accordingly, a formal statement of the taxonomic jargon in an hierarchical structure is offered to promote more consistent use. This is represented as a
Venn diagram to illustrate the relationships between the terms and the phenomena they represent. As shown in Figure 8.2, e-crime is made up of overlapping subsets of offences according to characteristics of the technology involved or its complexity. Computer crime is a subset of e-crime, because e-crime may involve digital technologies other than computers, such as mobile phones or digital video cameras. As discussed by the respondents to this study, what constitutes “high tech crime” is expected to change and what was once considered “high tech” will be pushed out and down. Thus as another subset of e-crime referring to sophisticated e-crime, the term “high tech crime” is flexible to such changes and permits separation of mundane from complex incidents.

Recall from Chapter Two that Smith and Grabosky writing with Gregor Urbas (2004) have preferred to use the term “cyber crime”. They argued that a distinction could be made between “cybercrime”, as a singular concept referring to “new” offences perpetrated in new ways, and “cyber crime”, denoting a range of traditional offences committed using new technologies (Smith, Grabosky and Urbas, 2004: 6). This development is disappointing as such a typographical distinction in terminology seems trifling and is more likely to confuse than enlighten. In reference to their example, what is the difference between cyberstalking and cyber stalking (McKenzie, 2005: 30)? “Cybercrime” has been used more usefully to refer to e-crime that also involves cyberspace; that is the Internet or another computer network (Wall, 1997, 1998, 1999; Thomas and Loader B.D., 2000; Etter, 2002; and especially Wall, 2005: 311). As Smith, Grabosky and Urbas (2004: 6) note, there is a need to distinguish between offences that involve “cyberspace” and those that do not. However appropriating “cyber crime” as a generic term removes useful

---

122 One reason given for the change was connotations of sexual offences in ‘digital’ (Urbas, Feb 2005, personal communication).
jargon that had been used previously to distinguish a subcategory of computer crime. Kowalski (2002: 18) noted that the core problem for law enforcement in Canada was a lack of distinction between Internet and other computer-related incidents. The involvement of networked information technology poses particular technical difficulties and requires different skill sets for law enforcement over and above some other forms of e-crime and so the distinction is useful.

Smith, Grabosky and Urbas include in their definition of cyber crime proscribed conduct involving digital technologies that “is incidental to the commission of other crimes” (Smith, Grabosky and Urbas, 2004: 7, italics in original). They state this includes the use of encryption or steganography to conceal evidence from law enforcement. As these have been proscribed under a separate offence for failing to assist law enforcement to access such protected data (see section 3LA, Cybercrime Act 2001, Cth) there is no need to complicate the definition through reference to “incidental” offences in this manner. These offences involve using information technology as a tool.

---

123 Cybercrime can also be subcategorised usefully by wider recognition of “virtual crime”, that is offences taking place in virtual realities (McKenzie, 1996; 2000), because of the explosive uptake of Massively Multiplayer Online Role Playing Games (MMORPGs). The South Korean cybercrime unit was created reportedly after a deluge of complaints from MMORPG players about the most common offence of “hacking into others’ accounts to steal weapons, stealing users’ online identification and fraud connected to the sale of virtual arms” (Levander, 4 June 2001). South Korean police report that of 40,000 incidents reported to them in the second half of 2003 over half involved online gaming (Ward, M. 29 Sept 2003). The law recognises that there can be value in intangible property. The most common examples of intangible property that can be stolen are bank account balances and intellectual property. Western societies are simply yet to reconcile these technological and social developments.
A difficulty arises when the definition requires that assaults are included as e-crime. US Department of Justice statistics for “computer crime” in 2000 included 878 cases of assault where a computer was used as the “tool” (cited in Kowalski, 2002: 12). However, this is not using the equipment as an instrument of information or communication, which is an implicit characteristic of e-crime. While it is not necessary that an ICT be used exactly as intended or designed—much e-crime subverts the intended (legal) use—to include use as a physical weapon misrepresents the phenomena. This requires a refinement of the definition of e-crime to reflect more accurately its intended usage as when a digital technology is:
- Used as an *information or communication technology tool* in the commission of an offence; or
- The *target* of an offence; and or
- The *storage medium* for illicit data or information.

A further difficulty with the definition of e-crime is an almost instinctive desire to exclude simple offences from “real” e-crime, such as theft of computers or computer components, as expressed by some respondents in Chapter Six. The literature hardly ever addresses these. Grabosky and Smith’s (1998, 2003) taxonomy does not.124 Smith, Grabosky and Urbas (2004: 9) exclude incidents that “have no other connection with digital technologies in terms of how the offence was perpetrated or the ultimate effect of the illegality”. However, theft of a computer can be, in the simplest sense, “denial of service” when it prevents the computer from working at its intended use. It constitutes the lowest end of an e-crime scale of complexity. Police respondents in this study noted that digital evidence analysis was often required to solve incidents of theft of computers or computer components, to identify the victim and return stolen goods. Therefore, information on these incidents is important to police and should be considered regularly.

Figure 8.2 illustrates that all cybercrime is computer-related and also telecommunications-related. All virtual crime is computer-related, but need not be telecommunications-related. Further subsets (see Wall, 1999) and individual terms that describe particular offence types, such as phishing, can be accommodated further within the subsets of Figure 8.2. Pharming would be classed as a high tech cybercrime. A further universe could be drawn to include non-criminal incidents of computer misuse. The positive impact of

---

124 Theft of hardware and software receives minor attention in Grabosky, Smith and Dempsey (2001: 62-3).
this hierarchy for law enforcement is that it facilitates flexible, directed response through common language. However, it does not by itself assist knowledge production about e-crime.

Krone (2005a: 1) proposes that the distinction of whether an ICT is the tool or the target of an offence provides a “consistent framework” for analysing high tech crime. This distinction might be used to analyse any e-crime, not only the complex ones. As seen in Chapter Five (pg. 143), a practical application of Etter’s (2000) definition of e-crime to incidents sampled for this study, as to whether digital technologies were used as tools, targets or storage media, demonstrated that categorisation on these characteristics is feasible.

However, what is the benefit to police, academics or the community of recording this distinction in modi operandi? First, to do so distinguishes e-crime incidents from others that do not involve information technology, thus identifying incidents of interest. Correctly, the Uniform Crime Reporting program in the United States notes that to reclassify traditional offences, now committed using information technologies, separately as “computer-crime” would skew time-series data on those offences (cited in Kowalski, 2002: 11). Second, these should also be fairly obvious characteristics of an offence for police to record. Beyond this, the value to law enforcement is not clear. These are not mutually exclusive characteristics, as in a single incident ICT may be the tool, target and a storage medium. Each e-crime incident sampled in this study involved information technology as the tool for committing an offence. Where it was a target or storage medium this was in addition to use as the tool.125 Each example given by Kowalski (2002: 24) of an incident that has computers as the object of the offence (“Hacking, defacing websites, creation

---

125 Recall that simple theft of a computer, which would change this, was excluded from this study.
and malicious dissemination of computer viruses”) also involves a computer as a tool to commit the offence. As even simple theft of a laptop might require digital forensic analysis, this classification would not delineate police resourcing easily.

This proposed disambiguation and hierarchical structure for taxonomic jargon aims to promote consistent understandings and use amongst law enforcement practitioners and academics. It suggests e-crime or digital crime as the generic terminology, and by retaining meanings for other terms that distinguish phenomena, rather than the common practice of interchanging terms as generic, permits more granular classifications of the phenomena at hand. Hopefully, this will permit research and policing responses to move usefully beyond the ‘syntax discrepancies’ reported in this study.

**Changes to routine activities of Victoria Police**

One of the key difficulties faced by police is lack of reporting of e-crime incidents. However, as seen in Chapter Six, local police practices contribute to under-reporting under the rhetoric of responsibilisation (see pg. 5), through “third party policing”-style requirements for evidence packages and the evidentiary model of recording incidents. What are the implications of requiring the provision of briefs of evidence to police, such that corporations are required to hire or employ their own private investigators in a defacto “user-pays” system? Does this exacerbate social inequalities of which Loader (1997: 385) warned?

First, there are practical concerns in terms of partnership policing. The responses of some potential partners to either under-report or direct reports where it suits them, described in Chapter Six, represents “marginalisation” of public police (see generally, Deering and Murphy, 2003: 132). Withdrawal of
support by community partners, such as financial institutions and Internet service providers, maintains police in a largely reactive position instead of developing proactive capabilities. That is clearly undesirable given advances in criminality that demand proactive responses reliant on information sharing. Although explicitly desiring an active response, the CCS reporting methodology provokes a passive one (MacNeil, 1968). The interplay between this policy and prioritisation of investigations is important to consider. The policy might engender exploitation of public police by organisations that are willing to pay for an initial investigation, secure in the knowledge that the incidents of others will not be reported to police through monetary considerations. Provision of an evidence package should not bias other prioritisation criteria.

However, there are also positives attached to this policy that defines victims strictly. Police advice that indicates a person has not been a victim of e-crime might empower them to avoid the “victim” label. It supposedly lessens the direct impact on them, if they are then able to force a bank or an online merchant to refund their losses, perhaps through an ombudsman. This might even be read cynically in terms of preferring not to create “ideal victims” (see Christie, 1986). Corporations make less objectionable victims than little old ladies. Further research on the impact of computer-mediated offending against individual victims is required (McKenzie, 2003). A policy of responsibilisation focused on corporations also promotes Internet commerce as safer to the individual consumer, which in turn is of benefit to the company and economy.

Should police make judgements about whether it is better to have corporate victims, who would be fewer in number and victimised repeatedly, than to have many more individual victims? Although this represents a bias against
corporate victims in favour of individuals, which might not meet Cohen and Feldberg’s (1991) ethical standard of non-partisan provision, it seems a fair compromise in the face of fiscal crises. If evidence packages are required more widely, police should formalise the policy as a matter of equity. On what basis will police decide that a particular company must hire their own investigators before public police will launch an investigation? This is the difficulty. How would police conduct legitimate means tests?

Police need to resolve the tension between whether they desire additional reporting of incidents and could cope with that or whether to discourage reporting and contribute to the dark figure of e-crime. Initiatives such as the VFIRC suggest a third way of requiring reporting for intelligence purposes only; but this is unlikely to achieve support from the corporations it intends to target. As suggested in Chapter Six, as a fundamental reform, Victoria Police should institute a strict *prima facie* model of report recording. Routine incident recording practices need improvement so that Victoria Police can more easily report on the nature of e-crime they encounter. A key example would be use of “Total Value Lost” fields in LEAP, found empty during this study. Disaggregation of “no offence disclosed” outcomes to highlight corporate reticence to report could offer means of reintegrative shaming that highlights communitarianism (Braithwaite, 1989: 86, 144).

The reporting methodology employed by the Computer Crime Squad to reduce reporting of unauthorised access incidents should be reviewed at two levels. First, to determine whether the targeted corporations have implemented better security practices since the introduction of the policy. If security procedures have improved, such that members of the community have taken responsibility, then continued use of this policy suggests an inappropriate avoidance of legislated responsibility for the costs of “agency
specific delivery capabilities” under section 332L of the *Telecommunications Act 1997* (Cth) on the grounds of responsibilisation. If security procedures have not improved, then additional regulatory measures would be required. Police might then consider accepting reports from secondary victims and undertaking investigations that might be considered analogous to “class-actions”, as a further means of reintegrative shaming of those corporations (Braithwaite, 1989: 88, 120).

Secondly, the policy should be reviewed in terms of its impact on actual levels of offending. Non-reporting should not be conflated with having reduced a crime problem. If the policy has not reduced levels of unauthorised access and credit card offences against Internet service providers and online merchants, instead only instituting non-reporting by these victims, then police have a public obligation to work with victims to investigate these offences when reported. Arguably, these offences present significant costs to the community, like fraud-related spam, as facilitators of more serious offences. Credit card fraud represented the most common deception offence in this study. It is also clear from the pressures on the Computer Crime Squad that Victoria Police would need to implement training and resourcing to permit investigation of minor e-crime offences outside of specialist squads.

In February 2005, towards the end of data collection for this study, the Assistant Commissioner of Crime for Victoria Police held a press conference and admitted that “existing police methods struggle to deal with high-level sophisticated crime” and that they had hired Boston Consulting Group to review the Crime department (Silvester, 8 February 2005). “Computer, Internet and identity crimes” were to receive a shift in priority under the review. On 28 February 2006, sections of the review were leaked to the media (Silvester, 1 March, 2006). The report recommended overhaul of the
department including disbanding several specialist squads as outmoded and inefficient including the MFID. Under the restructure, “a large bank of detectives will target individual criminals and larger crime groups” and “a series of mini-taskforces will be set up” (Silvester, 1 March, 2006). This is a reform supported by this research, as it should help remove the unintended “silo” mentality of specialist squads that hinders more effective information sharing and training. Specialists such as those in the Computer Crime Squad might more easily disseminate their specialist knowledge to their colleagues under these arrangements. Creation of specialist squads has often been a response to change in the criminal environment and subsequently they suffer policies of restricted tenure and rotation, designed to circulate skills and avoid corruption yet sometimes they reduces organisational knowledge and effectiveness (Wall, 1998: 212-3). For example, initial assessment processes, described by respondents in Chapter Six, that permit detectives to pick and choose incidents to investigate on personal preference are clearly inadequate. The issues raised by respondents about the Computer Crime Squad suggest consideration of whether the forensic computing role of the Computer Crime Squad should move to the Victoria Police Forensic Services Department; however a recommendation on this is beyond the scope of this thesis.

**Clarification of criminal law and legal advice**

The findings suggest that the model computer offences and other e-crime offences, such as those addressing cyberstalking, were not understood well by Victorian police. Inter-departmental memos are needed from Victoria Police solicitors to raise awareness of and clarify the circumstances in which these offences should be preferred. Similarly, the Privacy Commissioner of Victoria should publish advice for the public to clarify the application of the *Information Privacy Act 2000* (Vic) in relation to provision of assistance to police.
In this study, respondents raised concerns about a lack of legislation in Victoria to cover “stealing information”. There is uncertainty about what is included in the category of property under the *Crimes Act 1958* (Vic) as applies to theft (see Victoria Police, July 2003). Victoria Police raised concerns to that inquiry that a person who copies to CD an employer’s client list has not committed theft under Victorian law, despite having “taken something of immense value to the employer”. Such incidents could be investigated easily, excepting search warrant restrictions, as “unauthorised access” under the summary offence of s247G of the *Crimes Act 1958* (Vic). Arguably, the more severe offence in s247B of “unauthorised access with intent to commit serious offence” might apply. MCCOC (2001: 155) commented that in this “preparatory” offence “[m]ere unauthorised access is sufficient, if accompanied by an intent to commit an offence punishable by five years imprisonment.” If the serious offence considered is theft, which is punishable by ten years imprisonment in Victoria, and one notes in section 73(12) that theft does not require the intent to permanently deprive property, then a conviction might be secured. Under s247B, a person may be found guilty even if committing the serious offence is impossible (for instance on the basis that intangible property might not include computer data). However, this is a convoluted legal argument. Instead, the Victorian government could undertake legal advice to clarify whether the Victorian *Crimes Act* does prohibit theft of intellectual property as intangible property on the basis that intangible property includes “chooses in action” (see note 95). If this is the case, then the statutory provisions of sections 71 and 73(12) of the *Crimes Act* already override the precedent of *Federal Commissioner of Taxation v United Aircraft Corporation* (1943) 68 CLR 525. However, it would be simpler if the definition of property were amended to remove the obscurity by including “data held in a computer” explicitly. This would reflect commonwealth
legislation (DCPC: 2004: 265), which is an important consideration. Given advances in our technologically dependent society, this is an important community issue.

**Extend private investigator licensing**

As discussed in Chapter Seven, the licensing regime for private investigators in Victoria under the *Private Security Act 2004* exempts personnel from licensing if they only conduct inquiry work on behalf of their non-private security business employer. However, this research indicates that the investigative activities undertaken by many exempt investigators often resemble those of licensed investigators and police, including covert surveillance, collection of digital evidence and interviewing of suspects and witnesses. For many investigators this constituted the majority or totality of their work role. In these circumstances, the rights of those investigated, who might be employees or customers or others, need protection, however currently they lack the accountability mechanism of license suspension or revocation (see Figure 8.3).

Braithwaite (1993) argued that to “lop off the top of the enforcement pyramid, put in place nothing other than a system of rational incentives… and the firm is given little reason to cultivate business responsibility”.\(^{126}\) A complete regulatory pyramid permits escalation of responses avoiding a need for static matching of strategies according to prior identification of actors as “good” or “bad”, which as seen in Chapter Seven is problematic (Braithwaite, 1993: 89). In Victoria, disciplinary inquiries for licensed investigators are potent affairs. This is because disciplinary hearings are not bound by rules or practices of evidence (s.54(3), *Private Security Act 2004 Vic*) and may involve license

---

\(^{126}\) Critiques of the pyramid’s sole focus on state regulation (Grabosky, 1997) are acknowledged, however non-state regulation does not complete the pyramid in this context.
suspension during proceedings. The sanctions the Chief Commissioner may impose for licence contraventions or “unfair, dishonest or discreditable” activities follow a regulatory pyramid from no action through cancellation and five-year license bans. As discussed in Chapter Three, other accountability mechanisms are often not easily accessible or effective, such as civil suits that may be prohibitively costly.

However, others have argued it is difficult to include in-house security in legislative regimes:

The problem with in-house security is that every corporation has their own priorities in relation to education, objectives, training, etc., and it is very difficult to create common standards and control them (Gimenez-salinas, 2004: n.11).
This objection seems out of place in the context of regulating public interests and that Victorian private security legislation already imposes minimum training standards and probity checks successfully. Other objections include the costs licensing would impose on employers of in-house security and lack of evidence of complaints against in-house personnel.\textsuperscript{127} Investigators in this study argued against “backyard operators”, yet argued to protect their own exempt status. Thus licensing is a highly political issue.\textsuperscript{128} In the Victorian context of recent reforms to private security legislation, it is unlikely more reform will follow in the absence of a regulatory crisis similar to the death of David Hookes (see Haines, 2003: 465; and Chapter Two). Yet, it is the very lack of visibility of in-house investigators and mechanisms for review that are of concern.

How might more comprehensive licensing affect investigative partnerships? The study shows that exempted investigators are also the most likely candidates for partnership policing initiatives that concern e-crime. Private partners might be more reticent to join initiatives, given that do to so might coincidentally open them and their companies to scrutiny by police, who also conduct the inquiries into investigator misconduct. Haines (1997: 220) warns that relatively minor threats of public scrutiny can provoke changes to activities to minimise visibility and liability. Then again, more open accountability for investigative practices promotes the professional industry the respondents uniformly desired.

\textsuperscript{127} See for example, National Retail Association’s (2005) submission to a review of security provider legislation in Queensland.

\textsuperscript{128} In 2005, the Victoria Police Private Security Industry Reference Group was formed to represent industry members on licensing and regulation issues (Victoria Police, 29 June 2005).
Consequently, it is a recommendation of this research that Victorian licensing requirements be amended such that dedicated in-house investigators employed by non-security industry organisations must also be licensed, as a protection to those they investigate, to promote professionalism in the “backyards” of corporate Australia and to provide consistent regulation of practitioners. This would utilise a different test than the current one based on status of an employer as a seller of security services to determine who must seek a private security license. The test for in-house investigators should be based on classification of the investigation activities undertaken by a person in their job as a percentage of that role. Below a reasonable threshold, personnel would not require licensing. Rather than establish a separate system of accreditation requiring new oversight infrastructure (see concerns in Chapter Seven), accreditation of competency and professionalism to conduct e-crime investigations should be tied to the current licensing scheme.

**Public interest considerations for establishing public-private partnered investigations**

From the literature and research findings we can derive an inventory of legal, ethical and performance criteria that practitioners and policymakers either must or should address when forming partnered investigation of e-crime (see Table 8.1). As the format of investigative partnerships might vary from seeking cooperation for a single investigation through to the creation of a joint centre like the JBFSIT (see Chapter Seven and below) the processes required to evaluate and document fulfilment of these criteria will vary from case to case. Management of relationships within partnerships cannot be considered exhaustively here and the reader is referred to the copious management literature (for example, Huxham and Vangen, 2005; Deering and Murphy,
The issues and principles listed in Table 8.1 are detailed below.

**Table 8.1: Principles to guide decision making about partnered investigations of e-crime**

- Partnership based on necessity and potential for real collaborative advantage
  - Partnership goals translate into achievable projects
- Identify and utilise existing partnership / cooperation frameworks, avoiding duplication of effort
- Design projects to permit and withstand legal, ethical and performance scrutiny
  - Public police retain final responsibility for the professional performance of public policing
  - Build appropriate performance monitoring and evaluation into partnerships
  - Vet, select and manage partners on basis of investigation needs
  - Engagement of appropriate accountability mechanisms to coincide with partnership formation
- Anticipate wrongdoing and employ situational corruption prevention where police and private personnel interact

**Partnership based on necessity and potential for real collaborative advantage**

What collaborative advantage will the partnership deliver, instead of interacting on a purely legislated basis or going it alone (Huxham and Vangen, 2005)? Answering this will involve problem identification and scoping and setting goals. What is the issue and what is its impact on the community? Is enforcement of the law the correct solution to this problem? Does the problem warrant creation of a formal partnership?

The potential for collaborative advantage might relate to overcoming a characteristic of a class of e-crimes that is problematic to policing. For example, this might be one or a combination of the following: high prevalence
of offence, repeated victimisation, distributed targeting of victims, distributed dissemination of proscribed materials, groups of organised offenders, involvement of specialised technology or involvement of private infrastructure.

Table 8.2: Examples of benefits of investigative partnership that might combine to produce collaborative advantage

<table>
<thead>
<tr>
<th>Police interests</th>
<th>Private partner</th>
<th>Public interest</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reduces crime</td>
<td>Facilitates public image or recovery of loss</td>
<td>Public prosecution of crime</td>
</tr>
<tr>
<td>Facilitates criminal prosecution</td>
<td>Expedites case outcomes/Profit opportunity</td>
<td>Reduces inefficiencies</td>
</tr>
<tr>
<td>Reduces workload / backlog</td>
<td>Protection of revenue</td>
<td>Prevention is better than cure</td>
</tr>
<tr>
<td>Permits proactive investigation</td>
<td>Targets own serious crime problem</td>
<td>Provides for affected individuals and communities</td>
</tr>
<tr>
<td>Targets serious crime problem</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Streamlines processes and avoids duplication of effort</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Externalises or saves costs</td>
<td></td>
</tr>
</tbody>
</table>

Alternatively, it might relate solely to an efficiency gain in the processing of investigations, for example through partnership with a commercial software provider. Table 8.2 lists some examples of benefits of engaging in investigative partnership gleaned from this study that might be combined to form collaborative advantage or mutualism. These benefits need to be weighed against harms and constraints that would negate these benefits and remove the legitimacy of investigative partnership (see Table 8.3 below). If harms outweigh benefits and cannot be managed, then the initiative should not proceed.

Part of identifying collaborative advantage is that the goals of partnership should translate into achievable projects. Are the goals achievable? Are they
agreed? How would the partnership modify the factors currently inhibiting successful investigation?

Table 8.3: Examples of harms that would outweigh benefits of investigative partnerships

<table>
<thead>
<tr>
<th>Police</th>
<th>Private partner</th>
<th>Public interests breached</th>
</tr>
</thead>
<tbody>
<tr>
<td>Involves illegality</td>
<td>Involves illegality</td>
<td>Rule of law</td>
</tr>
<tr>
<td>Promotes or displaces crime</td>
<td>Increases victimisation</td>
<td>Community safety</td>
</tr>
<tr>
<td>Breaches or compromises privacy</td>
<td>Compromises client confidentiality</td>
<td>Privacy</td>
</tr>
<tr>
<td>Undermines security of investigations</td>
<td>Exposes to liabilities or profit loss</td>
<td>Security</td>
</tr>
<tr>
<td></td>
<td>Taints reputation</td>
<td>Professionalism and public confidence</td>
</tr>
<tr>
<td>Captured by outside interests</td>
<td>Juridification*</td>
<td>Independence of police, market freedoms</td>
</tr>
<tr>
<td>Lack of accountability</td>
<td></td>
<td>Accountability</td>
</tr>
<tr>
<td>Introduces or exacerbates inefficiencies and costs</td>
<td>Transparency and cost effectiveness</td>
<td></td>
</tr>
</tbody>
</table>

* See note 49.

To what degree would partnership affect this and is that worth pursuing? Decision makers should note the successes and failures of partnered investigation in other locations, but also recognise that local contexts and regulatory character will affect the success of initiatives (Haines, 2003).

Identify and utilise existing partnership / cooperation frameworks, avoiding duplication of effort

- Is there an existing partnership framework in place to guide this partnership?
- Will the envisioned initiative duplicate others unnecessarily?
- Will the proposed partnership enhance or undermine other (more important) policing efforts?

Partnerships should avoid reinventing the wheel. In the first instance, practitioners and policymakers should look to local, national and
international initiatives to avoid duplication of effort. For example, the POLSEC framework exists in Victoria to guide police and security industry partnerships. The existence and details of such frames should be made more transparent to all levels of police to reduce waste and promote efficiency and effective policing. Identifying existing structures will also aid in designing partnerships to withstand legal, ethical and performance scrutiny, which is addressed next.

**Design partnerships to permit and withstand legal, ethical and performance scrutiny**

- Do existing laws govern what arrangements can be entered into?
- Can potential harm to public interests be managed?
- Will the partnership enhance or threaten justice?
- Fair access to police services?
- Will the partnership breach privacy?
- Will police been seen as partisan?
- Will the partnership afford the partners undue commercial benefit over rivals not partnered?
- What will opponents of the proposed partnership argue? Are these fair arguments?
- Will commercial confidentiality be invoked and what are the potential impacts in terms of oversight?
- Have intellectual property issues been resolved?
- How will the respective roles in the partnership be defined?

Investigative partnerships should design in the standards proposed by MacNeil (1968) and Cohen and Feldberg (1991) detailed in Chapter Three and the POLSEC Code of Ethics (see Appendix D: POLSEC partnership documents). In Victoria, commercial partnerships will need to consider the Partnership Act
1958 Vic and the rules of equity and common law relating to partnerships. Legal advice should be sought in these circumstances. Designing to withstand scrutiny involves identifying underlying intentions. For example, does the partnership aim to influence public or the private policing? Is it a “public” or a “private” policing initiative? Will police be steering or rowing? Are you taking a proactive or reactive approach? Who is leading the process (Lendrum, 2003: 159)? Identifying intentions of partners leads to transparency of process for stakeholders and public accountability. The first imperative for partners is to make visible the invisible, on the basis that “you cannot steer when you cannot define and you cannot define what you cannot talk about” (Deering and Murphy, 2003: 22). Thus what partnership means to police should be at the top of the agenda.

When designing partnerships so that there is a clear distribution of responsibilities and obligations (MacNeil, 1968), police should work from the principle that the final responsibility for the professional conduct of criminal investigations lies with them as a public trust (Cohen and Feldberg, 1991: 39). The POLSEC Code of Ethics is premised on security practitioners observing “special standards of conduct” and manifesting “good faith in professional relationships”. While it is preferable to encourage higher standards of virtuous behaviour in private investigators, it is not preferable that the standards of public police are in any way lowered by involving private investigators in criminal investigations.

Demonstrated in Chapter Seven, the desire of police to exclude from partnership investigators who undertake criminal defence work is understandable, but belies the impartiality of their role. It is unlikely that criminal defence personnel would be admitted as partners of the Virtual Global Taskforce given its targets and partnership principles (see pp.39, 73).
However, even in adversarial justice systems collaborative advantage might be had on occasion from such investigative partnerships.

A prohibition on partners headhunting police was preferred during discussions of a commercial investigative partnership (see Chapter Seven). In general, the enforceability and value of such agreements is debatable. It is understood generally that contracts restricting an employee from entering into competition with an employer post-employment may be voided as a restraint of trade. These principles were stated by Latham CJ (dissenting) in *Linder v Murdock's Garage* (1950) 83 CLR 628 at 633-5:

> It is well established that prima facie all restraints upon trade are invalid, but that they may be upheld if the party seeking to enforce them shows that circumstances exist which make the restraint reasonably necessary for protection of a covenantee’s business and that it is not contrary to public interests.

There is a distinction made between contracts such as those for sale of property and employment contracts; the latter generally not permitting such restraints of trade. It is necessary to look at the nature of the business in question, in this case criminal investigation and prosecution. While some might conceive that police have a monopoly on investigating and prosecuting criminal matters and so should not be concerned, it is clear in practice that they do not have a monopoly on criminal investigation, as numerous private sector respondents to this study expressed frequently that they provide criminal investigation for their clients.

Though it may not be possible to restrict a member of Victoria Police from seeking employment in the private sector upon leaving the Force, it may be possible to arrange policing partnerships so that private sector partners agree
not to hire members leaving Victoria Police. The onus of establishing the reasonableness of a restraint of trade lies with the party seeking to enforce it (*Buckly v Tuty* (1971) 125 CLR 353 at 377). However, it is difficult to see the benefit to the covenantee firm that would permit such a restraint of trade (*Attwood v Lamont* (1920) 3 KB 571) except that a partnership might not take place without such a clause. Either way, enacting such anti-head-hunting provisions will not prevent the problem of members leaving for employment elsewhere in the private sector. Raising this concern confirms that in some sense police forces are in competition with the private sector. They are in competition to employ competent investigators and forensic technicians, if not in exact competition as to the services they provide.

Ethical investigative partnerships will also protect the occupational health and safety of police, their partners and the targets of investigation. For example if outsourcing digital evidence analysis results in a preponderance of child pornography analysis for individual police members this could be problematic. If publicising a policing partnership would compromise police or partner safety, this should be avoided. As demonstrated by Operation Auxin (see pg.38), undue publicity can also compromise suspects’ safety.

Performance standards required of partner investigators should attempt to avoid juridification that provokes contradictory imperatives of the “cost conscious, competitive market-oriented and risk-taking entrepreneur” and the “a risk-averse, standards conscious professional” (Haines and Sutton, 2003: 18) that would produce “gridlock” in partnerships (see Table 3.1). Appropriate performance monitoring and both formative and summative evaluation must be built into investigative partnerships. Was the partnership project implemented successfully and within specifications? Were its goals achieved, for example what impact did the partnership have on offending?
Measures of success need to be built in to address outcomes not just outputs. As discussed in Chapter Six, the Key Performance criteria for a general crime rate reduction of five percent by 2008 under *The Way Ahead Strategic Plan 2003–2008* conflates inputs (the recording of crime) with outcomes (reduction in crime) (see note 41).

Instituting shared measures of success, such as “mitigated loss” used by the AHTCC, is important to partnerships and might encourage development of initiatives between police and the private sectors. Mitigated loss speaks to police in terms of crime prevention and to businesses in terms of risk management and loss prevention.

**Vet, select and manage partners on basis of investigation needs**

- Who could help police with this problem and how?
- Should members of the community be involved with this investigation?
- Given the propensity for delay in investigations, will partners make resources available when needed at later dates?

Respondents suggested there is hypocrisy in asking whether potential partners are “worthy of participating in the partnership” (Greenberg, 2000: 320). This question might be framed better in terms of assessing the integrity of an investigation should that partner be involved. In investigations of child pornography it would be illegal to involve members of the public such that they viewed illicit materials.

The motivations of those who wish to partner with public police must be examined critically. It is not unimaginable that criminals may attempt to infiltrate the policing complex through partnership arrangements. A
particular conflict of interest affects companies that sell security like anti-virus, anti-spyware and firewall companies (Bode, 15 April 2004). They have an underlying interest in the continued threat of e-crime to generate business (see for example, Berinato, 2005). When considering formal partnerships, police and partners must be prepared to undertake security vetting, especially as Australian companies have demonstrated a willingness to hire convicted hackers. However, the question remains to what degree corporate partners will be either willing or able to fully disclose details of their associations with other persons or organisations due, for example, to commercial confidentiality or simply the complexities of their networks.

Respondents and the literature also note difficulties concerning the ongoing commitment of private partners to partnership. The investigation process can be lengthy. Will partners be available at a future date?

**Engagement of appropriate accountability mechanisms to coincide with or precede partnership formation**

- Would misconduct or corruption be detected in the proposed investigative partnership?
- Given a “breach” in a partnership agreement between law enforcement and a private sector partner, what regulatory mechanisms are available to either party?
- Could meaningful sanctions be pursued against partners whose behaviour breaches the partnership mission and standards?
- Who oversees the appropriate protection of public interests within that partnership?

Accountability mechanisms should not constitute “add-ons” or “afterthoughts” to investigative partnerships. Partnership projects must not
preclude oversight by independent accountability mechanisms, for example, on the grounds of commercial-in-confidence or similar restriction. Also, rather than impose an impossible juridification of new prescriptive standards, the key is identifying and conscripting existing mechanisms to permit regular scrutiny of investigative partnerships. The respondents identified many existing mechanisms by which interactions and joint investigations are held accountable (see Chapter Seven).

Given that the public police are highly scrutinised already, would private investigators interactions with police naturally receive scrutiny under that regulatory gaze? First, this presupposes that private investigative activities are visible to the police with whom they interact. As seen in the LEAP record analysis, this is not always the case: when police request assistance, generally private personnel obtain that information separately then provide it to police. Second, for oversight to actually occur it is critical to inform watchdogs of partnership initiatives and define their role to oversee partnerships. If police were not aware of POLSEC, were the watchdogs?

Victoria Police could certainly investigate private detectives with whom they are partnered, including those not licensed by Licensing Services Division; however the independence of this might be questioned. The Office of Police Integrity (OPI) does not have the power to investigate private individuals outside of their involvement with Victoria Police.129 However, it does have the

129 The jurisdiction and capacity of other ombudsmen to investigate misconduct and corruption of private investigators is unlikely and less than clear. For the federal Banking and Financial Services Ombudsman to investigate a complaint must relate to a “financial service”, confidentiality or privacy (section 3.1, BFSO, 2002). Similarly, inquiry into investigators employed in the Internet or telecommunications industry falls outside the jurisdiction of the Telecommunications Industry Ombudsman as “commercial activities which do not include the provision of carriage services” (TIO, 2001).
mandate and power to investigate partnership policing as a policy of Victoria Police and has a preventative role also (OPI, June 2005: 10). It also has a High Tech Crime team to investigate incidents involving digital evidence. However, does the open-ended granting of powers necessary or convenient to the Office of Police Integrity and its Director to perform their role ensure that this accountability watchdog has extraterritorial powers and jurisdiction to investigate interstate or overseas private partners (s.102B(2), Police Regulation Act 1958 Vic)? Coordination with overseas watchdogs is likely to be necessary.

In the longer term, given the increase in private policing and the hybridisation and joined-up policing by public and private actors might a broader policing accountability mechanism be required? Thus extending George Rigakos’ idea for policing boards in Canada, might an Office of Policing Integrity oversee more easily the modern merging of public and private policing personnel (see Law Reform Commission of Canada, 2002)? Such an agency might also involve tripartism through civilian participation in the oversight of both public and private policing (see generally, Ayres and Braithwaite, 1992).

Clearly, criminal sanctions exist to punish improper information sharing as evidenced by Kerry Milte’s sentence. However, the “consultant” or informer relationship that Milte had with Victoria Police was not adequately documented (see pg. 50). In late August 2005, the Victorian state government announced the creation of the Office of the Commissioner for Law Enforcement Data Security in response to the embarrassments surrounding unauthorised access to LEAP data. It will be the responsibility of this office to:

\[^{130}\text{This office would need a mechanism of oversight (“a watcher for the watchers”), just as the Special Investigation Monitor oversees the Office of Police Integrity.}\]
promote the use, by Victoria Police, of appropriate and secure management practices for law enforcement data;

• establish a regime for the monitoring of law enforcement data security management practices;

• establish appropriate standards for the access to and release of Victoria Police data, including that release to members of the public;

• refer findings from monitoring activities to other appropriate bodies for further action (Victoria, Commissioner for Law Enforcement Data Security Bill, Second reading, Legislative Assembly, 27 October, 2005, 37, Tim Holding, Minister for Police and Emergency Services).

The bill relates to data “obtained, received or held by Victoria Police”. This initiative provides an oversight mechanism to address the issues raised in this thesis about information sharing between police and private investigators. The new Commissioner should include in the new guidelines standards and protocols governing the sharing of information for investigation purposes,\(^{131}\) and also for the integrity of evidential data outsourced for forensic examination should that ever occur. Such protocols should refer to national and international standards, such as *HB171-2003 Guidelines for the management of IT Evidence* (Standards Australia, 2003).

**Anticipate wrongdoing and employ situational corruption prevention where police and private personnel interact**

• How will security be maintained?

• Can the partnership be designed to deter wrongdoing?

Chapter Six discussed the interactions between police and private investigators in terms of the interviewees’ responses to Sarre and Prenzler’s

\(^{131}\) The Commissioner should also set guidelines as to accessibility of data by researchers.
(2000) descriptive models of interaction. Table 8.4 summarises the common intersections detailed throughout this study between police and private investigators who investigate e-crime that need consideration in partnership policing. Misconduct or corruption that might arise from these interactions might resemble “quick dash” transactions as described by Felson (1998: 67-71). Ad hoc partnerships, involving different people each time, supposedly reduce opportunities for corrupt investigation on the basis that it “takes time to develop ties for most corruption” (Ede, Homel and Prenzler, 2002: 213).

Table 8.4: Intersections where police and private investigators of e-crime interact

- reporting incidents to police
- provision of evidence packages
- police requesting information during investigations
- sharing equipment
- secondments
- attendance at crime scenes and interviews
- conferences, seminars and association meetings
- training sessions
- donations and sponsorships
- online forums

However, they might also permit more predatory interactions where one group takes advantage of the other if capable guardians are absent.

From this study of LEAP records and interviews with police and private investigators, several suggestions can be made about situational prevention techniques that might reduce the facilitators of many potential forms of misconduct and corruption in partnered e-crime investigations. Table 8.5 matches concerns to techniques that might deter or prevent offending.
Table 8.5: Situational corruption and misconduct prevention techniques for partnership policing of e-crime

<table>
<thead>
<tr>
<th>Techniques</th>
<th>Issues</th>
<th>In practice</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Increasing perceived effort</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Harden targets</td>
<td>Evidence tampering, accidental destruction</td>
<td>Strategies to increase security of digital evidence, eg calculate MD5 hashes of seized digital evidence; use Write Once Read Many media; give copies at time of seizure; encrypt seized digital evidence; provide partners performing analysis duplicate digital evidence only (not originals);</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Coercion of partners to compromise investigations</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Counter-intelligence employed for joint investigations to protect police and partners</td>
</tr>
<tr>
<td>Screen entries/exits</td>
<td>Infiltration by corrupt practitioners</td>
<td>Background checking of potential partners; probationary periods in partnership agreements; referees required for overseas partners; restricted electronic card access or ‘visitor’ access for partners</td>
</tr>
<tr>
<td>Deflect offenders</td>
<td>Evidence tampering, poor work standards</td>
<td>Remove performance pressures to fabricate evidence; share responsibility for outcomes</td>
</tr>
<tr>
<td>Control facilitators</td>
<td>Unauthorised access to seized evidence</td>
<td>Disallow thumb drives and mobile phones in secure evidence rooms</td>
</tr>
<tr>
<td><strong>Increasing perceived risks</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Extend guardianship</td>
<td>Evidence tampering, poor collection practices</td>
<td>Assign police responsibility to oversee partners seconded onsite and vice versa</td>
</tr>
<tr>
<td>Assist natural surveillance</td>
<td>Abuse of due processes, excessive force</td>
<td>Clear identification of civilian partners on raids to distinguish from plain clothes detectives</td>
</tr>
<tr>
<td>Surveillance by peers</td>
<td>Evidence tampering, biased analysis</td>
<td>No solo-seizures of digital evidence; protections for whistle blowers built into partnerships; review of evidence packages by police</td>
</tr>
</tbody>
</table>

[cont.]
Table 8.5: Situational corruption and misconduct prevention techniques for partnership policing of e-crime (cont.)

<table>
<thead>
<tr>
<th>Techniques</th>
<th>Issues</th>
<th>In practice</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Increasing perceived risks (cont.)</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Strengthen formal surveillance</td>
<td>Kickback corruption, abuse of power eg, coercion of confessions</td>
<td>Centralised and auditable referrals; require video of interviews in private sector; engage formal watchdogs; auditing of information provided to police; integrity testing of police and partners; formal review of partnership agreements</td>
</tr>
<tr>
<td>Reduce anonymity</td>
<td>Unauthorised information sharing</td>
<td>Record access to police databases, details of partners who conduct forensic computing and other investigation tasks</td>
</tr>
<tr>
<td><strong>Reducing anticipated rewards</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Conceal targets</td>
<td>Unauthorised information sharing</td>
<td>Segment visibility and access of police computer directories</td>
</tr>
<tr>
<td>Target removal</td>
<td>Exposure to illicit materials in evidence (eg, child pornography)</td>
<td>Outsourced decryption tasks on keys only, i.e. not files possibly containing illicit material; clean desk and screensaver policies</td>
</tr>
<tr>
<td>Identify property</td>
<td>Theft of seized items &amp; shared equipment, software piracy</td>
<td>Mark police and partner property, record sharing of investigative equipment</td>
</tr>
<tr>
<td>Disrupt markets</td>
<td>Unauthorised information sharing</td>
<td>Sting operations, prosecute those who sell or leak information info</td>
</tr>
<tr>
<td>Removing inducements</td>
<td>Theft of seized items, abuse of process, eg not recording reported incidents</td>
<td>Timely destruction or return of seized evidence when no longer needed; remove discretion to not record reported incidents and policies of discretionary enforcement, eg for unauthorised access</td>
</tr>
<tr>
<td>Denying benefits</td>
<td>Evidence tampering, “tick and flick” mentality of investigators, non-reporting by victims</td>
<td>Exclude evidence obtained improperly; disaggregate and report on reasons for “no offence disclosed” incidents</td>
</tr>
</tbody>
</table>

[cont.]
### Table 8.5: Situational corruption and misconduct prevention techniques for partnership policing of e-crime (cont.)

<table>
<thead>
<tr>
<th>Techniques</th>
<th>Issues</th>
<th>In practice</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Reduce provocations</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reduce frustrations and stress</td>
<td>Deliberate delay of investigations</td>
<td>Negotiate and formalise deadlines for partnered tasks, remove improper discretions in prioritising investigations</td>
</tr>
<tr>
<td>Avoid disputes</td>
<td>Disputes between partners leading to bad publicity or civil actions</td>
<td>Negotiate agendas and responsibilities of partners upfront, risk analysis of partnership, agreed dispute resolution mechanisms</td>
</tr>
<tr>
<td>Reduce emotional arousal</td>
<td>Ill-will between partners undermines effectiveness</td>
<td>Change culture of slurring ex-police, now working as private investigators</td>
</tr>
<tr>
<td>Neutralise peer pressure</td>
<td>Circumventing procedures, unauthorised information sharing</td>
<td>Remove personal preference from assignment of investigations, “Partners in policing follow due process”</td>
</tr>
<tr>
<td>Discourage imitation</td>
<td>Sloppy practices</td>
<td>Communicate examples of good and inappropriate investigation practice</td>
</tr>
<tr>
<td><strong>Removing excuses</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rule setting</td>
<td>Lack of accessible accountability mechanisms</td>
<td>Extend licensing to all investigators</td>
</tr>
<tr>
<td>Post instructions</td>
<td>Sloppy practices, evidence tampering, unauthorised information sharing</td>
<td>Publication of accepted forensic computing techniques; clarify consequences and oversight mechanisms</td>
</tr>
<tr>
<td>Stimulating conscience</td>
<td>Software piracy</td>
<td>Chain of evidence procedures, “Copyright infringement is stealing”</td>
</tr>
<tr>
<td>Controlling disinhibitors</td>
<td>Exposure to illicit materials in evidence, breach of privacy</td>
<td>Secure unattended computers used for digital analysis of illicit materials, record access and reasons for access to evidence and databases</td>
</tr>
<tr>
<td>Facilitating compliance</td>
<td>Inaccuracy in reporting affecting police intelligence</td>
<td>Advise private investigators of police brief requirements (eg in VPM); hard code fields in police database systems</td>
</tr>
</tbody>
</table>

Mechanisms for public-private partnerships for e-crime investigation

Seven forms of investigative partnership are now discussed as they might be implemented ethically and effectively at the state police level. This is the “program specification” phase of this realist evaluation (see Figure 4.1). The partnership types discussed below are essentially local investigative partnerships to address e-crime. Respondents in this study, both public and private, acknowledged geographical and jurisdictional constraints that put transnational investigative partnerships low on their priority scales. International incidents are referred to the Australian High Tech Crime Centre and transnational investigations that might involve overseas or multinational private organisations are coordinated through overseas law enforcement agencies.

Partnerships through industry bodies: extending the POLSEC framework

As the purported, central coordination mechanism for strategic partnership between Victoria Police and the private security industry, POLSEC should be extended beyond its current focus on drug crime to facilitate coordination of partnered investigative efforts into e-crime and other crime requiring partnership policing. The focus only on drug offences and security personnel led to the reported withdrawal of AISP. That no other organisation representing Victorian e-crime investigators (see pg. 45) sits on the POLSEC committee is problematic. This highlights the attendant problems of a discourse of “private security” that can overlook the differences between security providers and investigators and consequently overlook opportunities and marginalise investigators from initiatives. A difficulty is that the initiative has been the responsibility of a few people within Victoria Police, instead of
an organisation wide program (POLSEC, 7 March 2006, personal communication).

The focus within POLSEC has been on liaison committees within local police districts, which might be thought to conflict with borderless e-crimes and not suit investigators or investigation firms representing national or even multi-national corporations. Where these organisations seek a one-stop-shop this is problematic. However, in the longer term, building networks into the levels lower than squad level would help extend e-crime investigation skills throughout police and complement the “push-down” nature of national initiatives like the JBFSIT. POLSEC needs to cater to both geographically bounded crime problems and also those that are based on class of crime or class of private partner. It should not become simply another discussion forum. The benefit POLSEC offers is guidance, structure and an informal oversight mechanism for partnership activities, such as the ones discussed in Chapter Seven and below.

To achieve this, POLSEC might form subcommittees for partnership initiatives not based in local districts, such as ones targeting e-crime. A concern of course is to avoid instituting the same silo mentality in partnership arrangements that has been denounced recently in police specialist squads or juridification. It would also be important not to duplicate function, such as the existing liaison with Internet service providers through CCS.

Sarre and Prenzler (2000: 106) suggested that an executive committee such as POLSEC should also involve an ombudsman. Accountability mechanisms are at the disposal of POLSEC, however the regulatory character is one of a “light touch”. The non-disclosure agreement for committee members would be familiar fare to private personnel (see Appendix D) and it is expected that separation of licensing issues from POLSEC assists with perceptions of
equality among members. Necessarily, POLSEC works behind closed doors in the interests of operational security and safety. It is not the public discussion forum Loader (1997) envisaged. Consequently, the Office of Police Integrity must have full access to POLSEC in a form it considers appropriate, which might or might not involve attending POLSEC meetings. Certainly POLSEC should produce or adopt generic guidance for other police officers on forming and running partnership initiatives between police and the security industry, such as standards Victoria Police requires, so that individuals need not reinvent these afresh nor act unguided. Police also need partnerships made more visible internally (whilst considering security of investigations), such that incidents might be directed to them where appropriate.

**Ad hoc joint investigations**

In Chapter Six, the interview respondents described the most common police-private sector interactions for e-crime investigation as ad hoc partnerships focused on investigation of individual incidents of crime. This interaction might occur within broader frameworks of cooperation between police and organisations or it might not. The “needs basis” and flexibility of this style of partnership is mutually beneficial and important to retain for routine reactive policing. Partnership frameworks, like POLSEC should not ignore this style of individual partnership to focus only on more formal arrangements. Nor, however does it seem that specific rules are required amidst the existing suite of regulations guiding police. POLSEC guidelines might simply acknowledge the status and importance of these “partnerships” without requiring other than existing bureaucracies. At most, clearer consistent documentation of private sector involvement in individual investigations is needed to facilitate overview by watchdogs.
Joint investigation teams and secondment of investigators

Can and should the model of secondments exemplified by the Joint Banking and Finance Sector Investigation Team at the AHTCC be replicated at the state police level? What are the key factors to the JBFSIT success? This study provides an exploratory evaluation of the JBFSIT model based on six interviews over two days. More rigorous formative and summative evaluations should be conducted as to the success and defensibility of this secondment model. However some factors were clear: the unambiguous need for partnership to address the problem effectively, a clear operational focus on a particular crime type, harnessing market rivals in co-opetition (see pg. 62), bi-directional learning and practice and physical secondment to a central location. Additionally, the JBFSIT exhibits each of the characteristics MacNeil (1968) proposed for relational contracts. Conceiving of the initiative as a “combined forces” model and either as a “do and review” or “radically new” style partnership (see Table 3.1) was also instrumental.

In the JBFSIT, the division of policing powers remained traditional. Public police had public policing powers and private partners did not. Federal police still held the leadership roles in the JBFSIT, reflecting the perhaps inevitable continuation of the turf war over “elite policing” (O’Malley and Palmer, 1996: 151-2). Further complicating Bayley and Shearing’s (2001: 3) description of how auspices and providers of policing combine, in the JBFSIT both public police and private banks authorised the secondment of private investigators. Personnel from both sectors also performed the investigations conducted by the team.

Arguably, the collaborative advantage to police and corporate partners of seconding investigators is derived already at the national level and to simply replicate joint investigation teams at the state level would create undue
duplication of effort. This would be true at least in terms of phishing and financial institutions. To form partnered investigation teams at the state level would re-introduce the problem of multiple physical locations that partner corporations need to resource, as described in Chapter Seven in the comments about selecting partners and the private sector preference for a one-stop shop to both receive and provide assistance.

Appropriate joint investigation teams at the state level could work on the basis of referrals from the AHTCC. They could also take responsibility for e-crime no longer considered “high-tech” and less complex incidents that would not otherwise receive national attention. These teams would most likely take on the characteristics of “mini-taskforces”, as envisaged for squads in the Victoria Police Crime department restructure, with seconded private investigators. Such teams should include in their terms of reference recognition of the national coordination role of the AHTCC in e-crime investigation matters.

Having been unable to analyse unsolved incidents, it is difficult to identify classes of e-crime that warrant the establishment of investigative partnerships in Victoria. The respondents suggested higher priority for a number of types of e-crime (see pg. 217), however that might not entail partnership policing. These might represent important ‘signal crimes’ to address (see Innes et al, 2004). Many of the prevalent e-crime incidents examined in Chapter Five would be amenable to partnership policing initiatives that might not include private investigators. For example, partnerships with the hospitality industry to address skimming, with computer repair companies to detect digital child pornography and with local marketplaces to address sale of pirated software and other media. E-crime that might benefit from secondment of one or more private investigators might include credit card fraud, false accounting,
Internet banking fraud, identity theft or fraud or even harassment via telephone, based on making up gaps in police skill sets, accessing transaction records more efficiently or manpower to process digital evidence. Investigative partnerships might be established to address backlog within the CCS and even investigation of cold cases, excluding child pornography cases.

Would this model be defensible legally and ethically? Underlying joint investigation are tensions between police interest in developing their own capabilities, maintaining independence, complying with regulations and addressing partners’ needs. First, secondment of private investigators into public police does not involve divestment of police investigative function or powers in this model. Second, it brings private personnel within the ambit of public accountability and its mechanisms. Judicious management of secondments, as in the JBFSIT where police “call the shots”, would reduce opportunities for secondees to influence priorities and decisions.

However, under s.5 of the Private Security Act 2004 (Vic) businesses might require private security business licenses to second their investigators to Victoria Police to conduct joint investigations as that could construe “the business of providing the services of other persons to carry on an activity...[of] an investigator”. Seconded investigators would then also require licenses.

**Outsourcing, referral of investigations and a VFIRC**

It is unlikely that any police force, government or community would agree with investigator suggestions that almost any investigative task could be outsourced; many police tasks are considered “core” and the province of public police alone. However, Victoria Police has tendered out some of its activities as “non-core” since 1993/94 (Davids and Hancock, 1998: 47). South
Australia Police considered outsourcing its e-crime investigations in 2002 (Douglas, 26 Sept, 2002). What constitutes “non-core business” in terms of e-crime investigation that could be outsourced and “core” that must not? Extending from Loader’s (1997) arguments that there are some aspects of policing that should not be contracted out, similarly should some elements of policing not be reframed as the defacto responsibility of non-state actors? These questions are “crucial to decisions about what should and should not be divested from state control and oversight” (Davids and Hancock, 1998: 49). Davids and Hancock suggest that previous privatisation of “non-core” police functions in Victoria has been motivated by political motives or cost savings without adequate reference to public discussion of “the actual activity of policing itself”.

For example, under a partnership arrangement might suitably qualified employees of a corporate investigation firm attend crime scenes to collect digital evidence with police officers who oversee the seizure? Would the officer need to be qualified to judge that the collection and preservation of evidence was performed correctly? Might that not entail training that might mean they could perform the collection themselves? One would also need to prohibit subcontracting to unqualified or unlicensed operators (see generally, Prenzler and King, 2002: 5). There is the possibility that improperly trained private investigators might contaminate crime scene evidence.\(^{132}\) Also, Victorian law prevents private investigators viewing seized computerised child pornography.

What might outsourcing of e-crime investigation activities mean to provision of public policing and accountability? Unless a partnership contract made other arrangements with their partners, police would remain liable for costs

\(^{132}\) Just as under-trained public police might also contaminate e-crime scenes.
awarded against them by courts. Flemming and Rhodes (2005: 194) argue that the unintended consequences of contracting out include rising transaction costs, often masked initially by short-term savings. Without conducting comprehensive security audits of potential partners and their systems, unintended breaches of privacy and displacement of crime could easily occur (see for example, Boggan, 3 May 2006). Corporate partners might challenge shared liability contracts to protect revenue, which would not benefit public police forces. Other costs might include weakening of traditional police authority to appeal for community support successfully over private police market competitors (Loader, 1999: 378).133

Police partnerships also need to consider commercial confidentiality and intellectual property issues. Once a policing task is contracted to a private organisation, commercial confidentiality could be invoked, as it has been done in the case of privatisation of prisons (Davids and Hancock, 1998: 58). Davids and Hancock warn that “aggrieved public customers” of policing tasks provided by private operators might find accountability mechanisms such as an ombudsman’s office unavailable to them and be forced to undertake civil litigation to seek redress. Partnerships that for example develop intellectual property should not restrict law enforcement from subsequently turning that intellectual property to other policing activities or perhaps even sharing it with other law enforcement agencies. Law enforcement should avoid getting locked into particular brands of forensic computing software (see for example, Victoria Auditor-General’s Office, 1996: section 2.6 on LEAP licensing concerns).

133 Alternately, forensic computing might be transferred to unsworn Victoria Police analysts, perhaps within the Forensic Services Department, which might address skill shortages through lateral entry of additional staff within the economic pressures of the police budget.
In short, Flemming and Rhodes argue that we do not know the medium- to long-term costs of contracting out police services. The infancy of partnership policing in relation to e-crime as found in this study precludes judgement about longer-term impacts, which will require further examination.

Outsourcing and referral amount essentially to the same divestment of policing activities, except in regards to who pays for the private service. Either a blanket prohibition on referring complainants to private investigators is needed or a centralised referral mechanism to coordinate fair referral. Either would promote accountability and help avoid repeats of the Window Shutters scandal, by raising the risk that referrals for kickbacks were detected. Should a Victorian Fraud and Information Reporting Centre (VFIRC) be established within Victoria Police, it might coordinate referrals as part of its mandate to refer matters to “appropriate agencies for investigation” (DCPC, 2004: 88), if investigation firms were considered appropriate agencies.

Police supported a VFIRC that would provide intelligence capability for proactive investigations. However, as noted on pg. 40, the proposal stated that the VFIRC would not perform an intelligence function, instead recommending that a national Australian Fraud Centre should perform this role. For a VFIRC to be of value it would need to provide timely information to investigators. Even though legitimate avenues may exist for information exchange, bureaucratic delay fosters corruption (Roden, 1992 cited in Fairchild, 1994: 116).

Private donations or sponsorship of public policing

As demonstrated in Chapter Six, the potential cost of an e-crime investigation is a key factor affecting whether or not that investigation or others like it commence. It is an economic pressure that raises the possibility of private
organisations offering donations or sponsorship to public police forces. Could it be in the public interest for private sector organisations to sponsor public policing of e-crime? Greenberg (2000) warned against entering partnership solely on the basis of funding. Grabosky (2001: 3) asks two important questions inherent to the issue of sponsorship, “Who pays?” and “Who benefits?” Those who offer gifts to police may seek recognition, preferential treatment or some other favour. The threats to police associated with private sponsorship are conflict of interests that can be described as ‘capture’ by a donor, personal benefit, actual or perceived endorsement of a donor and possible association with less savoury donor industries or interests (Grabosky, 2001). The issue is not black and white, Grabosky asking a telling question: what difference in perceived endorsement is there when police purchase commercial products, such as their weapons, stationery or even forensic software as opposed to receiving similar products or services via donation or sponsorship? Vendors are certainly able to and do advertise that they have sold their products to police. Another concern for law enforcement would be that government might reduce its contribution to the police purse in response to private donations and sponsorship (Grabosky, 2001: 12).

Grabosky argues that the goal must be a “win-win-win trifecta” of benefit to the private actor, public police and public (Grabosky, 2001: 5). Do these sponsorship considerations extend to “human resources”, such as secondment of investigators, analysts or solicitors to a joint investigation team? Most likely so. Clearly the financial institutions that have formed the JBFSIT profit from doing so; however it is also in the public interest to respond to this costly form of e-crime. Any joint investigative initiative
between police and private investigators in Victoria would likely be premised on at least partial funding by the private sector.134

Noting that even the Melbourne Cup horserace became the Fosters Melbourne Cup,135 Grabosky (2001) even wondered if we might one day see a “Microsoft Computer Crime Squad”? Clearly sponsorship should not give the donor any influence over police activities nor confer naming rights (Grabosky, 2001). The exemptions under section four of the Private Security Act 2004 (Vic) mean that companies not in the private security industry but with in-house e-crime investigation teams, such as banks, are not regulated by police and would not be prohibited prima facie from sponsorship on this basis. As discussed above, the uneven regulation in this regard seems arbitrary.

**Conclusions**

Law enforcement agencies worldwide, including those in Australia, declared as “critical” the pursuance of partnerships with the private sector to police e-crime. The imperatives relate primarily to bolstering police skill-sets, preservation of and timely access to digital evidence and sharing information about incidents and trends to permit and focus proactive responses. However, uncertainties about both appropriate formats and the potential to unintentionally foster corrupt policing weigh down this strategy. In particular Sarre and Prenzler (2000: 107) argued against “striving for a totally symbiotic tie” between police and the private security industry on those grounds and the inherent, conflicting principles on which each operates.

---

134 As was proposed for the Victorian Fraud and Information Reporting Centre (DCPC, 2004: 86).

135 In 2005, it was the “Emirates Melbourne Cup”. 
Consequently, this thesis set out to examine the contexts under which partnerships for investigating e-crime between public and private police could produce mutualism, while adhering to public interests. The thesis focused upon investigative public-private partnerships as the most controversial form of partnership. There is no doubt that effective reduction of e-crime requires that crime prevention be central to modern policing. Collaboration that focuses upon investigation of e-crime might by necessity form a part or subset of broader alliances aimed at addressing electronic and other crime problems. Rallying to Bayley and Shearing’s (2001: 35) research agenda, this research adds to our foundational knowledge of modern policing by describing routine activities of e-crime investigation and furthers debate on the appropriate normative relationships between public and private police.

The formation of the JBFSIT investigative partnership illustrates a realisation by private police in the financial sector similar to that public policing in general had in the 1980s (see Chapter Three) and which led to post-Keynesian community policing: private police cannot function independently to address high tech crime. Its complexities and transnational nature and their failure to contain it alone implies they need to work cooperatively with public law enforcement and other members of their industries. This context is facilitating information sharing and coordination efforts between the public and private policing sectors.

However, the results of this study cast doubt on the necessity of formal public-private partnerships for the successful investigation of e-crime by public police, especially when considered in the context of their legal powers and constraints. Police and investigators identified many other factors that affect their successful investigation of e-crime at the state level over and above partnership with the private sector (see Chapter Six). Instead, the primary
importance of partnerships to respondents appeared to be in achieving efficiencies and cost-savings. That said, clear synergistic benefit to investigating e-crime was evident in the secondment model used at the AHTCC.

Sarre and Prenzler’s (2000) descriptive models of police and private security interaction resonated with the interviewees, highlighting their usefulness to the examination of such relationships. The thesis examined Sarre and Prenzler’s (2000) *Regulated Intersections* model by both asking respondents to comment on it and through an analysis of its regulatory character. Its prescription of avoiding corrupt and wasteful relations enunciates worthwhile, if obvious, minimum standards for interaction. Targeting regulatory efforts at the intersections between police and private security accords with routine activity theories of crime and situational prevention.

However, this thesis has argued that as a normative model *Regulated Intersections* stops short of the final destination for which we should aim: an effective and ethical combined forces model. The relationship should be complementary and proactive. Sarre and Prenzler’s objections to the combined forces model were based on concerns about corruption and complicatedness, underscored perhaps by an assumption that symbiotic relationships entail divestment of public policing to the private sector (see Sarre and Prenzler, 2000: 103), which would, as Loader (1997) argued, advance socially divisive, two-tiered provision of security. However, this research demonstrates through examination of various investigative partnership mechanisms that this is neither a necessary outcome of closer ties between public and private police, nor the trajectory currently emerging in relation to e-crime investigation. *Regulated Intersections* should pave the way to that combined forces model.
In terms of proper investigative partnership mechanisms to pursue, the study concludes that this requires first establishing the collaborative advantage, clear projects, roles, funding and most importantly monitoring, accountability and integrity mechanisms. Where these can be established, investigative partnerships should be pursued. Earlier in this chapter, guidelines for establishing effective and ethical investigative partnerships were derived from the literature and research findings and seven forms of partnership favoured by key stakeholders who participated in the research were discussed.

The research indicates that policing partnerships that involve either joint criminal investigation or the secondment of private resources into public police agencies are more defensible both in terms of effectiveness and public interests than those that outsource investigation capability of public police to the private sector. The former arrangements do not entail divestment of public policing functions and offer a means to bring private policing into the spotlight of public policing accountability, whilst building public police capabilities.

In light of these findings, police need to establish firmly the successes of existing partnerships, such as the JBFSIT and POLSEC, to engender and reinforce support for partnership policing of e-crime both internally and with current and potential partners. Benchmarks and success stories are needed, by which future investigative partnerships might be judged and improved. This study highlights the importance that investigative partnerships not be mere public relations exercises. This will require institutionalisation of performance criteria for partnership policing that measures and reports outcomes as well as relevant outputs meaningfully. In general, Australian police should institute strict *prima facie* models of report recording to give credence to their
performance measures based on crime reduction and to avoid conflation of inputs (the recording of crime) with outcomes (reduction in crime). It is clear from this study that current practices contribute to the dark figure of e-crime and in so doing act to maintain public police in a reactive stance rather than enabling better proactive and intelligence-led policing of e-crime.

These conclusions also suggest an agenda for further academic research. As mentioned above, future research on e-crime reported to police should examine both solved and unsolved incidents and should analyse briefs of evidence as a richer and presumably more consistent source of detail. At the same time as addressing the most serious e-crime, what are the ‘signal e-crimes’ that disproportionately affect perceptions of e-crime and online safety? Addressing these could impact positively upon under-reporting (see generally, Leicestershire Constabulary (UK), 2004: 19).

Researchers should evaluate current and future partnership initiatives rigorously to confirm that they are successful, maintain public interests and do not divest core public policing responsibilities. The relationship AusCERT has with Australian law enforcement agencies, which it was not possible to examine in any depth during this study, should also be researched. Likewise, the effectiveness of situational prevention and accountability mechanisms suggested by this research, which might be applied to prevent or punish corrupt public-private e-crime investigations, should also be evaluated formally.
References

[Abbreviations used in the thesis are spelled out in the reference list.]


—— (1997) *Australian Standard Offence Classification (ASOC)*, ABS Catalogue No. 1234.0.


Crawford, A. (2005) “Governing the future? The contractual governance of youthful behaviour”, guest lecture to the Department of Criminology, University of Melbourne, 4 October.


Department of Communications, Information Technology and the Arts (June 2004) Phishing – don’t take the bait!, Canberra: Commonwealth of Australia.


“Hackwatch spokesman charged” (2 October 1989), Computing Australia.


In the Realm of Hackers (2002), documentary, Film Australia / John Moore Productions.


Lawler, B. (December 2001) “Economic crime investigations can’t be done in isolation”, *Platypus magazine*, No. 73.


Model Criminal Code Officers Committee of the Standing Committee of Attorneys-General (Jan 2001) “Damage and Computer Offences and Amendments to Chapter 2: Jurisdiction” in Model Criminal Code Report, Canberra: Commonwealth Attorney-General’s Department, Ch. 4.


The Courier Mail (4 October, 2004) “Police ponder porn deaths lesson”


War Games (1983) movie, CBS Fox.


Legislation

Statute title followed by thesis page references. Excludes references to statutes in Appendix O: LEAP sample demographics.

**Commonwealth of Australia**

- Copyright Act 1968: i, 285
- Crimes Act 1914: 37
- Crimes Legislation Amendment (Telecommunications Offences and Other Measures) Act (No. 2) 2004: 520
- Crimes Legislation Amendment Act 1989: 28
- Criminal Code 1995: 54
- Cybercrime Act 2001: 19, 32, 347
- Interception Act 1979: 54
- Privacy Act 1988: 246
- Spam Act 2004: 113
- Telecommunications (Interception) Act 1979: 54
- Telecommunications (Interception) Amendment (Stored Communications) Act 2004: 54
- Telecommunications Act 1997: 54, 203, 225, 354

**State of New South Wales**

- Crimes Act 1900: 103

**State of Queensland**

- Sexual Offences (Protection of Children) Amendment Act 2003: 520

**State of Victoria**

- Commissioner for Law Enforcement Data Security Act 2005: 371
- Confiscation Act 1997: 254, 255, 294
- Constitution Act 1975: 111, 464
- Crimes (Sexual Offences) Act 1991: 129
- Evidence Act 1958: 294
- Information Privacy Act 2000: 109, 246, 355
- Magistrates’ Court Act 1989: 294
- Partnership Act 1958: 58, 105, 365
- Police Regulation Act 1958: 110, 294, 371, 463
- Private Agents Regulations 2003: 44
- Private Security Regulations 2005: 43
- Summary Offences Act 1966: 129, 194
- Surveillance Devices Act 1999: 74, 218
Telecommunications (Interception) (State Provisions) Act 1988: 218

**United Kingdom**
- Crime and Disorder Act 1998: 75
- Police Reform Act 2002: 75

**United States of America**
- Sarbanes-Oxley Act 2002: 43

---

**Legal authorities**

Case title followed by thesis page references.

**Australia**

*Attwood v Lamont* (1920) 3 KB 571: 367
*Buckly v Tuty* (1971) 125 CLR 353 at 377: 367
*Federal Commissioner of Taxation v United Aircraft Corporation* (1943) 68 CLR 525: 216, 356
*Jago v District Court of New South Wales* (1989) 168 CLR 23: 265
*Kennison v. Daire* (1986) 160 CLR 129: 27, 204
*Linder v Murdock’s Garage* (1950) 83 CLR 628: 366
*R v Baxter* (1987) 84 ALR 537: 27
*R v Evenett* (1987) 2 Qd R 753: 27
*Thompson v Australia Capital Television* (1996) 141 ALR 1 at 10-11: 55

---

**Parliamentary debate**

Victoria, Commissioner for Law Enforcement Data Security Bill, Second reading, Legislative Assembly, 27 October, 2005, 37, Tim Holding, Minister for Police and Emergency Services: 372
Appendix A: Phishing, Pharming and DDoS

Phishing emerged in 2003 as a major threat against financial institutions. Email messages attempt to lure bank customers to “reconfirm” their logins and passwords at fake banking websites after which their funds are stolen from their accounts. These emails have appeared increasingly legitimate, sometimes linking to parts of the legitimate banking website as well as the fake one such as in the example in Figure App A.1. One variant told recipients they were under investigation by police and to visit a website for more information (Lebihan, 18 Feb 2004).

Figure App A.1: Example of a "phishing" email

136 The researcher has collected hundreds of examples of scam emails. The selection of this example for inclusion in the thesis should not infer any special vulnerability on the part of the Commonwealth Bank of Australia. All the major banks in Australia have been subject to phishing email scams.
The scam works because it does not involve initially compromising the financial institution’s website or accounts (see Figure App A.2). Instead the website is copied and hosted on a separate server most often overseas. After a victim logs into the faked banking website with their login details, these are sent to the scammers who access the account and withdraw funds. To target harden their accounts, financial institutions first implemented restrictions on overseas transfers, often imposing 24 hour or longer delays in processing transfers. But, the scammers avoid these restrictions by “hiring” unwitting “mules” via email ads offering what seem like legitimate “Jobs for Australian

**Figure App A.2: Anatomy of a phishing scam**

1. Crook sends phishing email to millions of potential phish

2. Victim visits fake site and enters banking details, which are sent to the crook

3. Crook accesses victim’s real account and transfers money to mule

4. Mule transfers stolen money to crook
Citizens” to act as “money transfer agents”. As the scammers say in their recruitment emails: “We just can’t wait weeks to receive money via international bank transfers” (scam email). The scam continues to work because the mules reside in Australia allowing the scammers to transfer the stolen funds first within Australia and then the mules transfer overseas. The mules often believe they are legitimate employees of multinational companies, working from home for commissions sometimes as high as fifteen percent of an amount transferred. This makes prosecution difficult when mules lack knowledge of their complicity.

**Figure App A.3: Example of HTML code used in phishing emails to redirect unsuspecting users**

*How the email displays on-screen:*

Dear user!

We are informing you that today, the amount of $721.00 AUD has been drawn out of your account.

Technical assistance of National Bank.

http://www.national.com.au

*The HTML code underlying the email:*

```html
<p>Dear user!</p>
<p>We are informing you that today, the amount of $721.00 AUD has been drawn out of your account.</p>
<p>Technical assistance of National Bank.</p>
<form action=http://aicworld.info/national.htm method=get>
</form>
```
Early phishing emails were easier to spot, written in poor English and with clearly faked web links. However, they are becoming increasingly sophisticated (see for example, Figure App A.3). Although in Figure App A.3 the hypertext link displays as the address of the real banking website, even when the mouse is hovered over it, clicking this link will take a user to an entirely different website, because of the underlying HTML code. The lower half of Figure App A.3 reveals the HTML code underlying the phishing email. The “style” described in the INPUT tag changes an otherwise familiar (and thus suspicious HTML form button) to appear as a hypertext link disguising the true destination. These technical tricks make it increasingly difficult for consumers to identify frauds from legitimate correspondence.

In addition to duping mules into committing theft, organised criminals collect personal details from their mules that permit identity fraud against the mules.
Figure App A.4 illustrates an example recruitment email that not only aims to attract unwitting accomplices to the phishing fraud, but also to harvest personal information from the many applicants. References to well known companies give the semblance of legitimacy, despite the fact they have no actual involvement.

In 2005, phishing scams became even more sophisticated with the advent of “pharming” (F-Secure, 2005). Rather than rely upon social engineering to trick users into visiting fake websites, pharming uses technical exploits to redirect the user automatically without their knowledge. This is the online equivalent of pointing signposts in a different direction to where they should point. This circumvents the advice from financial institutions to always type their bank’s website address into the browser, instead of clicking on links in emails. One form attacks the address bar in web browsers on individual computers, so that when certain addresses are typed in, such as a bank’s web address, a different address request is actually sent from the user’s computer. Another form exploits vulnerabilities in Domain Name Service (DNS) servers. DNS servers translate the text address typed into a browser (eg www.realbank.com) into the underlying unique numerical IP address (eg 137.253.30.2). This attack modifies the records a DNS hold about the target web server and redirects all traffic to a fake site. In 2006, phishing lures moved from emails into auction listings on auction sites (Evers, 3 April 2006).

Distributed denial of service (DDoS) attacks aim to disrupt online commerce and involve first compromising an army of computers attached to the Internet, known as a botnet (see Figure App A.5). This is done by exploiting security vulnerabilities in individual computers and then secreting DDoS software onto them. These zombie computers could come from anywhere:
Figure App A.4: Example “mule” recruitment email

Need Extra Income? Lack money?
New opportunities for you - today!

Australian Finance Group invites you to cooperation.
-you are responsible and accurate
-you can work without a supervision
-you are from 18 till 70 year old
-you have free time (2-4 hours daily)
-you have basic Internet knowledge and access to a computer with internet connection.(e-mail access)
-you have an idea of bank transfers and money payment systems operations
-you have Western Union/MoneyGram in your city

For this work you don’t need:
-a special education
-possessing some special skills or knowledge
-possessing storehouse, office, special equipment.

The job we offer is related to email. It is an easy job which doesn’t require leaving your main occupation. Contact us, your job is waiting for you!

If you are interested in the job please fill in this form and send it to job@au-fin.com

First name:
Last name:
Country:
City:
Email:
Current occupation:
Some words about you:

Please send your application forms to job@au-fin.com only!

Peter Stevens,
personnel manager
Australian Finance Group

home PCs, government computers, Internet Service Providers, universities, schools, businesses. These “zombies” are then controlled remotely and orchestrated to send an excess of packets to a target server in an attempt to overwhelm and crash it. See McClure, Scambray and Kurtz (2003: 518-523) for descriptions of the varieties of DDoS attacks launched commonly. Even more damaging and sophisticated are DRDoS attacks (distributed refle
service attacks) that incorporate the use of un-compromised computers to attack targets (Patrikakis, Masikos, and Zouraraki, Dec 2004).

The first major distributed denial of service attack came in 2000. Commercial companies such as Yahoo!, AOL, eBay and Amazon have all been targeted by DDoS attacks. In late 1999/00 the etoy DDoS attack bankrupted online toy company eToys (Mark, 2004). See also Berinato (2005) for the story of a foiled DDoS attack against an online gambling site.

Figure App A.5: Anatomy of a distributed denial of service (DDoS) attack

1. Malware compromises computers to provide a botnet

2. Crook “orders” zombies to attack specific target

3. Botnet sends an excess of packets to the target server in an attempt to overwhelm and crash it.

A hacktivist attack, the etoy fund DDoS attack worked differently to that described in Figure App.A.5, by encouraging people to use a denial of service “game”, rather than compromising bots.
In 2005, in response to the threat of distributed denial of service and other malware the Australian Communications and Media Authority (ACMA) developed software in conjunction with five major Internet Service Providers called the *Australian Internet Security Initiative* that identifies ‘zombies’ on the Australian portion of the Internet (Ferguson, 2004; ACMA, 7 November 2005). ACMA then notifies the ISPs who can educate their users, ask them to correct the problem and if they cannot or refuse then disconnects them from the Internet.
Appendix B: Victoria Police Computer Crime Squad Charter

In 2005, the CCS Charter is under review as part of the new Major Crime Management Model.

(a) To conduct proactive investigations and provide force wide reactive investigative computer support, technical assistance, and a computer evidence search, seizure and analysis response for criminal investigations involving information technology;

(b) To provide support to investigation and prosecution processes in the preparation and presentation of computer evidence;

(c) To conduct ongoing research and analysis of issues to identify emerging trends of criminal conduct in the utilisation of technology and to develop strategies to facilitate efficient computer forensic analysis processes and methodologies in accordance with best practice principles;

(d) To actively participate in the review of legislative proposals and to make recommendations for legislative change;

(e) To liaise, develop partnerships and provide assistance to outside agencies, including interstate and international law enforcement agencies and private sector organisations, to foster investigative co-operation and facilitate information exchange;

(f) To actively participate in the Australasian Computer Crime Managers’ Group to facilitate strategic management initiatives and to further develop technical practitioner skills;

(g) To provide risk management and crime prevention advice to external customers and investigative advice to internal customers via seminars, lectures and presentations;

(h) To maintain and further develop liaison initiatives with Internet Service Providers.

(6) Computer Offences

247A. Interpretation

(1) In this Subdivision—

"access", in relation 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;

"data" includes—

(a) information in any form; and

(b) any program or part of a program;

"data held in a computer" includes—

(a) data entered or copied into the computer; and

(b) data held in any removable data storage device for the time being in the computer; and

(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;

"impairment", in relation to electronic communication to or from a computer, includes—
(a) the prevention of any such communication; and
(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;

"modification", in relation to data held in a computer, means—
(a) the alteration or removal of the data; or
(b) an addition to the data;

"serious computer offence" means—
(a) an offence against section 247B, 247C or 247D; or
(b) conduct in another jurisdiction that is an offence in that jurisdiction and that would constitute an offence against section 247B, 247C or 247D if the conduct occurred in Victoria;
"unauthorised computer function" means any of the following—

(a) any unauthorised access to data held in a computer; or

(b) any unauthorised modification of data held in a computer; or

(c) any unauthorised impairment of electronic communication to or from a computer.

(2) In this Subdivision, a reference to access to data, modification of data or impairment of electronic communication is limited to access, modification or impairment caused (whether directly or indirectly) by the execution of a function of a computer.

(3) For the purposes of this Subdivision, access to data, modification of data or impairment of electronic communication by a person—

(a) is unauthorised if the person is not entitled to cause that access, modification or impairment;

(b) is not unauthorised merely because the person has an ulterior purpose for that action.

(4) For the purposes of an offence against this Subdivision, a person causes an unauthorised computer function if the person’s conduct substantially contributes to the unauthorised computer function.
247B. Unauthorised access, modification or impairment with intent 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 and liable to the same maximum penalty as applies to the commission of the serious offence in Victoria.

(2) In this section "serious offence" means—

(a) an offence in Victoria punishable on conviction for a first offence with imprisonment for a term of 5 years or more; or

(b) an offence in any other jurisdiction that would be punishable on conviction for a first offence with imprisonment for a term of 5 years or more if committed in Victoria.

(3) A person may be found guilty of an offence against this section—

(a) even if committing the serious offence is impossible; or

(b) whether the serious offence is to be committed at the time of the unauthorised conduct or at a later time.

(4) It is not an offence to attempt to commit an offence against this section.
247C. Unauthorised modification of data to cause impairment

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 is reckless as to any such impairment—

is guilty of an offence and liable to level 5 imprisonment (10 years maximum).

247D. Unauthorised impairment of electronic communication

A person who—

(a) causes any unauthorised impairment of electronic communication to or from a computer; and

(b) knows that the impairment is unauthorised; and

(c) intends to impair electronic communication to or from the computer or is reckless as to any such impairment—

is guilty of an offence and liable to level 5 imprisonment (10 years maximum).
247E. Possession of data with intent to commit serious computer offence

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

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

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

is guilty of an offence and liable to imprisonment for a term not exceeding 3 years.

(2) In this section, a reference to a person having possession or control of data includes a reference to a person—

(a) having possession of a computer or data storage device that holds or contains the data; and

(b) having possession of a document in which the data is recorded; and

(c) having control of data held in a computer that is in the possession of another person (whether the computer is in Victoria or outside Victoria).

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

(4) It is not an offence to attempt to commit an offence against this section.
247F. Producing, supplying or obtaining data with intent to commit serious computer offence

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

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

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

is guilty of an offence and liable to imprisonment for a term not exceeding 3 years.

(2) In this section, a reference to a person producing, supplying or obtaining data includes a reference to the person—

(a) producing, supplying or obtaining data held in a computer or contained in a data storage device; and

(b) producing, supplying or obtaining a document in which the data is recorded.

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

247G. Unauthorised access to or modification of restricted data

(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 the access or modification—
is guilty of an offence and liable to level 7 imprisonment (2 years maximum).

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

(3) In this section "restricted data" means data held in a computer to which access is restricted by an access control system associated with a function of the computer.

247H. **Unauthorised impairment of data held in computer disk, credit card or other device**

(1) A person who—

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

   (b) knows that the impairment is unauthorised; and

   (c) intends to cause the impairment—
is guilty of an offence and liable to level 7 imprisonment (2 years maximum).

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

(3) For the purposes of this section, impairment of reliability, security or operation of data is unauthorised if the person is not entitled to cause the impairment.
247I. Extra-territorial operation of offences

(1) It is immaterial that some or all of the conduct constituting an offence against this Subdivision occurred outside Victoria, so long as the computer or device used to store data by electronic means affected by the conduct was in Victoria at the time at which the conduct occurred.

(2) It is immaterial that the computer or device used to store data by electronic means affected by some or all of the conduct constituting an offence against this Subdivision was outside Victoria at the time the conduct occurred, so long as that conduct occurred in Victoria.

(7) Sabotage

247J. Interpretation

(1) In this Subdivision—

"property offence" means—

(a) an offence against Subdivision (1) of this Division or Division 4; or

(b) conduct in another jurisdiction that is an offence in that jurisdiction and that would constitute an offence against Subdivision (1) of this Division or Division 4 if the conduct occurred in Victoria;
"public facility" means any of the following (whether publicly or privately owned)—

(a) a government facility, including premises used by government employees in connection with official duties;

(b) a public infrastructure facility, including a facility providing or distributing water, sewerage, energy, fuel, communication or other services to, or for the benefit of, the public;

(c) a public information system, including a system used to generate, send, receive, store or otherwise process electronic communications;

(d) a public transport facility, including a conveyance used to transport people or goods;

(e) a public place, including any premises, land or water open to the public;

"unauthorised computer function" has the same meaning as in Subdivision (6).

(2) In this Subdivision "damage", in relation to 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.

(3) For the purposes of an offence against this Subdivision, a person causes any damage or disruption if the person's conduct substantially contributes to the damage or disruption.
Part I—Offences

Crimes Act 1958
Act No. 6231/1958

247K. Sabotage

A person who—

(a) damages a public facility by committing a property offence or by causing an unauthorised computer function; and

(b) 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 and liable to level 2 imprisonment (25 years maximum).

247L. Threats to 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 and liable to level 4 imprisonment (15 years maximum).
(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, 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.
Victoria Police/Security Industry Partnership Committee

"Partners in Policing"

Purpose of Committee

- The committee will develop and promote a strategic partnership between Victoria Police and Security Industry representatives to assist in achieving a safer and more confident Victoria by:
  - Developing a close working relationship
  - Developing and implementing strategies to improve communication between the partners and the community
  - Actively promoting the community benefits of successful partnerships

Partnership Charter

- Enhance co-operation by:-
  - Promoting the
    - exchange and management of stakeholder knowledge
    - continual advancement of technology towards community safety
    - Partnership throughout the Force, Industry & community
    - Community awareness of safety issues
  - Encouraging communication between stakeholders
  - Co-ordinating efforts between stakeholders to build on community confidence
  - Providing strategic advice to Police, Industry & Community
  - Recognition of "Partners in Policing"
<table>
<thead>
<tr>
<th>Objectives</th>
<th>Strategies</th>
<th>Outcome</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓ Promoting the exchange and management of stakeholder knowledge</td>
<td>Develop a memorandum of understanding</td>
<td>Enhanced information exchange</td>
</tr>
<tr>
<td>✓ continual advancement of technology towards community safety</td>
<td>Identify/encourage best practice common technology</td>
<td>Improved awareness and use of technology amongst stakeholders</td>
</tr>
<tr>
<td>✓ Partnership throughout the Force, Industry &amp; community</td>
<td>Develop/market media and stakeholder communication package</td>
<td>Common theme of working together</td>
</tr>
<tr>
<td>✓ Community awareness of safety issues</td>
<td>Identify initiatives for stakeholder involvement</td>
<td>Improved safety of community</td>
</tr>
<tr>
<td>✓ Encouraging communication between stakeholders</td>
<td>Develop a local communication strategy</td>
<td>Enhance communication</td>
</tr>
<tr>
<td>✓ Understanding and respecting each of the stakeholder roles</td>
<td>Research opportunities for workplace exchange</td>
<td>Enhance culture for exchange of ideas</td>
</tr>
<tr>
<td>✓ Co-ordinating efforts between stakeholders to build on community confidence</td>
<td>Identify roles/communicating roles to stakeholders</td>
<td>Improved working relationship</td>
</tr>
<tr>
<td>✓ Providing strategic advice to Police, Industry &amp; Community</td>
<td>Support the Victoria Police focus on critical crime</td>
<td>Reduction in crime</td>
</tr>
<tr>
<td>✓ Recognition of &quot;Partners in Policing&quot;</td>
<td>Increase community confidence in the Force and the Security Industry</td>
<td>Confident community and work force</td>
</tr>
<tr>
<td>✓ Monitoring issues of interest</td>
<td>Remove bias/barriers at all levels</td>
<td>Reduction in fear of crime</td>
</tr>
<tr>
<td></td>
<td>Eliminate inconsistencies in policy advice provided to stakeholders</td>
<td>Recognised &quot;Peak Committee&quot; proving consistent advice</td>
</tr>
<tr>
<td></td>
<td>Establish regular Local Liaison forums</td>
<td>Enhanced working relationship</td>
</tr>
<tr>
<td></td>
<td>Develop Information Sheet/Logo</td>
<td>Common identification of partnership</td>
</tr>
<tr>
<td></td>
<td>Promote partnerships within community</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Develop a criteria for advancing issues</td>
<td></td>
</tr>
</tbody>
</table>
Victoria Police/Security Industry Partnership Committee (POLSEC)

CODE OF ETHICS

The quality of professional security activity, in the State of Victoria, ultimately depends upon the willingness of security practitioners to observe special standards of conduct and to manifest good faith in professional relationships.

Observance of this Code of Ethics does not supersede, but enhances, the Code of Ethics of the Association the security practitioner is a member of in the State of Victoria.

I. A member shall perform professional duties in accordance with the law.

II. A member shall observe the precepts of truthfulness, honesty and integrity.

III. A member shall be diligent in discharging professional responsibilities.

IV. A member shall ensure he or she is competent in discharging professional responsibilities.

V. A member shall safeguard confidential information and exercise due care to prevent its improper disclosure.

VI. A member shall not maliciously injure the professional reputation or practice of colleagues, clients or employers.

VII. A member shall assist members of the Police Service or any officer of the Crown in carrying out their lawful duties.

VIII. A member will assist members of the public, where and when possible, in the prevention of crime.
NON DISCLOSURE AGREEMENT

I, understand that while performing the tasks and duties assigned to me as a member of the Victoria Police Security Industry Partnership Committee (POLSEC), that I may have access to or become aware of information of a sensitive or confidential nature and that I also understand that I may not be able to distinguish such information as being sensitive or confidential in nature.

Therefore, I HEREBY UNDERTAKE that I shall not discuss or disclose to any person information which has been classified by the Chair, Victoria Police Security Industry Partnership Committee (POLSEC) to be of a sensitive or confidential nature and which has been obtained by me as a result of my association with the Victoria Police Security Industry Partnership Committee (POLSEC).

Further, I HEREBY INDEMNIFY Victoria Police for any loss or damage howsoever caused, and arising directly or indirectly from my disseminating, permitting or suffering the dissemination of such information to any source whatsoever.

I agree that in the event that Victoria Police has reason to suspect me of having disseminated, permitted or suffered the dissemination of any such information, that my membership on the Victoria Police Security Industry Partnership Committee (POLSEC) may be suspended immediately and the subject of an inquiry or investigation. Depending upon such inquiry or investigation, a letter of termination from the Victoria Police Security Industry Partnership Committee (POLSEC) may be forwarded to the body that I represent on the Committee.

SIGNED by me on this day of 2004.
Appendix E: Letters of ethics clearance

6 November 2002

Mr S McKenzie & Dr S James
Department of Criminology

Dear Mr S McKenzie & Dr S James

I am pleased to advise that the Behavioural and Social Sciences Human Ethics Subcommittee approved the following project at its 10/02 meeting:

Policing Electronic Crime in Victoria: Partnerships and Prosecutions
Mr S McKenzie & Dr S James
Dr F Haines
HREC No. 020601

The Project has been approved for the period: 1/11/02 to 31/12/03. It is your responsibility to ensure that all people associated with this particular project are made aware of what has actually been approved.

Research projects are normally approved to 31 December of the year of approval. Projects may be renewed yearly for up to a total of five years upon receipt of a satisfactory annual report. If a project is to continue beyond five years a new application will normally need to be submitted.

Please note that the following conditions apply to your approval. Failure to abide by these conditions may result in suspension or discontinuation of approval and/or disciplinary action.

(a) Limit of Approval: Approval is limited strictly to the research proposal as submitted in your application.

(b) Variation to Project: Any subsequent variations or modifications you wish to make to your project must be notified formally to the Human Ethics Sub-Committee for further consideration and approval. If the Sub-Committee considers that the proposed changes are significant, you may be required to submit a new application for approval of the revised project.

(c) Incidents or adverse affects: Researchers must report immediately to the Sub-Committee anything which might affect the ethical acceptability of the protocol including adverse effects on subjects or unforeseen events that might affect continued ethical acceptability of the project. Failure to do so may result in suspension or cancellation of approval.

(d) Monitoring: Projects are subject to monitoring at any time by the ethics committee.

(e) Annual Report: You must submit an annual report on this project at the end of the year, or, at the conclusion of the project if it continues for less than a year. Requests for annual reports are sent out by the Human Research Ethics Office in November/December of each year. Failure to submit a progress report at the end of the year will mean approval for your project will lapse.

(f) Auditing: All projects may be subject to audit by members of the Sub-Committee.

If you have any further queries on these matters, or require additional information, please do not hesitate to contact me on telephone no. 8344 7507 or e-mail: k.murphy@unimelb.edu.au.

Please quote the HREC registration number and the name of the project in any future correspondence.

On behalf of the Sub-Committee I wish you well in your research.

Yours sincerely,

Kate Murphy
Executive Officer, Human Research Ethics

cc. Chair, DHEAG, Criminology
Dr F Haines

Melbourne Research and Innovation Office
The University of Melbourne Victoria 3010 Australia
Telephone: +61 3 8344 7114 Fax: +61 3 9347 6739
URL http://www.unimelb.edu.au/research
5 February 2004

Dr S James & Mr S McKenzie
Department of Criminology

Dear Dr S James & Mr S McKenzie

Re: Policing Electronic Crime in Victoria: Partnerships and Prosecutions
Dr S James & Mr S McKenzie
Dr F Haines
HREC No. 020601

I am pleased to advise that this project has been approved from 1 January 2004 to 31 December 2004 by the Behavioural and Social Sciences Human Ethics Sub-Committee. Approval may be renewed up to 31 December 2007 subject to the receipt of satisfactory annual reports.

Yours sincerely

Kate Murphy
Executive Officer
Human Research Ethics

cc. Chair, DHEAG, Criminology
17 June 2004

Mr. Shane McKenzie
Department of Criminology
The University of Melbourne
Victoria 3010

Dear Shane

**Policing Electronic Crime in Victoria: Partnerships and Prosecutions**

I have the pleasure to advise you that the Victoria Police Research Coordinating Committee has approved your request to undertake the above research involving Victoria Police.

Please complete and return the accompanying Conditions of Access form at your earliest convenience. Please note additional conditions included within Section 24 of the Conditions of Access document. To speed up the process, you might like to send the signed document by fax (9247 6712).

Please do not hesitate to contact me by phone (9247 6728) or facsimile (9247 6712) if you have any questions you wish to raise.

Yours sincerely,

Joseph Poznanski, PhD
Secretary, Victoria Police Research Coordinating Committee
CONDITIONS OF ACCESS TO POLICE RESOURCES TO CONDUCT RESEARCH

Approval for the researcher to conduct research using Victoria Police resources is dependent on the acceptance of the conditions, where applicable, set out below. The Research Coordinating Committee (RCC) reserves the right to withdraw support for a project at any time during its life due to non-compliance with this agreement, lack of acceptable progress, and inappropriate conduct of the researchers.

Research Project Number: RCC 380

Project Title: Policing electronic crimes in Victoria: Partnerships and Prosecutions

I, SHANE EDWARD H. MCKENZIE, of .................................................. (Full Name)
.................................................. (Residential Address)

HEREBY AGREE AND ACKNOWLEDGE THAT:

Information to which the applicant gains access

1. Only information relevant to the research project will be gathered.

2. Any information gathered will not be used for any purpose, other than that in the agreed project plan.

3. Any changes required to implement the project after the initial approval must have prior written approval of the RCC.

4. Any information relating directly or indirectly to the internal operations, practices or affairs of the Victoria Police to which I may have access as a consequence of this approval, will not be disclosed, divulged or released in any form to any other person, firm, corporation or government authority or department.

Access to police members

5. The involvement of members of Victoria Police Force in the research project will be voluntary.

6. The approval of their supervisor/s to involve these members will be obtained by the RCC.

7. The research proposal must be fully explained to all participants, whose consent will be sought prior to their involvement.

8. Participants will be supplied a plain language statement and sign an informed consent form prior to participating.

Signature: ............................ Date 18/6/14

20190420
9. Participants are free to withdraw from the research at any stage and to withdraw any unprocessed data supplied.

10. Members will not be asked any questions that may contravene Section 127A of the Police Regulation Act 1958 or Section 95 of the Constitution Act 1975

Access to data

11. The provision of information held by the Force may be conditional on the payment of a fee.

Management of data collected or obtained

12. It is the researchers responsibility to ensure security procedures are maintained that will ensure the confidentiality of data collected. This could include for secure storage, removing identifying information from records, and computer holdings held under password protection.

13. Research data resulting from the project must be held for a period of five years unless otherwise specified or agreed by the RCC.

Proof of check

14. Where access to confidential criminal or personnel records is required, the researcher/s must be prepared to undergo any clearance check deemed necessary by the Victoria Police which may include the provision of personal details (eg. full name, previous names, date of birth and residential addresses) and fingerprints.

15. All copies of confidential material (including data in a machine-readable form) will be returned to the Victoria Police Force upon completion of the relevant stage of the project.

Progress reporting

16. The researcher/s will provide the RCC with progress reports at stages of the project deemed appropriate by the RCC

Reporting the results of research

17. Where the views of individual members of Victoria Police (whether sworn or unsworn members) are quoted in the final research report, unless such members have been authorised to comment on behalf of Victoria Police, it must be stated that these views are personal and are not necessarily representative of Victoria Police in general.

18. Where, in the opinion of the Research Coordinating Committee confidential material can be provided to the researcher/s, such material identifying, either directly or indirectly, any section or person involved in the said material will be removed prior to publication.

19. A final draft copy of the research report, or comprehensive extracts of any passages referring either directly or indirectly to the Force, including any findings and or recommendations, must be submitted to the RCC prior to publication. Sufficient time must be given to the Committee to assess the material and provide comment.

20. The RCC reserves the right to have an accurate reflection of its views incorporated into the final report where it is considered that misuse of information, misrepresentation or inaccuracies have occurred. The RCC also reserves the right to provide comment upon any aspect of the project.

21. A complete copy of the final report, must be provided to the RCC for circulation within Victoria Police and possible lodgement in the Victoria Police Central Library

Initial: [Signature] Date: [Date] 2014/02

2
22. Victoria Police has the right to utilise the findings of research projects, but no unpublished information will be released without the permission of the author.

**Intellectual knowledge**

23. When research is undertaken for the purpose of developing programs and electronic programs the researcher shall have ownership intellectual property however, Victoria Police will have access and the option to use the program developed without costs.

**Additional conditions**

24. The following conditions should apply to the conduct of this research project:

1. That the information being disclosed will only be used by for the purposes of the research;
2. That the information to be disclosed will only relate to witnesses, suspects and offenders;
3. That the names of witnesses, suspects and offenders will not be recorded by Mr. McKenzie;
4. That access to relevant information shall be provided on Victoria Police premises, under Victoria Police supervision;
5. That the results of the case analyses will be published in aggregate form to prevent the identification of individuals or individual cases.

**Reporting schedule**

25.

**Approved actions**

26.
14 July 2004

Mr Shane McKenzie
Department of Criminology
University of Melbourne
Parkville
VIC, 3010

Dear Mr McKenzie

Project No: EC/04/14 – Policing Electronic Crime in Victoria: Partnerships and Prosecutions

The Chair of the Committee considered your revised material and has granted full approval, subject to ratification at the meeting on 27 July 2004.

To enable the Committee to fulfil its obligations in relation to monitoring the program, you are asked to provide a report within 12 months or on completion of your project, whichever is earlier. It would also be appreciated if a copy of the research findings could be provided for future reference and/or contact with the researchers by any interested parties.

You must ensure that the Department of Justice Research Ethics Committee is notified immediately of any matter which arises that may affect the nature of the approved project.

Please have Dr James sign the Undertaking attached and return it to me at the above address. Should you have any queries please do not hesitate to contact me on 9651 6974 or Tony.Ward@justice.vic.gov.au.

Yours sincerely

[Signature]

Tony Ward
Secretariat
Justice Research Ethics Committee
UNDERTAKING

Project Title: Policing Electronic Crime in Victoria: Partnerships and Prosecutions

Project No. EC/04/13

I acknowledge that I have read the conditions outlined in the guidelines of the Department of Justice Research Ethics Committee, and undertake to abide by them.

SIGNED: Dr Steve James

DATE: 15/7/04
Appendix F: Letter of support from Victoria Police

Dear Mr. Harmworth,


I write to you on behalf of to the Chief Commissioner, in respect to your letter dated 26 June, 2002 where you seek support of Mr. Shane McKenzie undertaking a PhD thesis on the policing of electronic crime in Victoria.

The area of study proposed by Mr. McKenzie complements work already undertaken by Victoria Police and the Australasian Centre for Policing and it is likely there will be a number of positive outcomes for Victoria Police from this research. The issue of electronic crime poses new challenges and issues for law enforcement throughout Australia and overseas. It is timely that Mr. McKenzie is undertaking this research and I believe law enforcement will benefit from this proposed study. Accordingly, Victoria Police supports this initiative.

The liaison officer for this project is Detective Superintendent Masters who is the Officer in Charge of the Major Fraud Group, and he can be contacted on Telephone 9626 6600. Detective Superintendent Masters has overall responsibility for e-crime issues including the management of the Computer Crime Investigation Squad.

Yours sincerely,

T.C. Thompson
Acting Assistant Commissioner (Crime)

*2-6/8/2002*
Appendix G: Private sector survey

Policing Electronic Crime in Victoria

Participant code: ____________________

Why a survey?
The Department of Justice and Multimedia Victoria have sponsored this independent research conducted by researchers at the University of Melbourne to learn more about how the private sector responds to crime involving information technology and how police can work with the private sector to lessen the impact of these crimes. Victoria Police supports and is participating in the research. The results of this study will be communicated to government, business and law enforcement to inform policy about partnerships between the private sector and law enforcement via the website below.

Who should fill in this questionnaire?
A senior manager or equivalent person at your workplace should complete the survey. If you cannot answer a question, we would appreciate you passing the questionnaire to a senior manager in your workplace who can. Participation in this survey is voluntary, and your completion of the questionnaire is appreciated greatly.

ALL INFORMATION WILL BE TREATED IN THE STRICTEST CONFIDENCE

We intend to protect your anonymity and the confidentiality of your responses to the fullest possible extent, within the limits of the law. Do not write your name or company name on this questionnaire. All information will be stored in compliance with University of Melbourne guidelines. You may withdraw your responses by quoting the above participant code, at any time prior to data analysis.

What do you do?
You can complete the survey online at the website below, or complete the attached questionnaire and return it in the supplied reply paid envelope to:

Policing Electronic Crime Study
Department of Criminology
University of Melbourne
Reply Paid 79619
CARLTON VIC 3053

You could expect the questionnaire to take about 20 minutes to complete.

Follow up Interview
IT security and e-crime investigation practitioners are invited to participate in an interview to expand on this survey and discuss best practice in investigative partnerships with law enforcement. If you or someone you know would like to be interviewed, please complete and sign the accompanying form and return it in the reply paid envelope. Shane McKenzie will then contact you to confirm your availability and arrange a mutually convenient time and location for an interview.

Any questions?
For any queries or concerns about this project, contact the researchers, Shane McKenzie on 8344 9459 or Dr Steve James on 8344 9449. Should you have concerns about the conduct of the project, contact the Executive Officer, Human Research Ethics, The University of Melbourne, on ph: 8344 2073, or fax: 9347 6739.

http://www.criminology.unimelb.edu.au/research/ecrime
**What does electronic crime mean to you (your workplace)?**

Electronic crime (or e-crime) is a term used increasingly by law enforcement, the private sector and government to describe crimes where a computer or other information or communication technology is used as a tool or as a target in the commission of a crime. It includes using these technologies as storage devices for illegal data.

**A1.** Does your workplace use this or another term or definition to describe crime involving information technology?

- [ ] This workplace uses the above term and definition in its documentation
- [ ] No formal definition is used at this workplace
- [ ] This workplace uses another term or definition (please specify)

**A2.** How useful or relevant is the above definition of “electronic crime” for you (your company)? Please explain your answer.

___________________________________________________________

___________________________________________________________

**A3.** What is important about electronic crime to you (your workplace)?

___________________________________________________________

___________________________________________________________

**A4.** Where do you get most of your information about electronic crime?

___________________________________________________________

**A5.** Circle your agreement or disagreement with the following statements:

<table>
<thead>
<tr>
<th>Statement</th>
<th>Agree completely</th>
<th>Agree somewhat</th>
<th>No opinion</th>
<th>Disagree somewhat</th>
<th>Disagree completely</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. Electronic crime is a major problem in Australia</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>b. Electronic crime is a major problem in my industry</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>c. Electronic crime is a major problem in my workplace</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
</tbody>
</table>

**Impact of Electronic crime for your workplace**

**B1.** Below is a list of crimes that are often characterised as “electronic crime”. In the last 12 months, has your company experienced any of the following incidents? (Circle the number of incidents, and if an incident was experienced, indicate the approximate monetary loss suffered)

<table>
<thead>
<tr>
<th>Incident</th>
<th>No. of incidents in last 12 months</th>
<th>AUS$ Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. Theft of telecommunications services</td>
<td>0 1-5 6-10 &gt;10 Don't Know</td>
<td>______</td>
</tr>
<tr>
<td>b. Theft of electronic funds</td>
<td>0 1-5 6-10 &gt;10 Don't Know</td>
<td>______</td>
</tr>
</tbody>
</table>
## No. of incidents in last 12 months

<table>
<thead>
<tr>
<th>Incident Description</th>
<th>No. of Incidents</th>
<th>AUS$ Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>c. Electronic vandalism (eg defaced websites)</td>
<td>0 1-5 6-10 &gt;10</td>
<td>Don't Know</td>
</tr>
<tr>
<td>d. Credit card fraud (including &quot;phishing&quot; scams)</td>
<td>0 1-5 6-10 &gt;10</td>
<td>Don't Know</td>
</tr>
<tr>
<td>e. Advance fee scams (eg, Nigerian email scams)</td>
<td>0 1-5 6-10 &gt;10</td>
<td>Don't Know</td>
</tr>
<tr>
<td>f. Identity theft &amp; fraud (eg counterfeit documents)</td>
<td>0 1-5 6-10 &gt;10</td>
<td>Don't Know</td>
</tr>
<tr>
<td>g. Defamation online</td>
<td>0 1-5 6-10 &gt;10</td>
<td>Don't Know</td>
</tr>
<tr>
<td>h. Unauthorised access to computer</td>
<td>0 1-5 6-10 &gt;10</td>
<td>Don't Know</td>
</tr>
<tr>
<td>i. Dissemination of offensive content (eg child porn, racial hatred)</td>
<td>0 1-5 6-10 &gt;10</td>
<td>Don't Know</td>
</tr>
<tr>
<td>j. Cyber-stalking</td>
<td>0 1-5 6-10 &gt;10</td>
<td>Don't Know</td>
</tr>
<tr>
<td>k. Digital piracy (eg software, music, multimedia)</td>
<td>0 1-5 6-10 &gt;10</td>
<td>Don't Know</td>
</tr>
<tr>
<td>l. Digital extortion (a demand accompanied by a threat)</td>
<td>0 1-5 6-10 &gt;10</td>
<td>Don't Know</td>
</tr>
<tr>
<td>m. Criminal communications</td>
<td>0 1-5 6-10 &gt;10</td>
<td>Don't Know</td>
</tr>
<tr>
<td>n. Illegal online gambling</td>
<td>0 1-5 6-10 &gt;10</td>
<td>Don't Know</td>
</tr>
<tr>
<td>o. Electronic money laundering or tax evasion</td>
<td>0 1-5 6-10 &gt;10</td>
<td>Don't Know</td>
</tr>
<tr>
<td>p. Spam (unsolicited email)</td>
<td>0 1-5 6-10 &gt;10</td>
<td>Don't Know</td>
</tr>
<tr>
<td>q. Virus/worm/trojan infection (actual infection)</td>
<td>0 1-5 6-10 &gt;10</td>
<td>Don't Know</td>
</tr>
<tr>
<td>r. Illegal interception of digital information (eg company email)</td>
<td>0 1-5 6-10 &gt;10</td>
<td>Don't Know</td>
</tr>
<tr>
<td>s. Denial of service attack</td>
<td>0 1-5 6-10 &gt;10</td>
<td>Don't Know</td>
</tr>
<tr>
<td>t. Theft of proprietary / confidential information</td>
<td>0 1-5 6-10 &gt;10</td>
<td>Don't Know</td>
</tr>
<tr>
<td>u. Online Auction fraud</td>
<td>0 1-5 6-10 &gt;10</td>
<td>Don't Know</td>
</tr>
</tbody>
</table>

**B2.** If incidents of electronic crime were experienced at your workplace in the last 12 months, describe any non-monetary costs or impacts incurred:

___________________________________________________________
___________________________________________________________
___________________________________________________________

*None of the above types of incident ❑ If none at all, Skip to C1.*
**Responses to electronic crime at this workplace**

**C1.** Who in your workplace (which positions or roles) are responsible for responding to e-crime?

---

**C2.** What security technologies does your workplace use to protect your networks?

<table>
<thead>
<tr>
<th>Technology</th>
<th>Yes</th>
<th>No</th>
<th>Do Not Know</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. Physical security</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>b. Anti-virus software</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>c. Digital ID certificates</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>d. Encrypted logins/sessions</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>e. Encrypted files</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>f. Intrusion Detection Systems</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>g. File Integrity Assessment tools</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>h. Firewalls</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>i. Biometrics</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>j. Smart cards, 1 time tokens</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>k. Reusable Passwords</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>l. Access control</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>m. Other _______________________</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
</tbody>
</table>

**C3.** Does your workplace have an incident response procedure in place?

- [ ] Yes
- [ ] No
- [ ] Do not know

**C4.** If this workplace experienced an incident in the last 12 months, which of the following responses were taken? (Tick all that apply)

- [ ] Sought advice from external consultant
- [ ] Sought advice from police
- [ ] Followed incident response or other plan
- [ ] Internal investigation
- [ ] Investigation was outsourced or contracted in (not to police)
- [ ] Reported incident to police
- [ ] Reported incident to other agency (eg ASIC, Dept of Finance)
- [ ] Reported incident to AusCERT or similar
- [ ] Improved training and education
- [ ] Reviewed security policies
- [ ] Installed new security technologies
- [ ] Undertook mitigation / recovery steps
- [ ] Other (please specify) ___________________________
**C5.** What do you (this company) consider *successful* resolutions to electronic-crime involving this company?

**C6.** What do you (this company) consider *unsuccessful* resolutions to electronic-crime involving this company?

**C7.** If electronic crime was experienced in the last 12 months, do you think it was resolved successfully?  
- Yes  
- No  
- Do not know

**C8.** In this workplace, how important are the following factors in the decision to report or not report an incident to police?

<table>
<thead>
<tr>
<th>Factor</th>
<th>not at all important</th>
<th>slightly important</th>
<th>moderately important</th>
<th>very important</th>
<th>extremely important</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. Measurable loss</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>b. Past experience with law enforcement</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>c. Seriousness of incident</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>d. Advice from IT staff</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>e. Shareholders views</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>f. Company policy</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>g. Inability to measure loss</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>h. Advice from security consultant</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>i. Suspect worked for company</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>j. Mandatory reporting requirement</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>k. Potential negative media reporting</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>l. Potential positive media reporting</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>m. Advice from police (ie, prior to official complaint)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>n. Partnership or alliance with police</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>o. Other ________________</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Priorities given to different types of electronic crime

**D1.** The police give some crimes higher priority than others. We are interested in finding out what you (your company) think these priorities are CURRENTLY. Please tick (✔) only ONE box next to each item.

<table>
<thead>
<tr>
<th>Crime</th>
<th>Very low priority</th>
<th>Low priority</th>
<th>Some priority</th>
<th>High priority</th>
<th>Very high priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>Theft of telecommunications services (aka “phreaking”)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Theft of electronic funds</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Electronic vandalism (eg defaced websites)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Credit card fraud (including “phishing” scams)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Advance fee scams (eg, Nigerian email scams)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identity theft &amp; fraud (eg counterfeit documents)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Defamation online</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unauthorised access to computer</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dissemination of offensive content (eg child porn, racial hatred)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cyber-stalking</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Digital piracy (eg software, music, multimedia)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Digital extortion (a demand accompanied by a threat)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Criminal communications</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Illegal online gambling</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Electronic money laundering or tax evasion</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Spam (unsolicited email)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Authoring computer viruses</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Illegal interception of digital information</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Denial of service attacks</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Theft of proprietary / confidential information</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Online Auction fraud</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**D2.** In the previous question, we asked for your views on the priorities police give currently to different types of e-crime. You may or may not agree with these priorities. Next, we are interested in finding out what you (your company) think police priorities SHOULD BE. Please tick (✔) only ONE box next to each item.

<table>
<thead>
<tr>
<th>Item</th>
<th>very low priority</th>
<th>low priority</th>
<th>some priority</th>
<th>high priority</th>
<th>very high priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. Theft of telecommunications services (aka “phreaking”)</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>b. Theft of electronic funds</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>c. Electronic vandalism (eg defaced websites)</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>d. Credit card fraud (including “phishing” scams)</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>e. Advance fee scams (eg, Nigerian email scams)</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>f. Identity theft &amp; fraud (eg counterfeit documents)</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>g. Defamation online</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>h. Unauthorised access to computer</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>i. Dissemination of offensive content (eg child porn, racial hatred)</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>j. Cyber-stalking</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>k. Digital piracy (eg software, music, multimedia)</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>l. Digital extortion (a demand accompanied by a threat)</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>m. Criminal communications</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>n. Illegal online gambling</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>o. Electronic money laundering or tax evasion</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>p. Spam (unsolicited email)</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>q. Authoring computer viruses</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>r. Illegal interception of digital information</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>s. Denial of service attacks</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>t. Theft of proprietary / confidential information</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>u. Online Auction fraud</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Partnerships and strategic alliances between law enforcement and the private sector have been suggested as important to tackling electronic crime successfully. This section explores issues about public-private partnerships for policing e-crime. In this section, “private police” refers to anyone who conducts investigations or prosecutions for your company, whether internal, contracted or outsourced staff.

**E1.** With which law enforcement agencies do you (your company) interact in relation to e-crime?

---

**E2.** In the past 12 months, how many times have you had formal contact with the police in relation to e-crime? (Please exclude purely social contact)

---

**E3.** What was the purpose of this contact? (Tick any that apply)

- Report a crime, police to investigate
- Report a crime, police and workplace to investigate jointly
- Report a crime, workplace to investigate
- Seeking advice from police
- Request from police for information or assistance with investigation
- Information session (eg Neighbourhood Watch, conference)
- Training course
- Other (please specify) _____________________

---

**E4.** If you worked in partnership with police in the past 12 months, what did you achieve through partnership that you could not have achieved without them?

---

**E5.** Successful partnerships are based upon *collaborative advantage*. What advantages for you (your workplace) would you expect from working with law enforcement to combat electronic crime?

---

**E6.** What *constraints*, if any, prevent you (your workplace) from collaborating with police to combat electronic crime?

---
E7. Circle your agreement or disagreement with the following statements about responding to electronic crime:

a. partnerships with police are necessary to combat e-crime effectively
   1 2 3 4 5

b. private police should have greater access to police intelligence and information
   1 2 3 4 5

c. private police need greater powers to investigate e-crime (eg, should be able to apply for warrants to conduct searches)
   1 2 3 4 5

d. this workplace should prepare a brief of evidence before reporting crime
   1 2 3 4 5

e. this workplace should retain computer records specifically in case of future e-crime
   1 2 3 4 5

f. private police meet the needs of this workplace
   1 2 3 4 5

g. public police meet the needs of this workplace
   1 2 3 4 5

h. police are only interested in prosecution
   1 2 3 4 5

i. private police are only interested in their clients
   1 2 3 4 5

j. joint investigations by public and private police need to be regulated by new legislation
   1 2 3 4 5

k. partnerships with police should be formalised (eg, codes of conduct, contracts or laws)
   1 2 3 4 5

l. effective partnerships need regular meetings
   1 2 3 4 5

m. partnerships should extend beyond a particular incident (ie, be long-term)
   1 2 3 4 5

n. partnerships will encourage corruption
   1 2 3 4 5

E8. What do police not understand about your workplace or industry, which they should when policing e-crime in your industry?

E9. How can law enforcement agencies work better with the private sector to police e-crime?

E10. In terms of e-crime, what would working with private police offer this workplace that public police cannot offer?
**E11.** In terms of e-crime, what would working with police offer this workplace that private police cannot offer?

**E12.** Think about the most serious incident of electronic crime experienced at your workplace in the last 12 months. The resolution of this incident may or may not have involved working with the police. Please describe the incident and its resolution in as much detail as possible. (Do not include any identifying information, such as names of individuals or companies).

___________________________________________________________
___________________________________________________________
___________________________________________________________
___________________________________________________________
___________________________________________________________
___________________________________________________________
___________________________________________________________
___________________________________________________________

**F1.** Please tick (✔) the industry sector that best describes your workplace:

- Accommodation, Cafes & Restaurants
- Agriculture, Forestry & Fishing
- Communication Services
- Construction
- Cultural and Recreational Services
- Education
- Electricity, Gas and Water Supply
- Finance & Insurance
- Government Administration and Defense
- Health and Community Services
- Manufacturing
- Mining
- Personal and Other Services
- Property and Business Services
- Retail Trade
- Transport and Storage
- Wholesale Trade

This section asks about characteristics of your workplace to permit analysis of your previous responses.

---

469
F2. What is the main activity undertaken at this workplace? That is, what does this workplace make or do?
___________________________________________________________

F3. How many employees work at this workplace? (Write in number) ________

F4. What percentage of employees use computers to do their work? (Tick one)

- None
- 1-5%
- 6-10%
- 11-25%
- 26-50%
- 51-75%
- 76-100%
- Don’t know

F5. What percentage of employees have Internet access at this workplace? (Tick one)

- None
- 1-5%
- 6-10%
- 11-25%
- 26-50%
- 51-75%
- 76-100%
- Don’t know

F6. Does your workplace have any e-commerce activities underway? Please specify.
___________________________________________________________
___________________________________________________________

F7. What is the approximate gross revenue of this company per annum? AUS$__________

About the person completing this questionnaire

This section asks about your background to permit analysis of your previous responses. Tick (✔) all appropriate boxes. Please answer all questions.

G1. What sex are you?
- Male
- Female

G2. How old are you?
- 18-20
- 21-24
- 25-29
- 30-34
- 35-44
- 45-54
- 55-64
- 65-74
- 75 or older

G3. What is the highest level of education you have completed?
- Some high school
- Completed Year 12
- Diploma / Trade certificate or equivalent
- Degree or higher

G4. Have you ever worked for a law enforcement agency?
- Yes
- No

If yes, in what capacity: _________________________________
G5. Have you completed any specialist IT training? (Please list any courses and accreditation you have attempted or completed)

G6. What is your position or role in your workplace?

G7. Do you have any additional comments about any aspect of this survey?

THANK YOU FOR TAKING PART IN THIS IMPORTANT STUDY

The study results will be made available at the study website:
http://www.criminology.unimelb.edu.au/research/ecrime

Please place your completed questionnaire in the enclosed reply paid envelope and post to:

Policing Electronic Crime Study
Department of Criminology
University of Melbourne
Reply Paid 79619
CARLTON VIC 3053

For emergency police attendance call 000 (police, fire or ambulance).

Advice and guidance on matters relating to fraudulent activity and electronic crime is available through a Victoria Police reporting service, without the need to make a formal complaint:

Major Fraud Investigation Division
Victoria Police
549 St Kilda Rd
Melbourne VIC 3004
Tel: (03) 9526 6666
Fax: (03) 9526 6614

Advice and guidance about electronic commerce is available from Multimedia Victoria:

Multimedia Victoria
Level 10, 55 Collins Street,
Melbourne VIC 3000
Email: queries@mmv.vic.gov.au
Web: www.mmv.vic.gov.au
Appendix H: Recruitment / plain language statement for non-police interviewees

Policing Electronic Crime in Victoria: Partnerships and Prosecutions

Explanation of Study and the Interview Process

You are invited to participate in the above research project, conducted by Mr Shane McKenzie (PhD candidate; 8344 9459) and Dr Steve James (supervisor; 8344 9449) of the Department of Criminology at the University of Melbourne. This project is part of Mr McKenzie’s PhD thesis. The Department of Justice and Multimedia Victoria have sponsored this independent research to learn more about how the private sector responds to crime involving information technology and how police can work with the private sector to lessen the impact of these crimes.

This study aims to examine the policing of electronic crimes in Victoria. In particular the study examines issues of under-reporting to law enforcement, factors affecting the success of investigations and prosecutions, investigative partnerships with law enforcement, and the impact of new computer offences legislation.

Should you agree to participate, you will take part in a brief interview of about 45 minutes discussing the issue of investigative partnerships with law enforcement to police electronic crime. With your permission, the interview will be audiotaped to make an accurate record from what you say. You may request a copy of the transcript and verify that the information is recorded correctly. The recording will be erased following transcription.

We intend to protect your anonymity and the confidentiality of your responses to the fullest possible extent, within the limits of the law. You may participate anonymously or you may elect to be named in the publications arising from this research. Unless you elect to be identified, you will be referred to by a pseudonym and we will remove any personal information that might allow someone to guess your identity or the name of your company. Only the researchers will be able to link you to your responses.

A summary of the research findings will be available to you from the research website at http://www.crim.unimelb.edu.au/research/ecrime.
Should you wish to withdraw at any stage or withdraw any unprocessed data you have supplied, you are free to do so without prejudice by quoting your participant code to the researchers.

You may contact the researcher, Shane McKenzie on 8344 9459 or Dr Steve James on 8344 9449 with any queries or concerns you may have about the project. Should you have any concerns about the conduct of the project, please do not hesitate to contact the Executive Officer, Human Research Ethics, The University of Melbourne, on ph: 8344 2073, or fax: 9347 6739, or the Secretary of the Research Ethics Committee of the Department of Justice on ph: 9651 6970, fax 9651 6955, or by writing to the Research Ethics Committee, Department of Justice Victoria, GPO Box 4356QQ, Melbourne Victoria 3001.

Thank you for your consideration,

Yours faithfully,

Shane McKenzie
PhD candidate
Department of Criminology
Appendix I: Recruitment / plain language statement for police interviewees

Invitation to participate in the study:
_Policing Electronic Crime in Victoria: Partnerships and Prosecutions_

You are invited to participate in the above research project, conducted by Mr Shane McKenzie (PhD candidate; 8344 9459 or 0424 640 249) and Dr Steve James (supervisor; 8344 9449) of the Department of Criminology at the University of Melbourne. Victoria Police authorises you to participate in this research, which is endorsed by the Chief Commissioner of Police and the Research Coordinating Committee.

This study aims to examine the policing of electronic crimes in Victoria. In particular the study examines issues of under-reporting, factors affecting the success of investigations and prosecutions, partnerships with the private sector, and the impact of new computer offences legislation. This project is part of Mr McKenzie’s PhD thesis, and is supported by Victoria Police, the Department of Justice and Multimedia Victoria.

Should you agree to participate, you will take part in a brief, confidential interview of about 60 minutes. With your permission, the interview will be audiotaped digitally to make an accurate record from what we discuss. The recording will be encrypted and then destroyed securely following transcription. You may request a copy of the transcript and verify that the information is recorded correctly.

We intend to protect your anonymity and the confidentiality of your responses to the fullest possible extent, within the limits of the law. Only the researchers will be able to link you to your responses. Your consent form, name and contact details will be kept securely and separate from any data that you supply, in a locked filing cabinet or encrypted, password-protected computer files. In any publications arising from this research, you will be referred to by a pseudonym and we will remove any personal information that might allow someone to guess your identity.

A summary of the research findings will be available to you from the research website at [http://www.crim.unimelb.edu.au/research/ecrime](http://www.crim.unimelb.edu.au/research/ecrime).

Should you wish to withdraw at any stage or withdraw any unprocessed data you have supplied, you are free to do so without prejudice. Your decision will have no effect on your employment. Victoria Police requires that you are reminded that Section 127A of the _Police Regulation Act 1958_, 'Unauthorised disclosure of information and documents' states:
(1) Any member of the police force who publishes or communicates, except to
some person to whom he is authorised to publish or communicate it, any fact
or document which comes to his knowledge or into his possession by virtue
of this office and which it is his duty not to disclose shall be guilty of an
offence against this Act.

and that Section 95 of the Constitution Act 1975 (Vic) provides that officers in
the public service must not:

a) publicly comment upon the administration of any department of the
State of Victoria.
b) use except in or for the discharge of this official duties, any information
gained by or conveyed to him through connection with the public
service; or
c) directly or indirectly use or attempt to use any influence with respect to
the remuneration or position of himself or of any person in the public
service.

Victoria Police authorises you to speak to the researchers about the specific
questions they will ask. You may not be authorised to comment on unrelated
matters.

If you would like to participate in this study, please complete the
accompanying reply slip and return it in the reply paid envelope provided.
Shane McKenzie will then contact you to arrange a mutually convenient time
and location for the interview. Shane is also under taking data analysis of
closed e-crime cases at Major Fraud Investigation Division and you may make
arrangements with him in person.

Should you have any concerns or complaints about the manner in which this
research has been conducted, please do not hesitate to contact:

The Secretary to the Research Coordinating Committee or The Executive Officer
Research and Development Human Research Ethics
Victoria Police Centre University of Melbourne VIC 3010
637 Flinders Street, Melbourne 3005 Tel: 8344 2073
Tel: 9247 6732 Fax: 9347 6712 Fax: 9347 6739

If any concerns about the conduct of the research remain unresolved, you
may contact the Secretary of the Ethics Committee of the Department of
Justice, which has approved the ethical aspects of this study.

The Secretary can be contacted at telephone 9651 6970; fax 9651 6955, or by writing to the
Research Ethics Committee, Department of Justice Victoria, GPO Box 4356QQ,
Melbourne Victoria 3001.

Thank you for your consideration,
Yours faithfully,
Shane McKenzie
Appendix J: Consent form for non-police interviewees

INFORMED CONSENT FORM FOR RESEARCH PARTICIPANTS

Participant Code:

I, _______________________, consent to participate in the research project entitled, Policing Electronic Crime in Victoria: Partnerships and Prosecutions, conducted by Shane McKenzie and supervised by Dr Steve James, from the Department of Criminology at the University of Melbourne. I consent to the audiotaping of the interview to ensure that the researchers make an accurate record of what I say.

My agreement is based on the understanding that: (Tick where appropriate)

- I have read and understand the general purpose, methods and demands of the study as explained in the letter of invitation and my consent to participate is given freely;
- The recording will be erased following transcription to maintain my anonymity. A copy of the transcript will be made available to me upon request for verification of its accuracy.
- The project is for the purpose of research;
- Details that might identify me or my company will be removed from any publication of results of the study and I will only be identified by a pseudonym;
- I am free to withdraw from the project at any time without explanation or prejudice and withdraw any unprocessed data supplied previously by quoting my participant code number to the researchers;
- the confidentiality of the information I provide will be safeguarded subject to any legal requirements;
- I am over 18 years of age.

Signed by the participant: ________________________________ date __________

Signed by the researcher: _______________________________ date __________

You may contact the researcher, Shane McKenzie on 8344 9459 or Dr Steve James on 8344 9449 with regard to any queries or concerns you may have with regard to the project. Should you have any concerns about the conduct of the project, you are welcome to contact the Executive Officer, Human Research Ethics, The University of Melbourne, on ph: 8344 2073, or fax: 9347 6739 or the Secretary of the Research Ethics Committee of the Department of Justice on ph: 9651 6970, fax 9651 6955, or by writing to the Research Ethics Committee, Department of Justice Victoria, GPO Box 4356QQ, Melbourne Victoria 3001.
Appendix K: Consent form for police interviewees

INFORMED CONSENT FORM FOR RESEARCH PARTICIPANTS FROM VICTORIA POLICE

I, _________________________, agree to participate in the research project entitled:
(Name of participant)

Policing Electronic Crime in Victoria: Partnerships and Prosecutions

conducted by Shane McKenzie from the Department of Criminology at the University of Melbourne. The project is supervised by Dr Steve James.

Shane has discussed this research with me. I have had the opportunity to ask questions about this research and I have received answers that are satisfactory to me. I have read and kept a copy of the Information sheet and understand the general purpose, risks and methods of this research.

My agreement is based on the understanding that:
1. I am aware of what I am expected to do.
2. I have read the participant information sheet and understand the general purpose, methods and demands of the study. All my questions have been answered and my consent to participate is given freely.
3. I consent to the audiotaping of the interview to ensure that the researchers make an accurate record of what I say.
4. The recording will be destroyed following transcription to maintain my anonymity. A copy of the transcript will be made available to me upon request for verification of its accuracy.
5. I have been informed that the confidentiality of the information I provide will be safeguarded subject to any legal requirements.
6. I understand that the project is for the purpose of research and may not be of direct benefit to me.
7. I can withdraw from the study at any time without prejudicing me and withdraw any unprocessed data supplied previously.
8. I can obtain overall results of the study.
9. I consent to the publication of results from this study provided details that might identify me are removed.

Signed by the participant: ____________________________ date__________

Signed by the researcher: ____________________________ date__________

You may contact the researcher, Shane McKenzie on 8344 9459 or Dr Steve James on 8344 9449 with regard to any queries or concerns you may have with regard to your participation in the project. Should you have any queries concerning the way this research is conducted please contact the Secretary to the Research Coordinating Committee, Victoria Police 637 Flinders Street, Melbourne 3005 Tel: 9247 6732.
Appendix L: Schedule for interviews of non-police personnel

Policing Electronic Crime in Victoria: Partnerships and Prosecutions
Semi-Structured Schedule for Private Sector Interviews

Respondent Code: _______ Bring respondent’s survey if completed.
Print a copy for each respondent, to record demographics and make notes during interview.

Explanation of Study and the Interview Process

This research aims to examine public and private policing of electronic crime in Victoria, with particular focus upon the issues of achieving successful investigative and prosecution partnerships. The Department of Justice and Multimedia Victoria have sponsored this independent research to learn more about how the private sector responds to crime involving information technology and how police can work with the private sector to lessen the impact of these crimes. Victoria Police supports and is participating in the research.

Throughout this interview, I would like to discuss with you theories about partnership policing and get your views from a private sector perspective, on how well they explain and would assist policing of electronic crime. Your views can then be fed back into the research about e-crime to improve the theory and practice. This process is known as realistic evaluation.

The results of this study will be communicated to business and law enforcement to inform policy about partnerships between the private sector and law enforcement.

To assist me in making an accurate record of what you say, do you agree to me taping the interview? The tapes will be destroyed once transcribed and you will not be named in any publication relating to this research. You may request a copy of the interview transcript, if you wish to check its accuracy.

Throughout the interview, if you wish to add any comments or ask any questions, please do so. You may stop the interview at any time.

Have respondent read Plain Language statement and sign Consent Form, if proceeding to participate. Copy to participant. Test tape recorder. Provide opportunity for respondent to ask questions

About the respondent and their workplace

(If respondent returned survey, check responses on it & skip to For all:). Before we begin, I’d like to get some demographic information from you to assist with analysis of our interview.

Record Sex of Respondent: ☐ Male ☐ Female
Record approx age of respondent: ☐ 18-20 ☐ 21-24 ☐ 25-29 ☐ 30-34 ☐ 35-44 ☐ 45-54 ☐ 55-64 ☐ 65-74 ☐ 75 or older

What is your role (or job title) in this organisation?
☐ IT security provider
☐ performs e-crime investigations (If either, ask all asterisked questions)
How many years have you been in your present position?

What is the highest level of education you have completed?
- Some high school
- Diploma / Trade certificate or equivalent
- Completed Year 12
- Degree or higher

Do you have any special qualifications or training in relation to investigation of e-crime?
(probe: for example CSSP (Cisco Certified Security Professional), higher degrees, internal company courses etc?)

Have you ever been a member of law enforcement? (If yes, record details)

Record industry sector:
- Accommodation
- Cafes & Restaurants
- Agriculture, Forestry & Fishing
- Communication Services
- Construction
- Cultural and Recreational Services
- Education
- Electricity, Gas and Water Supply
- Finance & Insurance
- Government Administration and Defense
- Health and Community Services
- Manufacturing
- Mining
- Personal and Other Services
- Property and Business Services
- Retail Trade
- Transport and Storage
- Wholesale Trade

What is the main activity undertaken at this workplace? That is, what does this workplace make or do?

How many employees work at your workplace? (Write in number)______

What percentage of employees use computers to do their work? (Tick one)
- None
- 1-5%
- 6-10%
- 11-25%
- 26-50%
- 51-75%
- 76-100%
- Don't know

What percentage of employees have Internet access at this workplace? (Tick one)
- None
- 1-5%
- 6-10%
- 11-25%
- 26-50%
- 51-75%
- 76-100%
- Don't know

Does your workplace have any e-commerce activities underway? Please specify.

For all: What are your usual day-to-day activities?
(probes: Do you investigate cases? Do you prosecute cases?)
For all: What type of work (or cases) do you do most often?

Understandings of “Electronic Crime”

“Electronic crime” is a rather new term. The next questions are about your understanding of these types of crime.

Provide respondent with the definition of e-crime to guide remainder of interview: “Electronic crimes are where a computer is used as a tool or as a target in the commission of the crime. It includes using a computer as a storage device for illegal data” (Etter, Dec 2002).

What does the term “electronic crime” to mean to you (your company)? (probe: what is important about it?)

✶ In terms of doing your job, how useful or relevant is this definition of “electronic crime” for you? (probe: increasing forms of crime; Explore operationalisation and scope of responsibilities & what is investigated)

Responses to e-crime

The next few questions look at your opinions and experiences about how people respond to electronic crime.

Handout of “Priority of e-crime types” question, if not completed as part of survey questionnaire

E-crime is a global problem, and offenders can be located on the other side of the globe or locally. What priority do you give to interstate or international incidents in comparison to local offences? What priority should be given?

(Non)-reporting of e-crime

Detecting e-crime and under-reporting are often mentioned as major problems in relation to e-crime.

What local factors do you think contribute to under-reporting of e-crime in Victoria? In your industry? In your workplace? For your clients?

What factors contribute to reporting of e-crime in Victoria? In your industry? In your company? How can reporting be encouraged?

If a relevant case came before you, would you choose to take civil action or to have police charge a person with a criminal offence?

✶ What charges do you usually prefer? Why is that?

The recent Parliamentary Inquiry into Fraud and E-Commerce recommended the introduction of a new Victorian Fraud Information Reporting Centre
(VFIRC). Your thoughts? In what circumstances would your company report e-crime incidents to it?

One private sector investigation firm reports some incidents to police in the form of letters indicating that they do not wish police involvement. Their purpose of doing so is to make sure incidents are included in police statistics without influencing their own investigations. Would your company undertake this type of reporting?

★ What’s different now about how electronic crime is investigated from the past?

## Factors affecting the outcome of e-crime cases

Part of my earlier work on this project has been to examine police and prosecution documents relating to closed electronic crime cases, to find common characteristics of those cases, and what characteristics might have led to successful or unsuccessful outcomes. What I’d like to do next is ask for your opinions about the factors affecting the outcomes of e-crime investigations from the private sector perspective.

### Outcomes
What outcomes do you consider “successful” outcomes for electronic crime cases?

Can a case be successful if it is not prosecuted?

What outcomes do you consider “unsuccessful” outcomes for electronic crime cases?

Thinking from the police point of view, what do you think they consider “successful” outcomes?

Again, from the police point of view, what do you think they consider “unsuccessful” outcomes?

### Factors influencing outcome
This is a list of factors identified from the documentary analysis as contributing to the success or failure of an investigation or prosecution. I’ll go through the list with you. Do you agree with the items on the list? Is there any item on this list that you would dispute or remove from the list? If yes, why would you remove that?

| Handout of factors derived from documentary analysis |

Are there any items you would add to the list? If yes, ‘Why would you include that?’
Using the scale next to each item, how important would you rate these factors as determining whether a case is *investigated* successfully?

Record answers (Number from 1 to 5):

___ Factor 1  ___ Factor 2  ___ Factor 3 etc

___ Any factors provided by interviewee

You rated [insert factor(s)] as most important to an investigation. Why is that?

Using the scale next to each item, how important would you rate these factors as determining whether a case is *prosecuted* successfully?

Record answers (Number from 1 to 5):

___ Factor 1  ___ Factor 2  ___ Factor 3 etc

___ Any factors provided by interviewee

You rated [insert factor(s)] as most important to a prosecution. Why was that?

**Case Study - Personal Experiences of E-Crime Policing**

Next, I would like to discuss some e-crime cases you have experienced. You may have either been involved in an investigation in some manner, or undertaken the investigation yourself. Remember, no person or company involved in any case will be identified in any publication arising from this research.

Could you tell me about your own experiences with electronic crimes cases?

Probes: Types of cases Number of cases Decision making

Tell me about a case you were involved in that had a successful outcome, which for you *exemplifies best practice*. (This may or may not involve the police). [Probes: Detection or report, initial assessment, investigation, prosecution or other outcome – might be civil or criminal case]

The earlier research was restricted to closed police cases. This is only half the picture, when it comes to investigated cases, some of which remain unsolved or open for various reasons. Without identifying these cases or any people involved, I would like to discuss factors involved in “unsuccessful” e-crime cases.

Tell me about a case you were involved in that did *not* have a successful outcome. (Explore the factors believed to have led to the unsuccessful outcome).
Ok, let’s move on to the main focus of this research – interactions and alliances between police (or other law enforcement agencies) and the private sectors. One of the aims of the research is to catalogue the various organisational means by which the private sector interacts with police in relation to e-crime.

With whom from law enforcement does your company or you in particular, interact in relation to e-crime? (General descriptions are fine)

In the past 12 months, how many times have you had contact with the police in relation to e-crime?

In what ways do police and your company interact in relation to e-crime? How often? What are the strategic aims of this interaction?


**Models of Interaction**

| Handout of Sarre and Prenzler's models of interaction |

These are descriptions proposed by two Australian researchers, Rick Sarre and Tim Prenzler. In your experience of e-crime cases, which of the following best describe the type of interaction you have with police investigators?

They have proposed the establishment of *standard procedures for interaction between the sectors*? Your thoughts? What should be standardised?

**Partnerships or Strategic Alliances with Police**

Now I would like to explore your thoughts on the issue of forming *best practice* strategic alliances or “partnerships” between the private sectors and police to police e-crime.

What does “working in partnership with” mean to you? (probe: what characteristics define “working in partnership” for you? information sharing, consultation on decisions, sharing control?)

With whom from the private sector should law enforcement be working to *investigate e-crime*? (Probe: What can your company offer law enforcement?)

With whom from the private sector should law enforcement be working to *prosecute e-crime*? 
**Probe - Industry sectors**

- Accommodation
- Cafes & Restaurants
- Agriculture, Forestry & Fishing
- Communication Services
- Construction
- Cultural and Recreational Services
- Education
- Electricity, Gas and Water Supply
- Finance & Insurance
- Government Administration and Defense
- Health and Community Services
- Manufacturing
- Mining
- Personal and Other Services
- Property and Business Services
- Retail Trade
- Transport and Storage
- Wholesale Trade

With whom should law enforcement NOT form partnerships to fight electronic crime? (probe: Hackers?)

Can you describe any partnerships between Victoria Police and the private sector for fighting e-crime? (alternative: Who wants to partner with Victoria Police?)

Do you have any specific concerns about the partnership of police with the private IT security industry?

**Format of strategic alliances or partnerships**

How can law enforcement agencies work better with the private sector to police e-crime?

There are many different ways in which police could work with the private sector to investigate e-crime. Which activities do you consider *most important* to pursue?

- Discussion forums (Face to face, Email?)
- Memoranda of Understanding
- Joint investigations
- Joint Taskforces
- Vendor-supplier relationships
- R&D projects
- Infrastructure projects
- Neighbourhood Watch style mtgs
- Crime Stoppers style hotlines
- Something else?

“Real-time assistance” has been highlighted as a major problem of interacting with the private sector. How can real time assistance be achieved?

Provide handout of additional partnership topics to discuss. Not all of these may be covered, depending upon the respondent.

**Regulating strategic alliances and partnerships**

Referring back to the different models of interaction between police and private security, Sarre and Prenzler further argue that cooperation between law enforcement and the private police needs to be limited and closely regulated.

Do you believe new laws are needed to regulate interactions between police and private police *when they investigate e-crime jointly*? What is needed?
What forms of regulation exist currently to guide strategic alliances and public-private partnerships? [Probe: Eg, Police Regulations Act and Constitution Act regulate police behaviour]

Should the private sector be given additional police-like powers to investigate e-crime? If yes, what sort, and how should they be regulated? If no, why not?

**Model Computer Crime Offences**

Finally, I’d like to discuss the influence of law for the private sector, especially the model computer offences which were introduced in Victoria on 6 May 2003 by the Crimes (Property Damage and Computer Offences) Act 2003 (Vic)

Offer copy of the new offences to respondent as mnemonic device.

If a relevant case came before you, would you choose to take civil action or to have police charge a person with one of these offences? Why is that?

In your opinion, what is useful about this model legislation?

In your opinion, are there any problems with the model computer offences?

What legislative changes would you like to see made in relation to computer offences? (Probe: What are your reasons for such changes?)

**The future – Suggestions to Improve E-Crime Investigation**

We’ve discussed a lot of different issues about investigating and prosecuting e-crime. To finish, are there any (further) suggestions you would like to make, which might help reduce the impact and incidence of e-crime?

**Debrief Respondent**

Thank you for taking part in the study. As explained before the interview I will be making the results from the study available on the research website: www.crim.unimelb.edu.au/research/ecrime.

You may request a copy of the interview transcript, if you wish to check its accuracy.

Requests copy of transcript:  □ Yes  □ No

Provide opportunity for respondent to ask questions
Appendix M: Schedule for interviews of police

Policing Electronic Crime in Victoria: Partnerships and Prosecutions
Semi-Structured Schedule for Victoria Police Interviews

Respondent Code: _______
Print a copy for each respondent, to record demographics and make notes during interview.

Explanation of Study and the Interview Process

This research aims to examine public and private policing of electronic crime in Victoria, with particular focus upon the issues of achieving successful investigative and prosecution partnerships. The Department of Justice and Multimedia Victoria have sponsored this independent research to learn more about how the private sector responds to crime involving information technology and how police can work with the private sector to lessen the impact of these crimes.

The Research Coordinating Committee of Victoria Police has approved the study and your participation in the study. Your participation or non-participation will have no effect upon your employment. The research is not an evaluation of job performance.

Throughout this interview, I would like to discuss with you theories about partnership policing and get your views as a policing practitioner, on how well they explain and would assist policing of electronic crime. Your views can then be fed back into the research about e-crime to improve the theory and practice. This process is known as realistic evaluation.

The results of this study will be communicated to business and law enforcement to inform policy about partnerships between the private sector and law enforcement.

To assist me in making an accurate record of what you say, do you agree to me taping the interview? The tapes will be destroyed once transcribed and you will not be named in any publication relating to this research. You may request a copy of the interview transcript, if you wish to check its accuracy.

Throughout the interview, if you wish to add any comments or ask any questions, please do so. You may stop the interview at any time.

Have respondent read Plain Language statement and sign Consent Form, if proceeding to participate. Copy to participant. Test tape recorder. Provide opportunity for respondent to ask questions

About the respondent

Before we begin, I’d like to get some demographic information from you to assist analysis of the interview.

Record Sex of Respondent: ☐ Male ☐ Female
Record approx age of respondent: ☐ 18-20 ☐ 21-24 ☐ 25-29 ☐ 30-34 ☐ 35-44 ☐ 45-54 ☐ 55-64 ☐ 65-74 ☐ 75 or older
Record department or CIU respondent is stationed in:
What is your present rank and job title within Victoria Police?

Are you a Detective?  ☑ Yes  ☐ No

Is that a sworn or unsworn position?  ☑ Sworn  ☑ Unsworn

How many years have you been in Victoria Police?

How many years have you been in your present position?

What are your usual day-to-day activities?
   (Probes: Do you investigate cases? Do you prosecute cases?)

What type of cases do you work on most often?

Provide respondent with the definition of e-crime to guide remainder of interview: “Electronic crimes are where a computer is used as a tool or as a target in the commission of the crime. It includes using a computer as a storage device for illegal data” (Etter, Dec 2002).

Now thinking about that definition of e-crime, are there other offences you would consider “e-crime”?

In terms of doing your job, how useful or relevant is this definition of “electronic crime” for you?

The next few questions look at your opinions and experiences about how people respond to electronic crime.

Handout of “Priority of e-crime types” question
E-crime is a global problem, and offenders can be located on the other side of the globe or locally. What priority do you give to interstate or international incidents in comparison to local offences? What priority should be given?

What’s different now about how police investigate electronic crime from the past?

**Factors affecting the outcome of e-crime cases**

Part of my earlier work on this project has been to examine police and prosecution documents relating to closed electronic crime cases, to find common characteristics of those cases, and what characteristics might have led to successful or unsuccessful outcomes. What I’d like to do next is ask for your opinions about the factors affecting the outcomes of e-crime cases.

**Outcomes**

What outcomes do you consider “successful” outcomes for electronic crime cases?

Can a case be successful if it is not prosecuted?

What outcomes do you consider “unsuccessful” outcomes for electronic crime cases?

Thinking from the public (or victims’) point of view, what do you think they consider “successful” outcomes?

Again, from the public (or victims’) point of view, what do you think they consider “unsuccessful” outcomes?

**Factors influencing outcome**

This is a list of factors identified from the documentary analysis as contributing to the success or failure of an investigation or prosecution. I’ll go through the list with you. Do you agree with the items on the list? Is there any item on this list that you would dispute or remove from the list? If yes, why would you remove that?

<table>
<thead>
<tr>
<th>Handout of factors derived from documentary analysis</th>
</tr>
</thead>
</table>

Are there any items you would add to the list? If yes, ‘Why would you include that?’

Using the scale next to each item, how important would you rate these factors as determining whether a case is *investigated* successfully?

Record answers (Number from 1 to 5):

___ Factor 1  ___ Factor 2  ___ Factor 3 etc
___ Any factors provided by interviewee

You rated [insert factor(s)] as most important to an investigation. Why is that?

Using the scale next to each item, how important would you rate these factors as determining whether a case is prosecuted successfully?

Record answers (Number from 1 to 5):
___ Factor 1   ___ Factor 2   ___ Factor 3 etc

___ Any factors provided by interviewee

You rated [insert factor(s)] as most important to a prosecution. Why was that?

---

**Case Study - Personal Experiences Policing E-Crime**

As I mentioned before, the first part of this study was an examination of cases for factors that affected the outcomes of those cases. You were involved with some of those cases. I would like to discuss some of those cases to confirm my understanding of the case documents. Remember, no person or company involved in any case will be identified in any publication arising from this research.

Could you tell me about your own experiences with electronic crimes cases?
Probes:   Types of cases   Number of cases   Decision making

Apart from being a police officer, do you have any special qualifications or training in relation to investigation of e-crime?
(probe: for example CSSP (Cisco Certified Security Professional), higher degrees, internal Victoria Police courses etc?)

Tell me about a case you were involved in that had a successful outcome, which for you exemplifies best practice. (This may or may not involve the private sector involvement). [Probes: Detection or report, initial assessment, investigation, prosecution or other outcome]

The earlier research was restricted to closed cases. This is only half the picture, when it comes to investigated cases, some of which remain unsolved or open for various reasons. Without identifying these cases or the people involved, I would like to discuss factors involved in “unsuccessful” e-crime cases.

Tell me about a case you were involved in that did not have a successful outcome. (Explore the factors believed to have led to the unsuccessful outcome).
Next, I’d like to discuss briefly your interactions with other law enforcement agencies in relation to investigating e-crime:

What’s routine; Processes, regulations; Benefits
Constraints or difficulties and possible improvements

Agency name prompts: Australian High Tech Crime Centre, Australian Crime Commission, AFP, other state police services
Overseas agencies – UK National High Tech Crimes Unit
New York Electronic Crimes Taskforce
FBI, Interpol

Ok, having discussed briefly your interactions with other law enforcement agencies, I want to move onto the main focus of this research – interactions and alliances between police and the private sectors. One of the aims of the research is to catalogue the various organisational means by which police interact with the private sector in relation to e-crime.

With whom from the private sector do Victoria Police, and you in particular, interact in relation to e-crime? (General descriptions are fine)

In what ways do police interact with these groups in relation to e-crime? How often? What are the strategic aims of this interaction?

(Non)-reporting of e-crime
Detecting e-crime and under-reporting are often mentioned as major problems in relation to e-crime.

What local factors do you think contribute to reporting and under-reporting of e-crime in Victoria? Is additional reporting desirable?

One private sector investigation firm reports some incidents to police in the form of letters indicating that they do not wish police involvement. Their purpose of doing so is to make sure incidents are included in police statistics without influencing their own investigations. Is this sort of reporting worthwhile?

Models of Interaction

These are descriptions proposed by two Australian researchers, Rick Sarre and Tim Prenzler. In your experience of e-crime cases, which of the following best describe the type of interaction you have as a police officer with private sector investigators?
Now I would like to explore your thoughts on the issue of forming strategic alliances or “partnerships” with the private sector to investigate e-crime.

What does “working in partnership with” mean to you? (probe: what characteristics define “working in partnership” for you?)

With whom from the private sector should law enforcement be working to investigate e-crime?

With whom from the private sector should law enforcement be working to prosecute e-crime?

With whom should law enforcement NOT form partnerships to fight electronic crime? (probe: Hackers?)

**Probe - Industry sectors**

- Accommodation
- Cafes & Restaurants
- Agricultural, Forestry & Fishing
- Communication Services
- Construction
- Cultural and Recreational Services
- Education
- Electricity, Gas and Water Supply
- Finance & Insurance
- Government Administration and Defense
- Health and Community Services
- Manufacturing
- Mining
- Personal and Other Services
- Property and Business Services
- Retail Trade
- Transport and Storage
- Wholesale Trade

Can you describe any partnerships between Victoria Police and the private sector for fighting e-crime? (alternative: Who wants to partner with Victoria Police?)

Do you have any specific concerns about the interaction of police with the private IT security industry?

**Format of strategic alliances or partnerships**

How can law enforcement agencies work better with the private sector to police e-crime?

There are many different ways in which police could work with the private sector to investigate e-crime. Which activities do you consider most important to pursue?

- Discussion forums (Face to face, Email?)
- Memoranda of Understanding
- R&D projects
- Joint investigations
- Infrastructure projects
- Joint Taskforces
- Neighbourhood Watch style mtgs
- Vendor-supplier relationships
- Crime Stoppers style hotlines
- Something else?
“Real-time assistance” has been highlighted as a major problem of interacting with the private sector. How can real time assistance be achieved?

Provide handout of additional partnership topics to discuss. Not all of these may be covered, depending upon the respondent.

**Regulating strategic alliances and partnerships**
Referring back to the different models of interaction between police and private security, Sarre and Prenzler further argue that cooperation between law enforcement and the private sector needs to be limited and closely regulated.

Do you believe new laws are needed to regulate interactions between police and private police *when they investigate e-crime jointly*? What is needed?

What forms of regulation exist currently to guide strategic alliances and public-private partnerships? [Probe: Eg, Police Regulations Act and Constitution Act regulate police behaviour]

They have proposed the establishment of *standard procedures for interaction between the sectors*? What do you think of this?

Should the private sector be given additional police-like powers to investigate e-crime? If yes, what sort, and how should they be regulated? If no, why not?

**Model Computer Crime Offences**

Finally, I’d like to discuss the influence of the law, especially the model computer offences which were introduced in Victoria on 6 May 2003 by the Crimes (*Property Damage and Computer Offences*) Act 2003 (Vic).

Offer copy of the new offences to respondent as mnemonic device.

If a relevant case came before you, would you choose to charge a person with one of these offences, or would you prefer other charges instead? Why is that?

In your opinion, what is useful about this model legislation?

In your opinion, are there any problems with the model computer offences, which effect your ability to investigate or prosecute?

What legislative changes would you like to see made in relation to computer offences? (Probe: What are your reasons for such changes?)
The future – Suggestions to Improve E-Crime Investigation

We’ve discussed a lot of different issues about investigating and prosecuting e-crime. To finish, are there any (further) suggestions you would like to make, which might help reduce the impact and incidence of e-crime?

Debrief Respondent

Thank you for taking part in the study. As explained before the interview I will be making the results from the study available to Victoria Police and also on the research website: www.crim.unimelb.edu.au/research/ecrime.

You may request a copy of the interview transcript, if you wish to check its accuracy.

Requests copy of transcript: ☐ Yes ☐ No

Provide opportunity for respondent to ask questions
Appendix N: Handouts used during police & private sector interviews

Definition of E-crime

“Electronic crimes are where a computer is used as a tool or as a target in the commission of the crime. It includes using a computer as a storage device for illegal data.” (Etter, Dec 2002)

<table>
<thead>
<tr>
<th>Sarre and Prenzler’s Models of Police and Private Security Interaction</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Model</strong></td>
</tr>
<tr>
<td>---------</td>
</tr>
<tr>
<td>Property</td>
</tr>
<tr>
<td>Division of Labor</td>
</tr>
<tr>
<td>Competing Forces</td>
</tr>
<tr>
<td>Supplementary Service</td>
</tr>
<tr>
<td>Ad Hoc Partnership</td>
</tr>
<tr>
<td>Combined Forces</td>
</tr>
<tr>
<td>Unholy Alliance</td>
</tr>
</tbody>
</table>
# Priority of different types of electronic crime

Below is a list of crimes that have been characterised as “electronic crime”. The police give some crimes higher priority than others. We are interested in finding out what you think these priorities are CURRENTLY. Please tick (✔) only ONE box next to each item.

<table>
<thead>
<tr>
<th>Crime Description</th>
<th>Very Low Priority</th>
<th>Low Priority</th>
<th>Some Priority</th>
<th>High Priority</th>
<th>Very High Priority</th>
</tr>
</thead>
</table>
a. Theft of telecommunications services ("phreaking") | | | | | |
b. Theft of electronic funds | | | | | |
c. Electronic vandalism (eg defaced websites) | | | | | |
d. Credit card fraud (including “phishing” scams) | | | | | |
e. Advance fee scams (eg, Nigerian email scams) | | | | | |
f. Identity theft & fraud (eg counterfeit documents) | | | | | |
g. Defamation online | | | | | |
h. Unauthorised access to computer | | | | | |
i. Dissemination of offensive content (eg child porn, racial hatred) | | | | | |
j. Cyber-stalking | | | | | |
k. Digital piracy (eg software, music, multimedia) | | | | | |
l. Digital extortion (a demand accompanied by a threat) | | | | | |
m. Criminal communications | | | | | |
n. Illegal online gambling | | | | | |
o. Electronic money laundering or tax evasion | | | | | |
p. Spam (unsolicited email) | | | | | |
q. Authoring computer viruses | | | | | |
r. Illegal interception of digital information | | | | | |
q. Denial of service attacks | | | | | |
s. Theft of proprietary / confidential information | | | | | |
t. Online Auction fraud | | | | | |
In the previous question, we asked for your views on the priorities police currently give to different types of e-crime. You may or may not agree with these priorities. We are interested in finding out what you think police priorities SHOULD BE. Please tick (✔) only ONE box next to each item.

<table>
<thead>
<tr>
<th>a. Theft of telecommunications services (“phreaking”)</th>
<th>very low priority</th>
<th>low priority</th>
<th>some priority</th>
<th>high priority</th>
<th>very high priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>b. Theft of electronic funds</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>c. Electronic vandalism (eg defaced websites)</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>d. Credit card fraud (including “phishing” scams)</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>e. Advance fee scams (eg, Nigerian email scams)</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>f. Identity theft &amp; fraud (eg counterfeit documents)</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>g. Defamation online</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>h. Unauthorised access to computer</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>i. Dissemination of offensive content (eg child porn, racial hatred)</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>j. Cyber-stalking</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>k. Digital piracy (eg software, music, multimedia)</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>l. Digital extortion (a demand accompanied by a threat)</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>m. Criminal communications</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>n. Illegal online gambling</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>o. Electronic money laundering or tax evasion</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>p. Spam (unsolicited email)</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>q. Authoring computer viruses</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>r. Illegal interception of digital information</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>q. Denial of service attacks</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>s. Theft of proprietary / confidential information</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>t. Online Auction fraud</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
</tbody>
</table>
“Partnership / Strategic Alliance” issues to explore:

- Benefits (especially, benefits unobtainable otherwise, compare to regular investigation processes)
- Constraints / restrictions
- Investigation powers – private sector wants more?
- Payment for resources? (Recompense to private sector; buying police services, joint ventures or partnerships)
- Accountability in private sector / police investigations
- Information flow (one way; shared)
- Security issues
- Privacy / Disclosure issues
- Likely and actual impacts – what have been the outcomes of partnered investigations? (Case outcome, expenditures, media etc)
# Appendix O: LEAP sample demographics

Table App O.1: E-crime incidents sampled from LEAP, 1999/00-2003/04

<table>
<thead>
<tr>
<th>LEAP offence group / Description</th>
<th>LEAP Code</th>
<th>Legislative source</th>
<th>Total LEAP incidents</th>
<th>Cleared incidents</th>
<th>E-crime incidents</th>
<th>Coded sample 1</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Deception</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Obtain property by deception</td>
<td>321A</td>
<td>81(1) Crimes Act (Vic)</td>
<td>50258</td>
<td>16107</td>
<td>1634*</td>
<td>163</td>
</tr>
<tr>
<td>Obtain financial advantage by deception</td>
<td>321B</td>
<td>82(1) Crimes Act (Vic)</td>
<td>7422</td>
<td>2963</td>
<td>443†</td>
<td>44</td>
</tr>
<tr>
<td>Make false document (Crimes Act)</td>
<td>321C</td>
<td>83A(1) Crimes Act (Vic)</td>
<td>2099</td>
<td>1328</td>
<td>119</td>
<td>12</td>
</tr>
<tr>
<td>False accounting</td>
<td>321L</td>
<td>83 Crimes Act (Vic)</td>
<td>279</td>
<td>124</td>
<td>39</td>
<td>4</td>
</tr>
<tr>
<td>Engage in money laundering</td>
<td>323AL</td>
<td>121 Confiscation Act 1997†</td>
<td>106</td>
<td>78</td>
<td>12</td>
<td>1</td>
</tr>
<tr>
<td>Make/possess article to make false doc</td>
<td>323C</td>
<td>83A(5C) Crimes Act (Vic)</td>
<td>11</td>
<td>8</td>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td>Conspiracy to cheat/defraud (common law)</td>
<td>321BP</td>
<td>321 Crimes Act (Vic)</td>
<td>39</td>
<td>18</td>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>Have custody false document (crimes act)</td>
<td>321N</td>
<td>83A(5) Crimes Act (Vic)</td>
<td>23</td>
<td>19</td>
<td>4</td>
<td>1</td>
</tr>
</tbody>
</table>

Source: Victoria Police Pilot Intelligence database and McKenzie 2005, E-Crime Investigation Study [computer file] cont...

* OPBD includes 965 incidents identified as e-crime by definition, having Modus Operandi entries of “ATM / EFTPOS INVOLVED” or “CREDIT CARD INVOLVED”
† OFABD includes 163 incidents identified as e-crime by definition, having Modus Operandi entries of “ATM / EFTPOS INVOLVED” or “CREDIT CARD INVOLVED”
‡ Repealed by No. 104/2003 s. 5(1) (Vic).
<table>
<thead>
<tr>
<th>LEAP offence group / Description</th>
<th>LEAP Code</th>
<th>Legislative source</th>
<th>Total LEAP incidents</th>
<th>Cleared incidents</th>
<th>E-crime incidents</th>
<th>Coded sample 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deception</td>
<td>[cont...]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HAVE CUSTODY FALSE DOCUMENT (CRIMES ACT)</td>
<td>321N</td>
<td>83A(5) Crimes Act (Vic)</td>
<td>23</td>
<td>19</td>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>PRODUCE/USE ACCOUNT TO MISLEAD/DECEIVE</td>
<td>321MG</td>
<td>83(1)(b) Crimes Act (Vic)</td>
<td>17</td>
<td>13</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>APPLY FALSE REGISTERED TRADEMARK</td>
<td>321NT</td>
<td>148(G) Trademarks Act 1958 (Cth)</td>
<td>4</td>
<td>3</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>FORGE PRESCRIPTION-DRUG OF DEPENDENCE</td>
<td>699B</td>
<td>77 Drugs, Poisons &amp; Controlled Substances Act 1981</td>
<td>499</td>
<td>292</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>OPEN ACCOUNT IN FALSE NAME</td>
<td>321CL</td>
<td>24 Financial Transaction Reports Act 1988 (Cth)</td>
<td>26</td>
<td>8</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>OBTAIN PTC TICKET CONCESSION BY FRAUD</td>
<td>321GT</td>
<td>221(5) Transport Act 1983 (Vic)</td>
<td>23</td>
<td>19</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>FORGE PRESCRIPTION-RESTRICTED SUBSTANCE</td>
<td>699A</td>
<td>36A Drugs, Poisons and Controlled Substances Act 1981</td>
<td>286</td>
<td>142</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>POSS INSTRUMENT FOR FORGING TRADE MARK</td>
<td>321CH</td>
<td>98(1)(d) Trademarks Act (Cth)</td>
<td>3</td>
<td>3</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>OPERATE ACCOUNT IN FALSE NAME</td>
<td>321CM</td>
<td>24(2) Financial Transaction Reports Act 1988 (Cth)</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

### Table App O.1: E-crime incidents sampled from LEAP, 1999/00-2003/04 (cont.)

<table>
<thead>
<tr>
<th>LEAP offence group / Description</th>
<th>LEAP Code</th>
<th>Legislative source</th>
<th>Total LEAP incidents</th>
<th>Cleared incidents</th>
<th>E-crime incidents</th>
<th>Coded sample 1</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Deception</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FALSE STATEMENT-DESTROY/DAMAGE PROPERTY</td>
<td>321K</td>
<td>247(b) Crimes Act (Vic)</td>
<td>2 2 1 1</td>
<td>1 1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PRODUCE/USE ACCOUNT TO MISLEAD/DECEIVE</td>
<td>321M</td>
<td>83(1)(b) Crimes Act (Vic)</td>
<td>181 87 1 1</td>
<td>1 1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FORGE LICENCE/LEARNER'S PERMIT MAKE EQUIP KNOWING TO MAKE FALSE DOC</td>
<td>321OA</td>
<td>72(1)(a) Road Safety Act (Vic)</td>
<td>1 1 1 1</td>
<td>1 1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAKE EQUIP KNOWING TO MAKE FALSE DOC</td>
<td>323AI</td>
<td>83A(5A) Crimes Act (Vic)</td>
<td>1 1 1 1</td>
<td>1 1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HAVE CUSTODY EQUIP KNOW MAKE FALSE DOC</td>
<td>323AJ</td>
<td>83A(5A) Crimes Act (Vic)</td>
<td>2 2 1 1</td>
<td>1 1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RECEIVE SECRET COMMISSION</td>
<td>854BB</td>
<td>180 Crimes Act (Vic)</td>
<td>7 6 1 1</td>
<td>1 1</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Sub-total</strong></td>
<td></td>
<td></td>
<td>61313 21244 2287 242</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Table App O.1: E-crime incidents sampled from LEAP, 1999/00-2003/04 (cont.)

<table>
<thead>
<tr>
<th>LEAP offence group / Description</th>
<th>LEAP Code</th>
<th>Legislative source</th>
<th>Total LEAP incidents</th>
<th>Cleared incidents</th>
<th>E-crime incidents</th>
<th>Coded sample 1</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Harassment</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>USE TELECOMMUNICATIONS SERVICE TO MENACE</td>
<td>832BA</td>
<td>85ZE Crimes Act (Cth)</td>
<td>945</td>
<td>462</td>
<td>462</td>
<td>46</td>
</tr>
<tr>
<td>USE TELECOMMUNICATIONS SERVICE TO HARASS</td>
<td>832BB</td>
<td>85ZE Crimes Act (Cth)</td>
<td>812</td>
<td>359</td>
<td>359</td>
<td>36</td>
</tr>
<tr>
<td>STALK ANOTHER PERSON (CRIMES ACT)</td>
<td>199AB</td>
<td>21A Crimes Act (Vic)</td>
<td>3830</td>
<td>2075</td>
<td>119</td>
<td>12</td>
</tr>
<tr>
<td>USE TELECOMMUNICATIONS SERVICE TO OFFEND USE LISTENING DEVICE</td>
<td>832BC</td>
<td>85ZE Crimes Act (Cth)</td>
<td>77</td>
<td>36</td>
<td>36</td>
<td>4</td>
</tr>
<tr>
<td>USEPOSSESS/SELL PHONE INTERCEPT DEVICE</td>
<td>832B</td>
<td>4(1A) Listening Devices Act 1969 (Vic)*</td>
<td>6</td>
<td>4</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>INTERCEPT A COMMUNICATION</td>
<td>832AS</td>
<td>85ZKB Crimes Act (Cth)</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>INTERCEPT A COMMUNICATION</td>
<td>832AZ</td>
<td>7(1)(a) Telecommunications Act (Cth)</td>
<td>3</td>
<td>2</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td><strong>Sub-total</strong></td>
<td></td>
<td></td>
<td>5675</td>
<td>2940</td>
<td>983</td>
<td>101</td>
</tr>
</tbody>
</table>

Source Victoria Police Pilot Intelligence database and McKenzie 2005, E-Crime Investigation Study [computer file]

* Repealed on 1 January 2000 by section 38 of the Surveillance Devices Act 1999 (Vic).
<table>
<thead>
<tr>
<th>LEAP offence group / Description</th>
<th>LEAP Code</th>
<th>Legislative source</th>
<th>Total LEAP incidents</th>
<th>Cleared incidents</th>
<th>E-crime incidents</th>
<th>Coded sample 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Regulated Public Order</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>KNOWINGLY POSSESS CHILD PORNOGRAPHY</td>
<td>571AI</td>
<td>70(1) Crimes Act (Vic)</td>
<td>283</td>
<td>250</td>
<td>204</td>
<td>20</td>
</tr>
<tr>
<td>MAKE/PRODUCE CHILD PORNOGRAPHY</td>
<td>571AJ</td>
<td>68 Crimes Act (Vic)</td>
<td>103</td>
<td>89</td>
<td>62</td>
<td>6</td>
</tr>
<tr>
<td>USE ON-LINE INFO TO PUBLISH CHILD PORN</td>
<td>572EB</td>
<td>57A Classification (Publications, Films &amp; Computer Games) (Enforcement) Act (Vic)</td>
<td>14</td>
<td>14</td>
<td>14</td>
<td>1</td>
</tr>
<tr>
<td>USE ON-LINE INFO SERV PUBLISH OBJEC MAT.</td>
<td>572DO</td>
<td>57 Classification (Publications, Films &amp; Computer Games) (Enforcement) Act (Vic)</td>
<td>8</td>
<td>7</td>
<td>7</td>
<td>1</td>
</tr>
<tr>
<td>PROCURE MINOR FOR CHILD PORNOGRAPHY</td>
<td>571AH</td>
<td>69 Crimes Act (Vic)</td>
<td>16</td>
<td>11</td>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td>CREDIT BETTING</td>
<td>592JX</td>
<td>119 Gambling Regulation Act 2003 (Vic)</td>
<td>16</td>
<td>16</td>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td>SCREEN OBJECT FILM</td>
<td>572AD</td>
<td>9(1)(b) Films (Classification) Act 1984</td>
<td>7</td>
<td>3</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>SELL FILM CLASSIFIED X</td>
<td>572DL</td>
<td>15(1) Classification (Publications, Films &amp; Computer Games) (Enforcement) Act (Vic)</td>
<td>5</td>
<td>5</td>
<td>3</td>
<td>1</td>
</tr>
</tbody>
</table>

Source: Victoria Police Pilot Intelligence database and McKenzie 2005, E-Crime Investigation Study [computer file] cont...
<table>
<thead>
<tr>
<th>LEAP offence group / Description</th>
<th>LEAP Code</th>
<th>Legislative source</th>
<th>Total LEAP incidents</th>
<th>Cleared incidents</th>
<th>E-crime incidents</th>
<th>Coded sample 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Regulated Public Order [cont...]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SELL UNCLASSIFIED FILM AS CLASSIFIED</td>
<td>572N</td>
<td>21 Films (Classification) Act 1984 (Vic)</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>PROCURE UNDER 18 TO MAKE OBJECT FILM</td>
<td>571A</td>
<td>11(3) Films (Classification) Act 1984</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>POSS UNCLASS FILM INTENT SELL/EXHIBIT</td>
<td>572DF</td>
<td>23(1)(b) Classifications (Publications, Films &amp; Computer Games) (Enforcement) Act 1995 (Vic)</td>
<td>10</td>
<td>10</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>POSS UNCLASSIFIED COMP GAME INTENT SELL</td>
<td>572DI</td>
<td>45(1)(b) Classifications (Publications, Films &amp; Computer Games) (Enforcement) Act 1995 (Vic)</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>SELL FILM CLASSIFIED RC</td>
<td>572DK</td>
<td>15 Classifications (Publications, Films &amp; Computer Games) (Enforcement) Act 1995 (Vic)</td>
<td>5</td>
<td>4</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>EXHIBIT IN PRIVATE TO MINOR &quot;X&quot; FILM</td>
<td>572DQ</td>
<td>12(1)(b) Classifications (Publications, Films &amp; Computer Games) (Enforcement) Act 1995 (Vic)</td>
<td>20</td>
<td>9</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>CAUSE CHILD TO TAKE PART IN PROSTITUTION</td>
<td>595DC</td>
<td>5 Prostitution Control Act (Vic)</td>
<td>9</td>
<td>6</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>

Table App O.1: E-crime incidents sampled from LEAP, 1999/00-2003/04 (cont.)

<table>
<thead>
<tr>
<th>LEAP offence group / Description</th>
<th>LEAP Code</th>
<th>Legislative source</th>
<th>Total LEAP incidents</th>
<th>Cleared incidents</th>
<th>E-crime incidents</th>
<th>Coded sample 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Regulated Public Order [cont...]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>POSSESS OBJECT FILM FOR SALE</td>
<td>572AC</td>
<td>9(1)(a) Films (Classification) Act 1984 (Vic)</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>SCREEN OBJTN FILM IN PRESENCE OF CHILD</td>
<td>572CE</td>
<td>12 Classification (Publications, Films &amp; Computer Games) (Enforcement) Act (Vic)</td>
<td>4</td>
<td>3</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>POSS X FILM INTENT TO SELL/EXHIBIT FILM</td>
<td>572DE</td>
<td>23(1)(a) Classification (Publications, Films &amp; Computer Games) (Enforcement) Act (Vic)</td>
<td>9</td>
<td>4</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>POSS RC FILM INTENT TO SELL/EXHIBIT FILM</td>
<td>572DM</td>
<td>23(1)(a) Classification (Publications, Films &amp; Computer Games) (Enforcement) Act (Vic)</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>EXTEND ANY FORM OF CREDIT TO ONESELF</td>
<td>592KC</td>
<td>119(d) Gambling Regulation Act (Vic)</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td><strong>Sub-total</strong></td>
<td></td>
<td></td>
<td><strong>524</strong></td>
<td><strong>444</strong></td>
<td><strong>323</strong></td>
<td><strong>44</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>LEAP offence group / Description</th>
<th>LEAP Code</th>
<th>Legislative source</th>
<th>Total LEAP incidents</th>
<th>Cleared incidents</th>
<th>E-crime incidents</th>
<th>Coded sample 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Other</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BOMB HOAX-MAKE STATEMENT/CONVEY INFO</td>
<td>199AG</td>
<td>317A(2) Crimes Act (Vic)</td>
<td>516</td>
<td>150</td>
<td>137</td>
<td>14</td>
</tr>
<tr>
<td>BLACKMAIL</td>
<td>221A</td>
<td>87 Crimes Act (Vic)</td>
<td>355</td>
<td>211</td>
<td>62</td>
<td>6</td>
</tr>
<tr>
<td>INSTALL/USE SURVEILL DEVICE W/O CONSENT</td>
<td>889LR</td>
<td>7 Surveillance Devices Act (Vic)</td>
<td>31</td>
<td>28</td>
<td>22</td>
<td>2</td>
</tr>
<tr>
<td>ENTER COMPUTER SYSTEM - NO AUTHORITY</td>
<td>593M</td>
<td>9A Summary Offences Act (Vic)*</td>
<td>19</td>
<td>19</td>
<td>19</td>
<td>2</td>
</tr>
<tr>
<td>GAIN ACCESS TO COMPUTER - NO AUTHORITY</td>
<td>593N</td>
<td>9A Summary Offences Act (Vic)*</td>
<td>12</td>
<td>12</td>
<td>12</td>
<td>1</td>
</tr>
<tr>
<td>RECEIVE/POSSESS PROCEEDS OF CRIME</td>
<td>331F</td>
<td>82 Proceeds of Crime Act (Cth) †</td>
<td>1238</td>
<td>1129</td>
<td>8</td>
<td>1</td>
</tr>
<tr>
<td>POSS DEVICE FOR MAKING INFRINGING COPIES</td>
<td>839J</td>
<td>132(3) Copyright Act (Cth)</td>
<td>8</td>
<td>7</td>
<td>6</td>
<td>1</td>
</tr>
<tr>
<td>UNAUTH INTERFERE WITH COMPUTER</td>
<td>321MQ</td>
<td>76E(b) Crimes Act (Cth)</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td>DISTRIBUTION OF INFRINGEMENT ARTICLE</td>
<td>839E</td>
<td>132(2A)(b) Copyright Act (Cth)</td>
<td>6</td>
<td>6</td>
<td>5</td>
<td>1</td>
</tr>
</tbody>
</table>

Source: Victoria Police Pilot Intelligence database and McKenzie 2005, E-Crime Investigation Study [computer file] cont...

* Repealed on 6 May 2003, replaced by Model Computer offences in the Crimes Act (Vic).
† Repealed by No. 86/2002 (Cth).
### Table App O.1: E-crime incidents sampled from LEAP, 1999/00-2003/04 (cont.)

<table>
<thead>
<tr>
<th>LEAP offence group / Description</th>
<th>LEAP Code</th>
<th>Legislative source</th>
<th>Total LEAP incidents</th>
<th>Cleared incidents</th>
<th>E-crime incidents</th>
<th>Coded sample 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Other [cont...]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CONVICTED SEX OFFENDER LOITER SCHOOL ETC</td>
<td>599CA</td>
<td>60B(2) Crimes Act (Vic)</td>
<td>67</td>
<td>54</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>KNOWINGLY CAUSE UNAUTH COMPUTER FUNCTION</td>
<td>321PJ</td>
<td>247B Crimes Act (Vic)</td>
<td>2*</td>
<td>2*</td>
<td>2*</td>
<td>1</td>
</tr>
<tr>
<td>FAIL REPORT USE OF LISTENING DEVICE</td>
<td>832E</td>
<td>5(a) Listening Devices Act 1969 (Vic)†</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td><strong>Sub-total</strong></td>
<td></td>
<td></td>
<td><strong>2260</strong></td>
<td><strong>1624</strong></td>
<td><strong>281</strong></td>
<td><strong>32</strong></td>
</tr>
</tbody>
</table>

**Sex (Non Rape)**

<table>
<thead>
<tr>
<th>Description</th>
<th>LEAP Code</th>
<th>Legislative source</th>
<th>Total LEAP incidents</th>
<th>Cleared incidents</th>
<th>E-crime incidents</th>
<th>Coded sample 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEX PEN OF A CHILD UNDER 16 YRS</td>
<td>137CY</td>
<td>45 Crimes Act (Vic)</td>
<td>1250</td>
<td>696</td>
<td>22</td>
<td>2</td>
</tr>
<tr>
<td>INDECENT ACT WITH CHILD UNDER 16</td>
<td>137DA</td>
<td>47 Crimes Act (Vic)</td>
<td>2996</td>
<td>1649</td>
<td>15</td>
<td>2</td>
</tr>
<tr>
<td>SEXUAL PENETRATION PERSON 10-16</td>
<td>137C</td>
<td>46 Crimes Act (Vic)</td>
<td>590</td>
<td>329</td>
<td>10</td>
<td>1</td>
</tr>
</tbody>
</table>

Source: Victoria Police Pilot Intelligence database and McKenzie 2005, E-Crime Investigation Study [computer file] cont...

* Does not include 3 incidents recorded under the incorrect code, but which in their narratives stated the charge was s247B of the Crimes Act 1958 (Vic).

† Repealed on 1 January 2000 by section 38 of the Surveillance Devices Act 1999.
Table App O.1: E-crime incidents sampled from LEAP, 1999/2000-2003/2004 (cont.)

<table>
<thead>
<tr>
<th>LEAP offence group / Description</th>
<th>LEAP Code</th>
<th>Legislative source</th>
<th>Total LEAP incidents</th>
<th>Cleared incidents</th>
<th>E-crime incidents</th>
<th>Coded * sample 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>sex (Non Rape) [cont…]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEX PEN WITH CHILD UNDER 10</td>
<td>137B</td>
<td>45 Crimes Act (Vic)</td>
<td>312</td>
<td>186</td>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td>INDECENT ACT IN PRESENCE</td>
<td>137DC</td>
<td>47 Crimes Act (Vic)</td>
<td>348</td>
<td>192</td>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>CHILD UNDER 16</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEX PEN 16-17 UNDER CARE/SUPER/AUTH</td>
<td>137E</td>
<td>48 Crimes Act (Vic)</td>
<td>33</td>
<td>18</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>INDECENT ACT-16 YR OLD-CARE/SUPER/AUTH</td>
<td>137L</td>
<td>49 Crimes Act (Vic)</td>
<td>49</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>PROCURE FOR SEX PEN-THREAT/INTIMIDATION</td>
<td>137Q</td>
<td>57 Crimes Act (Vic)</td>
<td>8</td>
<td>6</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>PROCURE FOR SEX PEN OF CHILD UNDER 16</td>
<td>137S</td>
<td>58 Crimes Act (Vic)</td>
<td>15</td>
<td>9</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td><strong>Sub-total</strong></td>
<td></td>
<td></td>
<td><strong>5601</strong></td>
<td><strong>3085</strong></td>
<td><strong>61</strong></td>
<td><strong>11</strong></td>
</tr>
<tr>
<td><strong>TOTAL INCIDENTS</strong></td>
<td></td>
<td></td>
<td><strong>75401</strong></td>
<td><strong>29301</strong></td>
<td><strong>3931</strong>‡</td>
<td><strong>429</strong>§</td>
</tr>
</tbody>
</table>


* Sample 1 represents a proportional 10% sample of the number of E-crime incidents identified for each offence.

‡ Total exceeds the count of unique incidents in the data file (n=3529), as police often charge offenders with more than one offence per incident.

§ Total exceeds the count of actual incidents coded in the data file (n=365), as police often charge offenders with more than one offence per incident.
<table>
<thead>
<tr>
<th>LEAP offence description</th>
<th>LEAP Code</th>
<th>Legislative source</th>
<th>Total LEAP incidents</th>
<th>Cleared incidents</th>
<th>E-crime incidents</th>
<th>Coded sample 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>ENTER COMPUTER SYSTEM - NO AUTHORITY</td>
<td>593M</td>
<td>9A Summary Offences Act (Vic)*</td>
<td>19</td>
<td>19</td>
<td>19</td>
<td>19</td>
</tr>
<tr>
<td>GAIN ACCESS TO COMPUTER - NO AUTHORITY</td>
<td>593N</td>
<td>9A Summary Offences Act (Vic)*</td>
<td>12</td>
<td>12</td>
<td>12</td>
<td>12</td>
</tr>
<tr>
<td>UNAUTH INTERFERE WITH COMPUTER</td>
<td>321MQ</td>
<td>76E(b) Crimes Act (Cth)</td>
<td>5</td>
<td>5</td>
<td>3†</td>
<td>3†</td>
</tr>
<tr>
<td>KNOWINGLY CAUSE UNAUTH COMPUTER FUNCTION INTERCEPT A COMMUNICATION</td>
<td>321PJ</td>
<td>247B Crimes Act (Vic)</td>
<td>2</td>
<td>2</td>
<td>4‡</td>
<td>4‡</td>
</tr>
<tr>
<td>USE/POSSESS/SELL PHONE INTERCEPT DEVICE</td>
<td>832AZ</td>
<td>7(1)(a) Telecommunications Act (Cth)</td>
<td>3</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>“UNAUTH MODIFICATN OF DATA TO CAUSE IMPAIRMENT”**§</td>
<td>None§</td>
<td>247C Crimes Act (Vic)</td>
<td>0</td>
<td>0</td>
<td>1**</td>
<td>1**</td>
</tr>
</tbody>
</table>

Source: Victoria Police Pilot Intelligence database and McKenzie 2005, E-Crime Investigation Study [computer file] cont...

† Excludes 1 incident charged with 321PJ and another charged with s247C of the Crimes Act, but miscoded in LEAP as 321MQ.
‡ Includes 1 incident recorded incorrectly as 321K (FALSE STATEMENT-DESTROY/DAMAGE PROPERTY) and 1 incident recorded as 321MQ, which in their narratives stated the charge was s247B of the Crimes Act 1958 (Vic).
§ No offence code or description existed in LEAP at the time of sampling in Sept-Oct 2004 for s.247C. At 27 April 2005, this and the remaining model computer offences, ss. 247D, 247F and 247K of the Crimes Act 1958 (Vic) did not have LEAP offence codes or descriptions (Victoria Police, personal communication, 27/4/05).
** Coded incorrectly in LEAP as 321MQ.
<table>
<thead>
<tr>
<th>LEAP offence description</th>
<th>LEAP Code</th>
<th>Legislative source</th>
<th>Total LEAP incidents</th>
<th>Cleared incidents</th>
<th>E-crime incidents</th>
<th>Coded sample 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>POSS DATA INTEND COMMIT COMPUTER OFFENCE</td>
<td>321PN</td>
<td>247E Crimes Act (Vic)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>CAUSE UNAUTH ACCESS TO RESTRICTED DATA</td>
<td>321PQ*</td>
<td>247G Crimes Act (Vic)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>CAUSE UNAUTH MODIFICATN-RESTRICTED DATA</td>
<td>321PR*</td>
<td>247H Crimes Act (Vic)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>ACCESS C'WEALTH COMPUTER DATA</td>
<td>321HN</td>
<td>76B(1) Crimes Act (Cth)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>ACCESS C'WEALTH COMPUTER DATA-TO DEFRAUD</td>
<td>321HO</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ACCESS C'WEALTH COMPUTER DATA-SENSITIVE</td>
<td>321HP</td>
<td>76B(2) Crimes Act (Cth)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>ACCESS C'WEALTH DATA VIA LEGIT FACILITY</td>
<td>321HQ</td>
<td>76D Crimes Act (Cth)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>CAUSE PHONE COMMUNICATION BE MISDIRECTED</td>
<td>832AL</td>
<td>85ZD Crimes Act (Cth)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>CAUSE PHONE CARRIER SUPPLY FREE SERVICE</td>
<td>832AN</td>
<td>85ZF(b) Crimes Act (Cth)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td><strong>TOTAL INCIDENTS</strong></td>
<td></td>
<td></td>
<td><strong>43</strong></td>
<td><strong>42</strong></td>
<td><strong>43†</strong></td>
<td><strong>43†</strong></td>
</tr>
</tbody>
</table>


* These offence codes did not exist in LEAP at the time of sampling in Sept-Oct 2004. At 27 April 2005, the other model computer offences, ss. 247C, 247D, 247F and 247K of the Crimes Act 1958 (Vic) did not have LEAP offence codes or descriptions (Howell, M., personal communication, 27/4/05).

† Includes miscoded, closed incidents. Total exceeds the count of actual incidents coded in the data file (n=41), as some incidents involved more than one offence.
Table App O.1: Number of e-crime incidents reported to Victoria Police by financial year, 1999/00-2003/04

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>321A</td>
<td>109</td>
<td>282</td>
<td>489</td>
<td>401</td>
<td>353</td>
<td>1634</td>
</tr>
<tr>
<td>832BA</td>
<td>47</td>
<td>157</td>
<td>150</td>
<td>108</td>
<td></td>
<td>462</td>
</tr>
<tr>
<td>321B</td>
<td>43</td>
<td>86</td>
<td>106</td>
<td>108</td>
<td>100</td>
<td>443</td>
</tr>
<tr>
<td>832BB</td>
<td>46</td>
<td>139</td>
<td>100</td>
<td>74</td>
<td></td>
<td>359</td>
</tr>
<tr>
<td>571AI</td>
<td>11</td>
<td>28</td>
<td>53</td>
<td>40</td>
<td>72</td>
<td>204</td>
</tr>
<tr>
<td>199AG</td>
<td>14</td>
<td>43</td>
<td>32</td>
<td>27</td>
<td>21</td>
<td>137</td>
</tr>
<tr>
<td>199AB</td>
<td>6</td>
<td>27</td>
<td>16</td>
<td>33</td>
<td>37</td>
<td>119</td>
</tr>
<tr>
<td>321C</td>
<td>14</td>
<td>12</td>
<td>29</td>
<td>32</td>
<td>32</td>
<td>119</td>
</tr>
<tr>
<td>221A</td>
<td>3</td>
<td>16</td>
<td>15</td>
<td>12</td>
<td>16</td>
<td>62</td>
</tr>
<tr>
<td>571AJ</td>
<td>1</td>
<td>6</td>
<td>20</td>
<td>18</td>
<td>17</td>
<td>62</td>
</tr>
<tr>
<td>321L</td>
<td>1</td>
<td>7</td>
<td>14</td>
<td>9</td>
<td>8</td>
<td>39</td>
</tr>
<tr>
<td>832BC</td>
<td>6</td>
<td>11</td>
<td>14</td>
<td>5</td>
<td></td>
<td>36</td>
</tr>
<tr>
<td>137CY</td>
<td>1</td>
<td>3</td>
<td>1</td>
<td>10</td>
<td>6</td>
<td>22</td>
</tr>
<tr>
<td>889LR</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>5</td>
<td>7</td>
<td>22</td>
</tr>
<tr>
<td>593M</td>
<td>3</td>
<td>4</td>
<td>6</td>
<td>4</td>
<td>2</td>
<td>19</td>
</tr>
<tr>
<td>137DA</td>
<td>1</td>
<td>2</td>
<td>6</td>
<td>6</td>
<td></td>
<td>15</td>
</tr>
<tr>
<td>572EB</td>
<td>1</td>
<td>3</td>
<td>6</td>
<td>5</td>
<td></td>
<td>14</td>
</tr>
<tr>
<td>323AL</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>4</td>
<td>4</td>
<td>12</td>
</tr>
<tr>
<td>593N</td>
<td>2</td>
<td>6</td>
<td>3</td>
<td>1</td>
<td></td>
<td>12</td>
</tr>
<tr>
<td>137C</td>
<td>1</td>
<td>3</td>
<td>5</td>
<td>1</td>
<td></td>
<td>10</td>
</tr>
<tr>
<td>331F</td>
<td>1</td>
<td>3</td>
<td>4</td>
<td></td>
<td></td>
<td>8</td>
</tr>
<tr>
<td>572DO</td>
<td>1</td>
<td>6</td>
<td></td>
<td></td>
<td></td>
<td>7</td>
</tr>
<tr>
<td>839J</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>6</td>
</tr>
<tr>
<td>321MQ</td>
<td>3</td>
<td></td>
<td>1</td>
<td>1</td>
<td></td>
<td>5</td>
</tr>
<tr>
<td>323C</td>
<td></td>
<td>3</td>
<td>2</td>
<td></td>
<td></td>
<td>5</td>
</tr>
<tr>
<td>571AH</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td></td>
<td></td>
<td>5</td>
</tr>
<tr>
<td>592JX</td>
<td>1</td>
<td></td>
<td>2</td>
<td>2</td>
<td></td>
<td>5</td>
</tr>
<tr>
<td>839E</td>
<td></td>
<td>3</td>
<td>1</td>
<td>1</td>
<td></td>
<td>5</td>
</tr>
<tr>
<td>137B</td>
<td>2</td>
<td>2</td>
<td></td>
<td>1</td>
<td></td>
<td>5</td>
</tr>
<tr>
<td>137DC</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td>4</td>
</tr>
<tr>
<td>321BP</td>
<td>1</td>
<td></td>
<td>3</td>
<td>4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>321N</td>
<td></td>
<td>2</td>
<td>1</td>
<td>1</td>
<td></td>
<td>4</td>
</tr>
<tr>
<td>321MG</td>
<td></td>
<td></td>
<td>1</td>
<td>1</td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>321NT</td>
<td></td>
<td></td>
<td>1</td>
<td>1</td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>572AD</td>
<td>1</td>
<td></td>
<td></td>
<td>2</td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>572DL</td>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
</tbody>
</table>

Source: McKenzie 2005, E-Crime Investigation Study [computer file] cont...
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>572N</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>699B</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>832B</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>137E</td>
<td>1</td>
<td></td>
<td>1</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>321CL</td>
<td></td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>321GT</td>
<td></td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>321PJ</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2</td>
</tr>
<tr>
<td>571A</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>572DF</td>
<td></td>
<td>1</td>
<td>1</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>572DI</td>
<td></td>
<td>1</td>
<td>1</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>572DK</td>
<td></td>
<td>1</td>
<td>1</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>572DQ</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2</td>
</tr>
<tr>
<td>595DC</td>
<td></td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>599CA</td>
<td></td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>699A</td>
<td></td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>832AS</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>832AZ</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2</td>
</tr>
<tr>
<td>137L</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>137Q</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>137S</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>321CH</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>321CM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>321K</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>321M</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>321OA</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>323AJ</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>323AJ</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>572AC</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>572CE</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>572DE</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>572DM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>592KC</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>832E</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>854BB</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Totals</strong></td>
<td><strong>317</strong></td>
<td><strong>854</strong></td>
<td><strong>1092</strong></td>
<td><strong>944</strong></td>
<td><strong>724</strong></td>
<td><strong>3931</strong>*</td>
</tr>
</tbody>
</table>


* Total exceeds the count of unique incidents in the data file (n=3529), as police often charge offenders with more than one offence per incident.
Appendix P: Respondents' views of police e-crimes priorities

Table App P.1: Respondents views of police priorities for e-crimes

| Priority | Police | | | | | | Private Sectors | | | |
|----------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|
|          | very low | low | some | high | very high | no | very low | low | some | high | very high |
| Theft of telecommunications services ("phreaking") | Current | 6 | 8 | 6 | 1 | 0 | 4 | 11 | 12 | 13 | 4 | 2 |
| | | (28.6%) | (38.1%) | (28.6%) | (4.8%) | (0%) | (8.7%) | (23.9%) | (26.1%) | (28.3%) | (8.7%) | (4.3%) |
| | Should be | 4 | 6 | 6 | 4 | 1 | 5 | 6 | 8 | 12 | 11 | 4 |
| | | (19.0%) | (28.6%) | (28.6%) | (19.0%) | (4.8%) | (10.9%) | (13.0%) | (17.4%) | (26.1%) | (23.9%) | (8.7%) |
| Theft of electronic funds | Current | 1 | 1 | 9 | 9 | 1 | 3 | 4 | 1 | 11 | 15 | 12 |
| | | (4.8%) | (4.8%) | (42.9%) | (42.9%) | (4.8%) | (6.5%) | (8.7%) | (2.2%) | (23.9%) | (32.6%) | (26.1%) |
| | Should be | 2 | 4 | 11 | 4 | | 5 | 2 | 4 | 15 | 20 |
| | | (9.5%) | (19.0%) | (52.4%) | (19.0%) | | (10.9%) | (4.3%) | (8.7%) | (32.6%) | (43.5%) |
| Electronic vandalism (eg defaced websites) | Current | 7 | 5 | 6 | 3 | 0 | 4 | 12 | 15 | 7 | 5 | 3 |
| | | (33.3%) | (23.8%) | (28.6%) | (14.3%) | (0%) | (8.7%) | (26.1%) | (32.6%) | (15.2%) | (10.9%) | (6.5%) |
| | Should be | 4 | 6 | 7 | 4 | 0 | 6 | 1 | 17 | 14 | 2 | 6 |
| | | (19.0%) | (28.6%) | (33.3%) | (19.0%) | (0%) | (13.0%) | (2.2%) | (37.0%) | (30.4%) | (4.3%) | (13.0%) |
| Credit card fraud | Current | 2 | 3 | 6 | 9 | 1 | 4 | 4 | 3 | 9 | 14 | 12 |
| | (9.5%) | (14.3%) | (28.6%) | (42.9%) | (4.8%) | | (8.7%) | (8.7%) | (6.5%) | (19.6%) | (30.4%) | (26.1%) |
| | Should be | 1 | 0 | 6 | 10 | 4 | 5 | 0 | 1 | 6 | 14 | 20 |
| | | (4.8%) | (0%) | (28.6%) | (47.6%) | (19.0%) | (10.9%) | (0%) | (2.2%) | (13.0%) | (30.4%) | (43.5%) |

### Table App P.1: Respondents views of police priorities for e-crimes (cont.)

<table>
<thead>
<tr>
<th>Priority</th>
<th>Police</th>
<th>Private Sectors</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>very low</td>
<td>low</td>
</tr>
<tr>
<td>Advance fee scams (eg, Nigerian email scams)</td>
<td>Current</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td>Should be</td>
<td>33.3%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>28.6%</td>
</tr>
<tr>
<td>Identity theft &amp; fraud (eg counterfeit documents)</td>
<td>Current</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Should be</td>
<td>4.8%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>9.5%</td>
</tr>
<tr>
<td>Defamation online</td>
<td>Current</td>
<td>13</td>
</tr>
<tr>
<td></td>
<td>Should be</td>
<td>61.9%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>38.1%</td>
</tr>
<tr>
<td>Unauthorised access to computer</td>
<td>Current</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>Should be</td>
<td>23.8%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>9.5%</td>
</tr>
<tr>
<td>Dissemination of offensive content (eg child porn, racial hatred)</td>
<td>Current</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Should be</td>
<td>4.8%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4.8%</td>
</tr>
</tbody>
</table>

Source: McKenzie 2005, E-Crime Investigation Study [computer file#2], n=21 police, 46 private sector respondents. [cont.]
Table App P.1: Respondents views of police priorities for e-crimes (cont.)

<table>
<thead>
<tr>
<th>Priority</th>
<th>Police</th>
<th></th>
<th>Private Sectors</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>no</td>
<td>very low</td>
<td>low</td>
<td>some</td>
</tr>
<tr>
<td>Cyber-stalking</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Current</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>7</td>
</tr>
<tr>
<td>1.0%</td>
<td>9.5%</td>
<td>4.8%</td>
<td>33.3%</td>
<td>38.1%</td>
</tr>
<tr>
<td>Should be</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>5</td>
</tr>
<tr>
<td>1.0%</td>
<td>4.8%</td>
<td>0.0%</td>
<td>23.8%</td>
<td>33.3%</td>
</tr>
<tr>
<td>Digital piracy (eg software, music, multimedia)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Current</td>
<td>10</td>
<td>7</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>47.6%</td>
<td>33.3%</td>
<td>14.3%</td>
<td>4.8%</td>
<td>0.0%</td>
</tr>
<tr>
<td>Should be</td>
<td>9</td>
<td>6</td>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td>42.9%</td>
<td>28.6%</td>
<td>23.8%</td>
<td>4.8%</td>
<td>0.0%</td>
</tr>
<tr>
<td>Digital extortion (a demand accompanied by a threat)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Current</td>
<td>2</td>
<td>0</td>
<td>10</td>
<td>6</td>
</tr>
<tr>
<td>9.5%</td>
<td>0.0%</td>
<td>47.6%</td>
<td>28.6%</td>
<td>14.3%</td>
</tr>
<tr>
<td>Should be</td>
<td>1</td>
<td>0</td>
<td>4</td>
<td>8</td>
</tr>
<tr>
<td>4.8%</td>
<td>0.0%</td>
<td>19.0%</td>
<td>38.1%</td>
<td>38.1%</td>
</tr>
<tr>
<td>Criminal communications*</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Current</td>
<td>4</td>
<td>5</td>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td>19.0%</td>
<td>23.8%</td>
<td>23.8%</td>
<td>28.6%</td>
<td>4.8%</td>
</tr>
<tr>
<td>Should be</td>
<td>1</td>
<td>2</td>
<td>5</td>
<td>8</td>
</tr>
<tr>
<td>4.8%</td>
<td>9.5%</td>
<td>23.8%</td>
<td>38.1%</td>
<td>23.8%</td>
</tr>
</tbody>
</table>

* ‘Criminal communications’ referred to use of telecommunications by criminals to organise or plan their offending.
Table App P.1: Respondents views of police priorities for e-crimes (cont.)

<table>
<thead>
<tr>
<th>Priority</th>
<th>Police</th>
<th>Private Sectors</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>very low</td>
<td>low</td>
</tr>
<tr>
<td>Illegal online gambling</td>
<td>Current</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td>Should be</td>
<td>33.3%</td>
</tr>
<tr>
<td>Electronic money laundering or tax evasion</td>
<td>Current</td>
<td>42.9%</td>
</tr>
<tr>
<td></td>
<td>Should be</td>
<td>19.0%</td>
</tr>
<tr>
<td>Spam (unsolicited email)</td>
<td>Current</td>
<td>0.0%</td>
</tr>
<tr>
<td></td>
<td>Should be</td>
<td>13</td>
</tr>
<tr>
<td>Authoring computer viruses</td>
<td>Current</td>
<td>47.6%</td>
</tr>
<tr>
<td></td>
<td>Should be</td>
<td>42.9%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>14.3%</td>
</tr>
</tbody>
</table>

Source: McKenzie 2005, E-Crime Investigation Study [computer file#2], n=21 police, 46 private sector respondents. [cont.]
Table App P.1: Respondents views of police priorities for e-crimes (cont.)

<table>
<thead>
<tr>
<th>Priority</th>
<th>Police</th>
<th>Private Sectors</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>very low</td>
<td>low</td>
</tr>
<tr>
<td>Illegal interception of digital information</td>
<td>Current 6</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>Should be 1</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>Current 4.8%</td>
<td>23.8%</td>
</tr>
<tr>
<td>Denial of service attacks</td>
<td>Current 38.1%</td>
<td>23.8%</td>
</tr>
<tr>
<td></td>
<td>Should be 14.3%</td>
<td>14.3%</td>
</tr>
<tr>
<td>Theft of proprietary / confidential information</td>
<td>Current 38.1%</td>
<td>19.0%</td>
</tr>
<tr>
<td></td>
<td>Should be 4</td>
<td>3</td>
</tr>
<tr>
<td>Online Auction fraud</td>
<td>Current 19.0%</td>
<td>14.3%</td>
</tr>
<tr>
<td></td>
<td>Should be 28.6%</td>
<td>14.3%</td>
</tr>
<tr>
<td></td>
<td>14.3%</td>
<td>9.5%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Issue</th>
<th>Current</th>
<th>Should be</th>
<th>very low</th>
<th>low</th>
<th>some</th>
<th>high</th>
<th>very high</th>
<th>no answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Theft of telecommunications services (“phreaking”)</td>
<td>17 (25.4%)</td>
<td>10 (14.9%)</td>
<td>20 (29.9%)</td>
<td>19 (28.4%)</td>
<td>5 (7.5%)</td>
<td>2 (3%)</td>
<td>4 (6%)</td>
<td></td>
</tr>
<tr>
<td>Theft of electronic funds</td>
<td>5 (7.5%)</td>
<td>0 (0%)</td>
<td>2 (3%)</td>
<td>20 (29.9%)</td>
<td>24 (35.8%)</td>
<td>13 (19.4%)</td>
<td>3 (4.5%)</td>
<td></td>
</tr>
<tr>
<td>Electronic vandalism (eg defaced websites)</td>
<td>19 (28.4%)</td>
<td>5 (7.5%)</td>
<td>20 (29.9%)</td>
<td>13 (19.4%)</td>
<td>8 (11.9%)</td>
<td>3 (4.5%)</td>
<td>4 (6%)</td>
<td></td>
</tr>
<tr>
<td>Credit card fraud (including “phishing” scams)</td>
<td>6 (9%)</td>
<td>1 (1.5%)</td>
<td>15 (22.4%)</td>
<td>23 (34.3%)</td>
<td>9 (13.4%)</td>
<td>13 (19.4%)</td>
<td>4 (6%)</td>
<td></td>
</tr>
<tr>
<td>Advance fee scams (eg, Nigerian email scams)</td>
<td>21 (31.3%)</td>
<td>12 (17.9%)</td>
<td>16 (23.9%)</td>
<td>14 (20.9%)</td>
<td>8 (11.9%)</td>
<td>4 (6%)</td>
<td>4 (6%)</td>
<td></td>
</tr>
<tr>
<td>Identity theft &amp; fraud (eg counterfeit documents)</td>
<td>5 (7.5%)</td>
<td>2 (3%)</td>
<td>17 (25.4%)</td>
<td>19 (28.4%)</td>
<td>17 (25.4%)</td>
<td>3 (4.5%)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Defamation online</td>
<td>33 (49.3%)</td>
<td>16 (23.9%)</td>
<td>13 (19.4%)</td>
<td>10 (14.9%)</td>
<td>5 (7.5%)</td>
<td>3 (4.5%)</td>
<td>3 (4.5%)</td>
<td></td>
</tr>
<tr>
<td>Unauthorised access to computer</td>
<td>18 (26.9%)</td>
<td>6 (9%)</td>
<td>17 (25.4%)</td>
<td>16 (23.9%)</td>
<td>7 (10.4%)</td>
<td>5 (7.5%)</td>
<td>4 (6%)</td>
<td></td>
</tr>
<tr>
<td>Dissemination of offensive content (eg child porn, racial hatred)</td>
<td>4 (6%)</td>
<td>1 (1.5%)</td>
<td>6 (9%)</td>
<td>12 (17.9%)</td>
<td>22 (32.8%)</td>
<td>19 (28.4%)</td>
<td>4 (6%)</td>
<td></td>
</tr>
<tr>
<td>Cyber-stalking</td>
<td>10 (14.9%)</td>
<td>2 (3%)</td>
<td>13 (19.4%)</td>
<td>17 (25.4%)</td>
<td>17 (25.4%)</td>
<td>6 (9%)</td>
<td>4 (6%)</td>
<td></td>
</tr>
</tbody>
</table>

[cont.]
Table App P.2: Combined views of police priorities for e-crimes (cont.)

<table>
<thead>
<tr>
<th>Issue</th>
<th>Current</th>
<th>Should be</th>
<th>Current</th>
<th>Should be</th>
</tr>
</thead>
<tbody>
<tr>
<td>Digital piracy (eg. software, music, multimedia)</td>
<td>29 (43.3%)</td>
<td>20 (20.9%)</td>
<td>7 (10.4%)</td>
<td>2 (3%)</td>
</tr>
<tr>
<td></td>
<td>16 (23.9%)</td>
<td>11 (16.4%)</td>
<td>4 (6%)</td>
<td>2 (3%)</td>
</tr>
<tr>
<td></td>
<td>10 (14.9%)</td>
<td>20 (20.9%)</td>
<td>24 (35.8%)</td>
<td>11 (16.4%)</td>
</tr>
<tr>
<td></td>
<td>4 (6%)</td>
<td>4 (6%)</td>
<td>12 (17.9%)</td>
<td>20 (30.9%)</td>
</tr>
<tr>
<td></td>
<td>4 (6%)</td>
<td>4 (6%)</td>
<td>3 (4.5%)</td>
<td>2 (3%)</td>
</tr>
<tr>
<td>Digital extortion (a demand accompanied by a threat)</td>
<td>6 (9%)</td>
<td>1 (1.5%)</td>
<td>6 (9%)</td>
<td>1 (1.5%)</td>
</tr>
<tr>
<td></td>
<td>13 (19.4%)</td>
<td>7 (10.4%)</td>
<td>16 (25.4%)</td>
<td>8 (12.4%)</td>
</tr>
<tr>
<td></td>
<td>15 (22.4%)</td>
<td>14 (22.4%)</td>
<td>16 (25.4%)</td>
<td>20 (30.9%)</td>
</tr>
<tr>
<td></td>
<td>14 (22.4%)</td>
<td>14 (22.4%)</td>
<td>20 (30.9%)</td>
<td>8 (12.4%)</td>
</tr>
<tr>
<td></td>
<td>2 (3%)</td>
<td>7 (10.4%)</td>
<td>3 (4.5%)</td>
<td>5 (7.5%)</td>
</tr>
<tr>
<td>Criminal communications*</td>
<td>25 (37.3%)</td>
<td>15 (22.4%)</td>
<td>25 (37.3%)</td>
<td>15 (22.4%)</td>
</tr>
<tr>
<td></td>
<td>17 (25.4%)</td>
<td>14 (20.9%)</td>
<td>17 (25.4%)</td>
<td>20 (30.9%)</td>
</tr>
<tr>
<td></td>
<td>17 (25.4%)</td>
<td>20 (20.9%)</td>
<td>2 (3%)</td>
<td>20 (30.9%)</td>
</tr>
<tr>
<td></td>
<td>3 (4.5%)</td>
<td>27 (40.3%)</td>
<td>3 (4.5%)</td>
<td>3 (4.5%)</td>
</tr>
<tr>
<td>Electronic money laundering or tax evasion</td>
<td>23 (34.3%)</td>
<td>6 (9%)</td>
<td>8 (11.9%)</td>
<td>4 (6%)</td>
</tr>
<tr>
<td></td>
<td>15 (22.4%)</td>
<td>11 (16.4%)</td>
<td>20 (20.9%)</td>
<td>12 (18.2%)</td>
</tr>
<tr>
<td></td>
<td>7 (10.4%)</td>
<td>8 (11.9%)</td>
<td>8 (11.9%)</td>
<td>12 (18.2%)</td>
</tr>
<tr>
<td></td>
<td>1 (1.5%)</td>
<td>9 (13.4%)</td>
<td>5 (7.5%)</td>
<td>5 (7.5%)</td>
</tr>
<tr>
<td>Spam (unsolicited email)</td>
<td>46 (68.7%)</td>
<td>23 (34.3%)</td>
<td>46 (68.7%)</td>
<td>23 (34.3%)</td>
</tr>
<tr>
<td></td>
<td>10 (14.9%)</td>
<td>15 (22.4%)</td>
<td>2 (3%)</td>
<td>6 (9%)</td>
</tr>
<tr>
<td></td>
<td>12 (17.9%)</td>
<td>7 (10.4%)</td>
<td>4 (6%)</td>
<td>5 (7.5%)</td>
</tr>
<tr>
<td></td>
<td>9 (13.4%)</td>
<td>8 (11.9%)</td>
<td>1 (1.5%)</td>
<td>4 (6%)</td>
</tr>
<tr>
<td></td>
<td>4 (6%)</td>
<td>9 (13.4%)</td>
<td>4 (6%)</td>
<td>4 (6%)</td>
</tr>
<tr>
<td>Authoring computer viruses</td>
<td>26 (38.8%)</td>
<td>6 (9%)</td>
<td>26 (38.8%)</td>
<td>6 (9%)</td>
</tr>
<tr>
<td></td>
<td>12 (17.9%)</td>
<td>11 (16.4%)</td>
<td>12 (17.9%)</td>
<td>14 (20.9%)</td>
</tr>
<tr>
<td></td>
<td>12 (17.9%)</td>
<td>14 (16.4%)</td>
<td>9 (13.4%)</td>
<td>14 (20.9%)</td>
</tr>
<tr>
<td></td>
<td>9 (13.4%)</td>
<td>16 (23.9%)</td>
<td>4 (6%)</td>
<td>4 (6%)</td>
</tr>
<tr>
<td></td>
<td>4 (6%)</td>
<td>15 (22.4%)</td>
<td>4 (6%)</td>
<td>4 (6%)</td>
</tr>
<tr>
<td>Illegal interception of digital information</td>
<td>17 (25.4%)</td>
<td>5 (7.5%)</td>
<td>17 (25.4%)</td>
<td>5 (7.5%)</td>
</tr>
<tr>
<td></td>
<td>20 (29.9%)</td>
<td>11 (16.4%)</td>
<td>12 (17.9%)</td>
<td>17 (25.4%)</td>
</tr>
<tr>
<td></td>
<td>12 (17.9%)</td>
<td>17 (25.4%)</td>
<td>9 (13.4%)</td>
<td>17 (25.4%)</td>
</tr>
<tr>
<td></td>
<td>5 (7.5%)</td>
<td>21 (31.3%)</td>
<td>7 (10.4%)</td>
<td>21 (31.3%)</td>
</tr>
<tr>
<td>Denial of service attacks</td>
<td>22 (32.8%)</td>
<td>5 (7.5%)</td>
<td>22 (32.8%)</td>
<td>5 (7.5%)</td>
</tr>
<tr>
<td></td>
<td>15 (22.4%)</td>
<td>7 (10.4%)</td>
<td>15 (22.4%)</td>
<td>7 (10.4%)</td>
</tr>
<tr>
<td></td>
<td>16 (23.9%)</td>
<td>17 (25.4%)</td>
<td>8 (11.9%)</td>
<td>17 (25.4%)</td>
</tr>
<tr>
<td></td>
<td>8 (11.9%)</td>
<td>18 (26.9%)</td>
<td>2 (3%)</td>
<td>18 (26.9%)</td>
</tr>
<tr>
<td></td>
<td>5 (7.5%)</td>
<td>14 (20.9%)</td>
<td>4 (6%)</td>
<td>14 (20.9%)</td>
</tr>
<tr>
<td>Theft of proprietary / confidential information</td>
<td>16 (23.9%)</td>
<td>5 (7.5%)</td>
<td>16 (23.9%)</td>
<td>5 (7.5%)</td>
</tr>
<tr>
<td></td>
<td>15 (22.4%)</td>
<td>7 (10.4%)</td>
<td>15 (22.4%)</td>
<td>7 (10.4%)</td>
</tr>
<tr>
<td></td>
<td>19 (28.4%)</td>
<td>17 (25.4%)</td>
<td>8 (11.9%)</td>
<td>17 (25.4%)</td>
</tr>
<tr>
<td></td>
<td>8 (11.9%)</td>
<td>18 (26.9%)</td>
<td>5 (7.5%)</td>
<td>18 (26.9%)</td>
</tr>
<tr>
<td></td>
<td>4 (6%)</td>
<td>14 (20.9%)</td>
<td>4 (6%)</td>
<td>4 (6%)</td>
</tr>
<tr>
<td>Online Auction fraud</td>
<td>15 (22.4%)</td>
<td>4 (6%)</td>
<td>15 (22.4%)</td>
<td>4 (6%)</td>
</tr>
<tr>
<td></td>
<td>14 (20.9%)</td>
<td>14 (20.9%)</td>
<td>20 (29.9%)</td>
<td>20 (29.9%)</td>
</tr>
<tr>
<td></td>
<td>20 (29.9%)</td>
<td>13 (19.4%)</td>
<td>8 (11.9%)</td>
<td>13 (19.4%)</td>
</tr>
<tr>
<td></td>
<td>11 (16.4%)</td>
<td>11 (16.4%)</td>
<td>6 (9%)</td>
<td>6 (9%)</td>
</tr>
</tbody>
</table>

* ‘Criminal communications’ meant use of ICT by criminals to plan their offending.
Appendix Q: Forms for ISPs & online merchants to report incidents

### INTERNET SERVICE PROVIDER

**Report re Credit Card Fraud**

<table>
<thead>
<tr>
<th>ISP DETAILS</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>ISP Name :</td>
<td>Address :</td>
</tr>
<tr>
<td>Contact Name :</td>
<td>Phone :</td>
</tr>
<tr>
<td>Contact e-mail :</td>
<td>Fax :</td>
</tr>
</tbody>
</table>

Name of employee making statement and :  
authorised to give evidence as a witness :

A draft statement is it to be forwarded with the report (Soft format please Word-97)  
Attached :  Y / N

<table>
<thead>
<tr>
<th>ACCOUNT OPENING DETAILS</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name :</td>
<td>Opened :  /  /</td>
</tr>
<tr>
<td>Surname :</td>
<td>First Names :</td>
</tr>
<tr>
<td>Street Address :</td>
<td>DOB :  /  /</td>
</tr>
<tr>
<td>Suburb :</td>
<td>State :</td>
</tr>
<tr>
<td>Phone No:</td>
<td>Postcode :</td>
</tr>
<tr>
<td>Credit Card No:</td>
<td>Bus / Mobile No :</td>
</tr>
<tr>
<td>Type:</td>
<td>Fax No :</td>
</tr>
</tbody>
</table>

Name on Credit Card :  
Other Relevant Information :

<table>
<thead>
<tr>
<th>APPLICATION VALIDATION</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>List all steps taken to validate the credit card number? :</td>
<td></td>
</tr>
</tbody>
</table>

List all steps taken to validate Name and Address of applicant? :

Applicant’s contact telephone no. verified by - CLI:  (Y / N)  
Call back :  (Y / N)  
White Pages:  (Y / N)  
Other  (Provide Details) :

Name of ISP employee who spoke with applicant :  
Date :  /  / |

List any other steps taken to validate applicant’s details :

A search has been conducted to identify other accounts opened with this credit card number  (Y / N)

<table>
<thead>
<tr>
<th>HOW DETECTED</th>
<th></th>
</tr>
</thead>
</table>
| How was offence detected? :  
(Circle as appropriate)  |

Internal Investigation / Complaint from CC Holder / Bank Reversal

Contacted by the legitimate Credit Card holder :  (Y / N)  
Holder’s Name & Address:  
Contact No/s:

<table>
<thead>
<tr>
<th>DOCUMENTATION ATTACHED</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>All account opening details are attached :</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Account usage logs, including CLI information, is attached :  (Provided in Excel 97 format where possible)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>If more than one - a list of POP’s used to access account is attached :</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Phone subscriber details relevant to suspects are attached :</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# INTERNET SERVICE PROVIDER

*Report re Unauthorised Account Usage*

## ISP DETAILS

<table>
<thead>
<tr>
<th>ISP Name</th>
<th>Address</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Contact Name</th>
<th>Phone</th>
<th>Fax</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Contact e-mail</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name of employee making statement and authorised to give evidence as a witness</th>
</tr>
</thead>
<tbody>
<tr>
<td>A draft statement is to be forwarded with the report (Soft format please Word-97)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Attached</th>
</tr>
</thead>
<tbody>
<tr>
<td>Y / N</td>
</tr>
</tbody>
</table>

## ACCESSED ACCOUNT DETAILS

<table>
<thead>
<tr>
<th>User Name</th>
<th>Opened</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>/</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Surname</th>
<th>First Names</th>
<th>DOB</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>/</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Street Address</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Suburb</th>
<th>State</th>
<th>Postcode</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Phone No</th>
<th>Bus / Mobile No</th>
<th>Fax No</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## ACCESS DETAILS

List all steps taken to validate User identity on log on:

Were safeguards other than Username and Password breached? (Y/N)

(Provide details):

What safeguards other than Username and Password are in place to prevent unlawful access?

(Provide details):

What was the CLI/CND telephone number used for the unauthorised access?

Has any other account been accessed by the above telephone number? (Y/N)

(Provide details):

## HOW DETECTED

How was the unauthorised access detected?: Internal Investigation / Complaint from Account Holder / Other

(If other please supply details)

## DOCUMENTATION ATTACHED

<table>
<thead>
<tr>
<th>All account opening details:</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account usage logs for the relevant period: (Provided in Excel 97 format where possible)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>All captured CLI/CND information: (Provided in Excel 97 format where possible)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>List of all POP's used to access the account:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Phone subscriber details relevant to suspect telephone numbers:</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## OTHER RELEVANT INFORMATION
**INTERNET ONLINE MERCHANT**  
*Report re Credit Card Fraud*

### MERCHANT DETAILS
- **Merchant Name:**  
- **Address:**
- **Contact Name:**  
- **Phone:**  
- **Fax:**
- **Contact e-mail:**
- **Name of employee making statement and:**
  - **authorised to give evidence as a witness:**
  - Attached: Y / N
  - A draft statement is to be forwarded with the report (Soft format please Word-97)

### ACCOUNT OPENING DETAILS
- **User Name:**
- **Surname:**  
- **First Name(s):**  
- **DOB:**
- **Street Address:**
- **Suburb:**
- **State:**
- **Postcode:**
- **Phone No:**
- **Bus / Mobile No:**
- **Fax No:**
- **Credit Card No:**
- **Type:**
- **Expiry Date:**
- **Name on Credit Card:**
- **Other Relevant Information:**

### APPLICATION VALIDATION
- List all steps taken to validate the credit card number? :
- List all steps taken to validate Name and Address of applicant? :
- Applicant’s contact telephone no. verified by - CND: (Y/N) Call back: (Y/N) White Pages: (Y/N) Other (Provide Details):
- Name of employee who spoke with applicant (if applicable): Date: / /
- List any other steps taken to validate applicant’s details :
- Search conducted to identify other accounts opened/purchases made with this credit card number (Y/N)

### HOW DETECTED
- **How was offence detected?**
  - Internal Investigation / Complaint from CC Holder / Bank Reversal
  - (Circle as appropriate)
- **Contacted by the legitimate Credit Card holder:** (Y/N)
- **Holder’s Name & Address:**
- **Contact No/s:**

### DOCUMENTATION ATTACHED
- **All account opening details are attached:**
- **Account usage logs, including server log information, is attached:** (Provided in Excel 97 format where possible)
- **Captured IP is:**

---

521
This page blank intentionally
Appendix R: EFTA Mission and objectives

Mission Statement:

EFTA aims to build a professional collective to proactively share our knowledge, create partnerships and build public awareness of our services to the community.

Objectives:

1. Develop and promote the EFTA as the premier organisation of professional computer forensic investigators in Australasia through professional co-operation and communication between public and private bodies.
2. Establish a standard of professional conduct incorporated in a code of ethics to uphold the trust given to our profession.
3. Promote prevention and awareness of Electronic/Technological based crime / fraud;
4. Promote and assist in the professional development of EFTA members and Associates with peer-reviewed assessment on subject matters / topic of relevance.
5. Develop, implement and facilitate cross learning partnership arrangements with law enforcement and regulatory agencies.
6. Foster relationships between the EFTA and other bodies with similar aims in order to discuss matters or exchange information of common interest or concern.
7. Provide a united and unbiased response to public debate on issues affecting the E-Crime & Forensic investigative profession.
8. Foster fellowship, professional development and practice by establish standards of professionalism within the Institute by organising workshops, seminars, and providing lectures on topics concerning the industry.
9. Provide a member skills matrix database for the benefit of Institute members and Law Enforcement Agencies.
10. Take remedial and disciplinary action against members and associates where appropriate.
Abbreviations

ACC  Australian Crime Commission
ACCF  Australasian Crime Commissioners’ Forum
ACMA  Australian Communications and Media Authority
ACPO  Association of Chief Police Officers, UK
ACPR  Australasian Centre for Policing Research
AFP  Australian Federal Police
AHTCC  Australian High Tech Crime Centre
AIC  Australian Institute of Criminology
AIPD  Australian Institute of Professional Detectives
AIPI  Australian Institute of Professional Investigators
ANZSIC  Australian and New Zealand Standard Industrial Classification
ASCED  Australian Standard Classification of Education
AusCERT  Australian Computer Emergency Response Team
AUSTRAC  Australian Transaction Reports and Analysis Centre
BFSO  Banking and Financial Services Ombudsman
CIU  Criminal Investigation Unit, previously CIB, Criminal Investigation Bureau
CCS  Computer Crime Squad of Victoria Police
CDEB  Central Data Entry Bureau of Victoria Police
CERT  Computer Emergency Response Team
COAG  Council of Australian Governments
CUSCAL  Credit Union Services Corporation (Australia) Limited
DCITA  Department of Communications, Information Technology and the Arts
DHEAG  Department Human Ethics Advisory Group
DCPC  Drugs and Crime Prevention Committee, Parliament of Victoria.
DDoS  distributed denial of service
DRDoS  distributed reflector denial of service
DSD  Defence Signals Directorate
DTS  Detective Training School
e-crime  Electronic crime
EFA  Electronic Frontiers Australia
EFT  Electronic Funds Transfer
EFTA  Electronic Crime and Forensic Technology Association
FIC  Field Investigators Course
HREC  Human Research Ethics Committee
HTML  Hypertext Mark up Language
IACIS  International Association of Computer Investigative Specialists
IACP  International Association of Chiefs of Police
IAFCI  International Association of Financial Crime Investigators
ICAC  New South Wales Independent Commission Against Corruption
ICH  Internet Content Host
ICT  information and communication technology
IP  Internet Protocol
IRC  Internet Relay Chat
ISP  Internet Service Provider, also know as Internet Access Provider or IAP
JBFSIT  Joint Banking and Finance Sector Investigation Team of the AHTCC
LEAP  Law Enforcement Assistance Program of Victoria Police
MCCOC  Model Criminal Code Officers Committee of the Standing Committee of Attorneys-General
MFID  Major Fraud Investigation Division of Victoria Police
MMORPG  Massively Multiplayer Online Role Playing Game
MOU  Memorandum of understanding
NCA  National Crime Authority
NCCJS  National Centre for Crime and Justice Statistics
NPRU  National Policing Research Unit, now titled the Australian Centre for Policing Research
NSW  New South Wales
OPI  Office of Police Integrity, Victoria
PERL  Practical Extraction and Reporting Language
PGP  Pretty Good Privacy
PIN  Personal identification number
POLSEC  Victoria Police Security Industry Partnership Committee
PPP  Public-private partnership
RCC  Research Coordinating Committee of Victoria Police
TAFE  Technical and Further Education institution
TIO  Telecommunications Industry Ombudsman
VPM  Victoria Police Manual
VPN  Virtual Private Network
VSI  Victorian Security Institute
<table>
<thead>
<tr>
<th>Glossary</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anton Piller</td>
<td>Under British and British-derived legal systems, an order granted by courts to search premises and inspect or seize items without prior notice to the respondent; effectively a civil search warrant, with more restrictions than criminal search warrants.</td>
</tr>
<tr>
<td>blended attack</td>
<td>an attack that combines and automates methods, for example mixing propagation characteristics of viruses, worms and Trojans and exploiting vulnerabilities.</td>
</tr>
<tr>
<td>bot</td>
<td>abbreviation of “robot”, also known as software agents or spiders, referring to software that runs autonomously to achieve some purpose.</td>
</tr>
<tr>
<td>botnet</td>
<td>a collection of bots, capable of remote control and thus use in distributed denial of service attacks.</td>
</tr>
<tr>
<td>bulletin board system</td>
<td>electronic version of a noticeboard, where users can read and post messages, upload and download files and sometimes chat.</td>
</tr>
<tr>
<td>chose in action</td>
<td>“An intangible personal property right which is incapable of physical possession and can only be claimed or enforced by a legal or equitable action” (Encyclopedic Australian Law Dictionary).</td>
</tr>
<tr>
<td>click-kiddies</td>
<td>the generation of criminal hackers who are skilled only to utilise intrusion tools that require mere clicking of a mouse; also describes automated intrusion software. The previous generation was known as script-kiddies, who simply copied others’ programs.</td>
</tr>
<tr>
<td>cracking</td>
<td>to subvert digital copyright and registration protections of software enabling free use and unlimited copying; also to obtain and decrypt passwords.</td>
</tr>
<tr>
<td>electronic crime</td>
<td>an act prohibited by criminal law in which a digital technology, such as a computer, is used as:</td>
</tr>
<tr>
<td></td>
<td>- the tool in the commission of an offence;</td>
</tr>
<tr>
<td></td>
<td>- the target of an offence; or</td>
</tr>
<tr>
<td></td>
<td>- the storage medium for illicit data or information (Etter, 2000).</td>
</tr>
</tbody>
</table>
grooming conditioning a child to engage in sexual activities, whether online or in person; often involves befriending the child and desensitisation to pornography. Prohibited by Sexual Offences (Protection of Children) Amendment Act 2003 (Qld) and Crimes Legislation Amendment (Telecommunications Offences and Other Measures) Act (No. 2) 2004 (Cth).

hack back to counter-attack a hacking attempt with hacking.

incident an occurrence of an offence; where a member of Victoria Police records an event (or “matter”) in the LEAP database it becomes an “incident” (Carcach & Makkai, 2002: x).

keylogger device or software that records a user’s keystrokes and mouse clicks for later retrieval.

man in the middle hacking technique for interception and manipulation of electronic information without the sender or receiver noticing; for example, faking login pages for public wireless Internet hotspots.

Mareva injunction Under British and British-derived legal systems, an order granted by a civil court to freeze assets or property.

MD5 hash The “message digest 5” algorithm invented by Ronald Rivest that produces a 128-bit “fingerprint” of a file used in forensic computing to verify the integrity of files.

mule person undertaking low-level, courier activities in relation to organised crime. In terms of phishing scams, person who makes Internet banking transfers on the pretext of legitimate employment as a ‘money transfer agent’.

offence an act prohibited by legislation, of which a particular instance is referred to as an “incident” once recorded.

page-jacking hijacking of World Wide Web pages such that a user visits a different site instead of visiting their intended site.

pharming outgrowth of phishing, where hackers redirect all traffic from a legitimate site to a fake site. It can be
performed at the user’s computer through malicious software or by changing the records of Domain Name Servers.

**phishing** a type of fraud that uses faked email correspondence and websites to trick people into disclosing their personal details, such as banking passwords, to permit electronic theft of funds and identity theft.

**shoulder surfing** watching another person enter their password to then misuse that information.

**steganography** process of concealing data within other data, eg text hidden within an image file.

**sub-incidents** all offences attached to an incident and recorded in LEAP (Carcach & Makkai, 2002: x).

**telescoping** an error of memory affecting research where recent events are considered farther back in time or vice versa.

**zero-day exploit** an attack that takes advantage of a software vulnerability on the same day it is discovered and thus before it becomes known to computer security professionals or the public.

**zombies** computers that have been taken over as part of a distributed denial of service attack.
Index of authors

@Mark: 432
Abbey, N.: 7, 58, 77
ABC Local Radio: 51
Akindemowo, O.: 13, 216
Alexandra, A.: 8, 72
Association of Chief Police Officers (UK): 46
Australian Bureau of Statistics: 26, 112, 123, 283
Australian Centre for Policing Research: 37, 46, 48, 65, 77, 269
Australian Crime Commission: 31
Australian Federal Police: 36, 37
Australian High Tech Crime Centre: 236
Australian Institute of Criminology: 102, 147
Australian Institute of Professional Detectives: 303
Australian Institute of Professional Investigators: 49, 75
Australian Media and Communication Authority: 35
Ayres, I.: 88, 371
Balfour, C.: 7
Banking and Financial Services Ombudsman: 370
Bavinton, F.: 15
Bayley, D.: 6, 23, 81, 93
Bell, D.: 77
Benedict, R.: 72
Berinato, S.: 369, 432
Best, J.: 53
Beuger, M.E.: 62, 205
Blackler, J.: 8, 72
Blayney, J.: 3
Bode, K.: 369
Boggan, S.: 54, 384
Bon, N.: 112, 214
Bottoms, A.: 95, 96, 97, 98
Braithwaite, J.: 88, 353, 354, 357, 358, 371
Brankovic, L.: 9
Brereton, D.: 22
Broucek, V.: 101
Butcher, S.: 313
Butten, D.: 7, 77
Button, M.: 6, 23, 24, 43, 58, 83, 239
Calhoun, J.A.: 67, 71
Callahan, D.: 76
Campbell, D.: 30
Campbell, D.T.: 30, 97, 103
Carca, C.: 129, 193, 519, 520
Casey, E.: 19, 33, 46, 52, 119
Cha, A.E.: 30
Chan J.: 22
Chan, H.K.H.: 51, 52, 101, 144, 186, 189–90, 267
Chandler, A.: 20
Cherney, A.: 5, 88, 344
Chulov, M.: 36
Clarke, R.: 14
Clarke, R.V.: 90, 376
Cochrane, N.: 4, 47
Cohen, H.: 8, 72, 73, 74, 96, 353, 364, 365
Cohen, L.E.: 90, 102
Cook, T.: 97, 103
Cornish, D.B.: 90, 376
Council of Australian Governments: 32
Covey, S.R.: 270
Crawford, A.: 63, 64, 88, 298
D’Ambra, F.: 59
Dadds, V.: 76
Davids, C.: 23, 58, 60, 63, 64, 321, 382, 383, 384
D’Eco, E.: 23, 58, 60, 63, 64, 321, 382, 383, 384
de Bono, E.: 270
de Waard, J.: 26
Deacons: 190
Deering, A.: 61, 67, 68, 69, 87, 282, 351, 360, 365
Defence Signals Directorate: 120
Delattre, E.J.: 8, 72
Dempsey, G.: 6, 94, 216, 349
Department of Communications, Information Technology and the Arts: 19
Department of Justice and Finance: 73
Deputy Ombudsman (Police Complaints) Victoria: 49
Detroit Free Press: 192
Doran, S.: 22
Dormody, T.J.: 189, 214, 215
Doss, D.: 53
Douglas, J.: 4, 383
Dowling, J.: 107
Dreyfus, S.: 13, 27, 28, 30, 41, 49
Subject index

AusCERT, 41, 104, 187, 311, 313, 327, 333, 335
Computer Crime and Security survey, 3, 10, 18, 21, 102, 122
Australia described, 26
Australian High Tech Crime Centre, 36–38, 104, 109, 120, 125, 192, 223, 235, 261, 270, 368, 389
Joint Banking and Finance Sector Investigation Team, 11, 38, 104, 125, 243, 272, 286, 308–18, 336, 340, 380–81
Computer Crime Squad. See Victoria Police
coopetition, 310, 380
defined, 62
crime prevention, 89–90
and routine activity approach, 90
applied to investigative partnerships, 372–76
defined, 26
criminal investigation points of proof, 29
e-crime investigation
evidence packages, 207–13
in Victoria, 150–71
factors affecting, 175–271
outsourcing of, 4, 339, 372, 375, 382–85, 390
referral to private sector, 5, 40, 275, 298, 319, 332–33, 339, 375, 382–85, 390
secondment for, 37, 104, 272, 308–21, 340, 373, 380
EFTA, 11, 105
electronic crime
cost of, 20, 143
defined, 16–17
distributed denial of service, 430–33
distributed reflector denial of service, 431
in Victoria, 130–50
jargon, 14–15, 16–17
pharming, 430
phishing, 426–30
taxonomies of, 16, 345–51, 348
theft of information, 216–17, 269, 356–57
e-policing, 22
ethics clearances, 108
juridification, 88, 363, 367, 370, 378
defined, 88
data demographics, 127–29, 498–511
model computer crime legislation, 32, 194–200, 269
Operation Auxin, 9, 38, 271, 367 partnership
as projects, 66–71
defined, 66
in e-crime policing strategy, 46–49
partnership policing, 1, 5, 57–92
accountability mechanisms, 78, 369–72
compared to community policing, 57–66
concerns about, 4–5, 49–55, 243
mechanisms of. see e-crime investigation
mutualism in, 7, 79–80, 95, 238, 344, 361–63, 362
normative standards for, 360–76
of e-crime, 283–92, 272–341
   LEAP data, 161–62
   problems of, 2–4
   public interest criteria, 71–80
policing
   defined, 22
POLSEC, 106–8, 272, 299, 308, 321,
   330, 340, 341, 364, 370, 379
   Code of Ethics, 365
documents, 447–49
Privacy Commissioner, 247
   Victorian, 246
privacy legislation, 294
   and search warrants, 247
   impact of, 244
private investigation
   Australian industry, 42–43
   industry associations, 45
private investigators, 44
   defined, 43
private police
   defined, 24
Regulated Intersections model, 9, 11,
   57, 84–91, 92, 293–303, 342
   evaluated, 343–45, 344, 389
   regulatory character of, 89
   regulatory character, 89, 343–45
defined, 88
relations between public and
private police, 80–92, 161, 238–
46, 270
descriptive models, 81–82, 84–85
normative models. see Regulated Intersections model, see
   partnership policing
   under-reporting, 184–88
responsibilisation, 5, 221, 268, 269,
   351, 352, 354
VFIRC, 39–40, 333–36, 385
victimisation surveys. see AusCERT
   Computer Crime and Security survey
   TruSecure survey, 20, 21
Victoria Police
   and headhunting, 261–64, 330,
   339, 366–67
   Computer Crime Squad, 28, 32,
   33–35, 34, 258–60, 271
   workload data, 153–60
   incident data. see LEAP
   reporting policies, 193, 201–7,
   268, 269, 270, 351–54
Virtual Global Taskforce, 39, 73,
   275, 365