11th International Anti-Corruption Conference
Different Cultures, Common Values
Seoul, Korea
27 May 2003
11.30am to 1.00pm

Stream 11 Workshop: Chipping Away at Corruption: Can we Rely on eGovernance?

eCorruption and Unmanaged Risk

Electronic Theft of Personal Information

Dr Russell G. Smith
Australian Institute of Criminology

Introduction

One of the emerging areas of risk of electronic corruption that transcends national boundaries concerns the misuse of personal information. The convergence of computing and communications technologies has greatly facilitated the dissemination of personal information across the globe, principally via the Internet and electronic mail. The rapid expansion of mobile communications and messaging services will greatly enhance the ability of people to spread personal information both quickly and cheaply for work and social purposes. Although still predominantly English-language based, the Internet now has users located throughout the globe communicating in many languages, and developing nations, in particular, are seeing dramatic growth in their use of on-line services (Smith and Urbas 2001).

Both government agencies and private sector entities are now making full use of these technologies, sometimes without adequate consideration having been given to their potential for misuse. With increasing amounts of data travelling electronically, risks of misappropriation, manipulation and misuse have become a feature of modern life.

One recent example of misuse of personal information that was reported in the media in England in March 2003 concerned a 72 year-old man, Derek Lloyd Sykes, whom the FBI were investigating in connection with alleged telemarketing fraud involving millions of dollars in the United States. Since 1989, Sykes had been making use of the identity of a 72-year old retired businessman from Bristol in England, Derek Bond, who had never met Derek Sykes, and had no connection with his alleged crimes at all.

The FBI issued a warrant for the arrest of Derek Sykes and this was executed by South African Police in Durban on 6 February 2003 in the name of Derek Bond. Unfortunately, Derek Bond, the retired businessman, who was on holiday with his wife, was arrested instead of Derek Sykes. The police relied on the fact that the warrant was in the name of Mr Bond, he was the correct age, looked similar, and had the same passport number.

Mr Bond was held in custody at police headquarters in Durban until 26 February 2003 when he was released following the arrest of the real suspect, Derek Sykes, the day before in Las Vegas. Mr Bond is now planning to sue the FBI for wrongful arrest and detention for three weeks in South Africa (BBC News 2003).

The case highlights the kinds of problems that arise when someone's personal information has been misappropriated for illegal purposes.

Increasing Use of Communications Technologies

As with most forms of crime, as opportunities for illegal conduct arise, so the number of crimes perpetrated increases. In the case of electronic crime, the opportunities created by the greatly expanding use of on-line services are substantial. Moreover, increased distribution of transactions across jurisdictions, networks and Internet sites reduces the potential for systematic regulatory initiatives to be used.

In Australia, there were 571 Internet Service Providers (ISPs) supplying Internet access services to 4.2 million active subscribers at the end of March 2002. Of the 4.2 million Internet subscribers in Australia at the end of March 2002, there were 3.7 million household subscribers and 505,000 business and government subscribers. There were 1,234 million megabytes (Mbs) of data downloaded by Internet subscribers during the March quarter 2002, which is an average of 290 Mbs per subscriber. Of this, household subscribers downloaded 713 million Mbs (average of 191 Mbs per household subscriber) and business and government subscribers downloaded 520 million Mbs (average of 1,010 Mbs per business and government subscriber) (Australian Bureau of Statistics 2002).

These quantities of data are considerable when one considers that one thousand pages of text approximates to one megabyte of data (1,234 million megabytes of data would correspond to some 1,234,000 billion pages of text). Of course, much of this would comprise images and video files. A single JPEG image could contain up to 3 megabytes of data.

In the Asia-Pacific region, information technology industries are developing rapidly and although individual countries have varying policies on access to and use of technologies such as the Internet, use of the Internet is expanding quickly. Recent research predicts that the Asia-Pacific region will soon have more Internet users than either the United States or Western Europe (Dataquest 2001; see also IDC 1999).

In Korea, the information technology market is large and has been estimated to be worth $US194 billion a year. The Korean Software Industry Association estimates that more than a third of Korean homes have broadband access (Sinclair 2001). In South Korea, the Internet is experiencing a period of spectacular growth with the number of users increasing from three million to sixteen million in less than two years. The 2001 figure has been estimated at 22.3 million, making the Korean Internet market the world's fourth largest, behind the United States, Japan and Germany (Nielsen NetRatings 2001). Thirty-five percent of South Korean Internet users buy online at least once every three months

(Yankee Group 2001). Nearly nine per cent of the population has traded shares on-line (Korea Times 2001). The government has also created 'Cyber Korea 21', an investment plan of the equivalent of more than nine billion Euros, to increase connectivity and to improve infrastructure (Reporters Sans Frontières 2001).

The market research and consultancy service eTForecasts, predicts that there will be over 1 billion Internet users in the world by the year 2005. Of six regions considered alongside the United States, it is predicted that the Asia-Pacific region will become the largest Internet usage region with 242 million Internet users in 2005 (Figure 1).

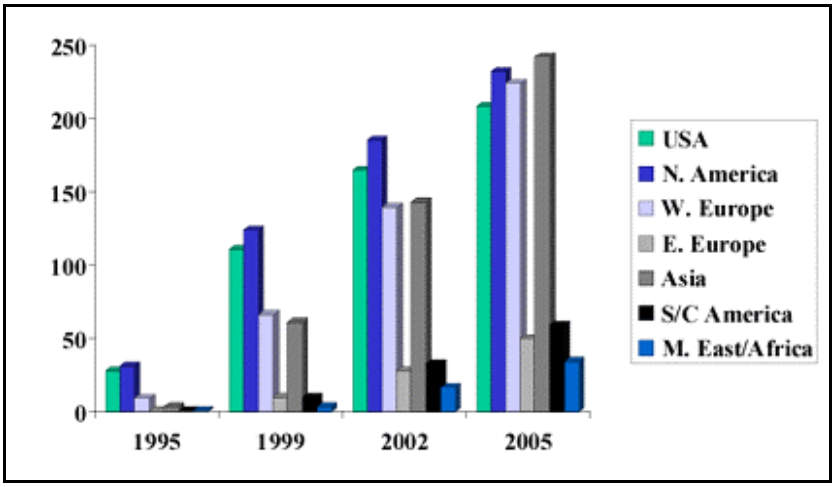

Figure 1: Internet Usage by Region 1995-2005
Source: eTForecasts (2001)

The Extent of the Problem

Each year, a number of surveys are conducted of the fraud risks associated with conducting on-line activities.

In early 2002, the Computer Security Institute and the FBI's Computer Intrusion Squad based in San Francisco released the seventh *Computer Crime and Security Survey* (Computer Security Institute 2002). This was a survey of over 500 computer security practitioners in corporations, government agencies, financial institutions, medical institutions and universities in the United States. Ninety per cent of respondents (primarily large corporations and government agencies) detected computer security breaches within the preceding 12 months, up from 85% the previous year. Eighty per cent acknowledged financial losses due to computer breaches (64% the year before). Forty-four per cent (223 respondents) provided quantification of their financial losses, which came to US$455,848,000. The year before, 35% (186 respondents) reported total losses of US$377,828,700, and the losses from 249 respondents in the 2000 survey totalled only US$265,589,940. The average annual loss reported over the three years prior to 2000 was US$120,240,180.

As in previous years, the most serious losses occurred through theft of proprietary information and financial fraud. For the fifth year in a row, more respondents (74%) cited their Internet connection as a frequent point of attack than cited their internal systems as a frequent point of attack (33%). Thirty-four per cent of respondents reported the intrusions to law enforcement. In 2001 the figure was 36%; 25% in 2000; and just 16% in 1996).

In terms of reported incidents relating to electronic commerce, the survey found that of the 98% of respondents who maintained web sites, 38% suffered unauthorised access or misuse within the preceding 12 months, while 21% said that they did not know if there had been unauthorised access or misuse of their sites. Twenty-five per cent of those acknowledging attacks reported between two and five incidents while 39% reported 10 or more incidents. Twelve percent reported theft of transaction information, and 6% claimed financial fraud (8% in 2001, 3% in the 2000 survey).

In the United States during 2001, the Internet Fraud Complaint Centre, organised by the United States Department of Justice and the Federal Bureau of Investigation, received 49,711 complaints relating to Internet fraud, 16,775 of which were referred to other authorities for further action. The average (median) monetary loss per referred complaint was US$435.00, with 43% of complaints relating to auction fraud (Internet Fraud Complaint Centre 2002).

The Federal Trade Commission's fraud database 'Consumer Sentinel', which compiles identity theft and consumer fraud data from United States and Canadian agencies, recorded over 200,000 complaints in 2001 (Federal Trade Commission 2002). This compares with 18,600 complaints in 1999, and 8,000 in 1998 (Department of Justice, United States 2000).

Finally, in a telephone survey of 1,006 online consumers conducted for the National Consumers League in the United States between April and May 1999, 24% said they had purchased goods and services online. However 7%, which represents 6 million people, said that they had experienced fraud or unauthorised use of credit card or personal information online (Louis Harris and Associates Inc 1999).

One of the most recent studies of identity fraud in Australia was conducted by the Australian Bureau of Criminal Intelligence (2002)(now part of the Australian Crime Commission) in 2002. In the pilot study, 23 law enforcement and other public sector agencies, and one private sector organisation provided information relating to identity fraud offenders, fraudulent identities and victims of identity takeovers known to them.

The study found that between 25 February 2002 and 23 August 2002, 1,195 fraudulent identities were identified relating to 597 suspects and involving 1,404 documents. 1,183 cases involved fraudulent identities, 12 cases involved identity takeovers, and 12 involved known identity fraud offenders. In all, 1,404 offences were identified in which $2,639,797 had been obtained and a further $239,532 attempted to be stolen.

The study found that fraudulent identities were used to support or to commit a variety of criminal activities such as obtaining finance, opening bank accounts, money laundering, car re-birthing, credit card skimming, obtaining family allowance benefits, obtaining security guard licences, boat licences and shooters' licences, avoiding driving demerit points and producing English language certificates for migrants.

The Nature of the Problem

There are many opportunities that exist within both the public and private sectors for digital information to be misused for personal and business gain. The following examples illustrate the range and diversity of ways in which computers have facilitated the commission of information-related crimes.

Theft of Government Information

The are many opportunities for Government employees to steal information by obtaining unauthorised access to computers, copying data, and selling the copies to third parties. In Australia, for example, charges were laid against an employee of the Australian Department of Social Security (DSS) following the removal of a large quantity of records from the Department's database. Details of individuals held on the database were sold to a private investigator who sold them on to insurance companies (Australian Federal Police 1996, p. 20). In 1996, an employee of the DSS, a former police detective, was sentenced to 200 hours community service and fined $750 in Sydney after he was found guilty of unlawfully gaining access to and disclosing DSS information (Australian Federal Police 1997, p. 30).

Also in Australia, some years ago, the New South Wales Independent Commission Against Corruption (1992) investigated employees of the national telecommunications carrier, Telecom (as it then was), who had sold confidential government information to private investigators.

Government employees have access to and make use of various forms of intellectual property in connection with their employment. Copyright, patents, trademarks, designs and certain other specific rights may all be used without authority. The greatest area of risk, however, lies in government-owned software being downloaded and used on personal computers for private purposes.

The possibility also exists that government employees may sell confidential, sensitive information obtained in the course of their employment. Although this has always been a risk, particularly in matters involving national defence, the use of computers to discover information, such as through hacking, or to transmit information obtained illegally, makes the problem potentially much worse.

Government employees are also in a position to steal computer equipment which often contains valuable software and sometimes sensitive information. In one recent

investigation undertaken by the Australian Federal Police, a government department was the victim of a series of thefts of computers containing sensitive information. A number were recovered and three individuals charged. The department in question has since undertaken a review of its security and employee screening procedures to prevent similar incidents occurring (Australian Federal Police 1998, p. 43).

Laptop computers are particularly attractive targets for thieves, not only because of their portability, but also because of the information which they hold. One computer insurance company in Columbus, Ohio, received 309,000 claims in respect of stolen laptop computers and 100,000 claims in respect of desktop computers in 1997, worth US$1.3 billion in all (Denning 1998).

Another Australian incident involved the Australian Taxation Office's Website, GST Assist, that was established following the introduction of Australia's new taxation system, being compromised. A student known variously as K2 and Kelly exposed a glaring security breach in the Website. Simply by typing in a string of numbers, K2 was able to gain access to the records of more than 20,000 GST-registered providers, which contained their bank account details. He alerted more than 17,000 of the providers by sending their confidential details to them by E-mail (Dancer 2000, p. 76).

Electronic procurement carries risks of fraud and abuse through internal controls being removed when new electronic procurement systems are introduced. Government agencies are particularly vulnerable in view of the extensive procurement activities in which they engage, and the large sums of money involved. In one Australian case, for example, in New South Wales, a sub-contractor to a local Council allegedly gained access to the Council's database of tendering information and was able to secure numerous contracts through the use of this information (Bell 2000, p. 31).

Theft of Financial Information

One of the most attractive targets for criminals in recent years has been credit card account details and other personal information used in commercial on-line transactions. Sometimes, security information such as passwords and account details can be obtained by gaining access to databases held by businesses or financial institutions. On other occasions, insiders may move funds electronically by sending instructions via electronic mail. As the use of electronic commerce becomes more widespread, abuses relating to the transfer of funds electronically can be expected to increase.

In one case, for example, two individuals who worked for a computer training company, Aptech, in India, allegedly sent electronic mail messages in the name of Microsoft and Videsh Sanchar Nigam (India's overseas telephone service provider) that contained an attachment which, when opened, sent messages back to the accused containing passwords and other data from the State Bank of India. Both were arrested and charged under India's Information Technology Act 2000 with hacking which carries a maximum penalty of three years' imprisonment and 200,000 rupees fine (US$4,300)(Bloomberg News 2001).

An example of a recent case of abuse of credit card information disclosed in an unencrypted E-mail message, involved a New Zealand consumer who had purchased a book from Amazon.com. The woman had purchased a book with her debit card and gave her cell phone number as a contact number. The book arrived, but a few days later, she found her debit card had been used to make a number of unauthorised purchases from companies in Portugal, Indonesia and Brazil. All of the charges included the information she had given only to Amazon.com, namely, her card number, address and cell phone number. She also discovered that five new accounts had been opened with her details (Slane 2001).

The so-called Citibank case is one of the most prominent cases involving misuse of financial information. Between June and October 1994, a group of Russian computer hackers attempted to steal approximately US$10.7 million from various Citibank customers' accounts in the United States by manipulating its computerised funds transfer system. One offender, Vladimir L. Levin, was working in a Russian firm, and gained access over 40 times to Citibank's funds transfer system using a personal computer and stolen passwords and account identification numbers. Using a computer terminal in his employer's office in St Petersburg, he authorised transfers of funds from Citibank's head office in New Jersey to accounts which he and his co-conspirators held in California, Finland, Germany, the Netherlands, Switzerland, and Israel.

After protracted legal proceedings which went to the House of Lords, he was extradited to stand trial before the Federal District Court in New York's Southern District. On 24 February 1998, he pleaded guilty to conspiracy to defraud and was sentenced to thirty-six months' imprisonment and to pay Citibank US$240,015 in restitution. Citibank was able to recover all but $240,000 of the $10.7 million worth of illegally transferred funds. None of the bank's depositors lost money and since the fraud was discovered, Citibank required customers to use an electronic password generator for every transfer of funds. The consequences for Citibank's business reputation were, however, considerable (R. v *Governor of Brixton Prison*; *Ex parte Levin* [1996] 3 WLR 657; *In re Levin* House of Lords, 19 June 1997).

Identity Theft

Digital technologies make it relatively simple to disguise one's identity. Electronic mail and Internet addresses may be manipulated by including details which are misleading or the source of a message may be made anonymous or changed so that it appears to be coming from another user. Similarly, there is no way of knowing the commercial affiliations of those on the Internet. Referees for organisations might, in fact, be individuals employed specifically to indicate their approval of the organisation in question.

It is also possible to choose legitimate-sounding names in order to improve one's credibility or include domain names which are misleading (see Bachner and Jiang 2000). There has recently developed a practice in the United States and Canada, for example, of

some organisations adopting domain names containing the names of Australian cities in order to improve their credibility, despite the fact that they have no connection at all with Australia.

An example of a recent identity theft case that made use of the Internet concerned 200 of America's richest people who were victimised by a 32 year-old New York chef, Abraham Abdallah. Abdallah was alleged to have used computers in a public library to obtain millions of dollars from the accounts of billionaires such as George Soros, Steven Spielberg, talk show host Oprah Winfrey, former presidential candidate Ross Perot, George Lucas and Ted Turner. Abdallah allegedly obtained information from credit reference companies by forwarding letters, purporting to be from major banks, requesting information. He used answering machines, courier drop-offs and E-mail accounts to discover enough information to take over the electronic identity of his victims (Ringin 2000). He was only detected when he sent an E-mail message to Merrill Lynch pretending to be billionaire Thomas Siebel, asking for US$10 million to be transferred to an Australian account. Merrill Lynch was concerned that the transfer would overdraw his account and contacted Siebel (Broughton, 2001).

In Japan, the Internet was used by an offender to advertise the availability of bank accounts he had opened using false identities. In September 1999, Osaka police arrested a 31-year-old man, Teruhiko Ikeda, on suspicion of having used forged health insurance certificates to open bank accounts in false names. He allegedly sold the bank accounts through the Internet to enable his customers to use the accounts to perpetrate fraud and other crimes. In May 1998, Ikeda allegedly instructed his accomplice, Kyuzo Takehara, to open five accounts at a bank in Kyoto under a false identity by using forged health insurance certificates. Some 50 accounts at banks in Tokyo and Kyoto were opened in a similar way and then sold on the Internet. Both Ikeda and Takehara were arrested for alleged forgery and use of private documents (Japan Times Online 1999).

Identity fraud also lies at the heart of many cases involving illegal movement of funds from government agencies to offenders. In one case, on 25 September 2001, a financial consultant formerly contracted to the Department of Finance and Administration was convicted of defrauding the Australian government by transferring $8.7 million electronically to private companies in which he held an interest. He did this by logging on to the Department's computer network using another person's name and password. He was also able to obscure an audit trial through the use of other employees' logon codes and passwords. He was sentenced to 7 years and six months' imprisonment with a non-parole period of 3 years and six months (R v *Muir*, ACT Supreme Court, 25 September 2001).

The latest forms of identity theft have involved the cloning or duplication of entire Websites. In New South Wales, for example, a case was investigated in which the offenders copied official Web sites of premier entertainment venues, including the Sydney Opera House, in respect of almost every detail, including theatre layouts and restaurant information. Programs were constantly up-dated to maintain the façade of legitimacy. The crucial difference was that the fictitious site had its own credit card

booking arrangement, so that customers' money would be credited to the offender's account. The bogus site for Sydney appeared on the Internet with a similar URL to the genuine site. The offenders created 23 similar sites mirroring opera houses in Europe, including Paris and Vienna. The computer crime unit of the New South Wales Police Commercial Crime Agency contacted the FBI after tracing the bogus site to a Miami Internet server. Since then, the server has re-located to California (Kennedy 2002). Similar so-called Website mirroring cases have involved on-line banking sites with the potential for extensive losses.

Theft of Intellectual Property

Computers can also be used to make illegal copies of data in breach of copyright laws. Any type of data transmission can be copied with the greatest concerns relating to audio and visual data such as music and films. As broadband services continue to become available with text, graphics, sound, and video information being freely accessible via cable modems, the potential for copyright infringement involving such works will be enhanced enormously. It is now possible, for example, to download compact disks and feature films from the Internet. According to the *Straits Times* (8 November 1999), a copy of the James Bond Film *The World is Not Enough*, was available free on the Internet before its official release.

The Business Software Alliance's (2001) annual survey of software piracy for 2000 found that the Asia-Pacific region was the only area globally to increase its rate of piracy since the study first commenced in 1994. Piracy rates were calculated by comparing the difference between software applications installed (demand) and software applications legally shipped (supply). The piracy rate was thus defined as the volume of software pirated as a percent of total software installed in each country.

Several large countries in Asia experienced increases in their piracy rates in 2000. For example, China's rate increased to 94 per cent while Korea's rate increased to 56 per cent. Vietnam, with a piracy rate at 97 per cent, continued as the country with the highest piracy rate in the region. In terms of the dollar value lost to piracy, the survey found that in 2000 the Asia-Pacific region sustained the highest percentage of losses (Figure 2) of all regions owing to its having an extensive PC and software market.

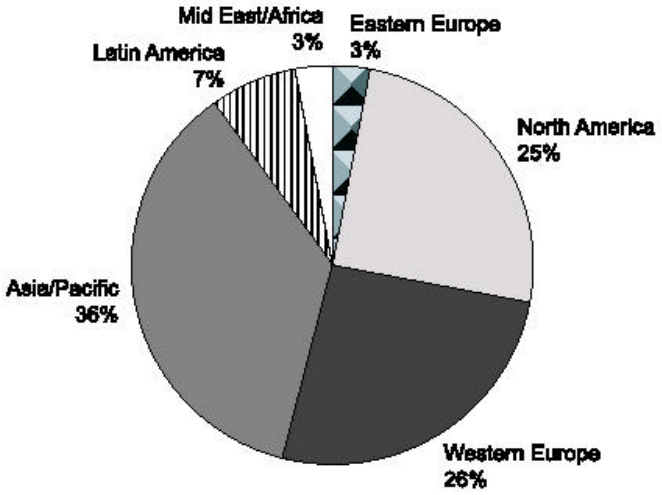

Figure 2. Percentage Dollar Losses Due to Software Piracy by Region
Source Business Software Alliance 2001, p. 4.

Theft of Health Information

Many countries are now using digital technologies to store and process medical records and health information. The processing of health benefits is now also done electronically in a number of countries. This extensive use of computers in health care, or what is know as 'tele-medicine' or 'tele-healthcare' raises a number of concerns relating to information security (Smith 2002).

In Britain, the government's proposal to have a fully-networked health records system failed principally through concerns over confidentiality. On 26 November 1995, the *Sunday Times* revealed how confidential medical records of prominent people had been obtained illegally from National Health Service staff and doctors' surgeries for £150, thus confirming predictions regarding the insecurity of on-line medical data banks (Rogers and Leppard 1995; Davies 1996: 63).

In the United States, a panel of the National Research Council some time ago identified a number of security risks associated with electronic patient records and recommended greater use of access restriction devices (Leary 1997). An example of such risks which took place in Pinellas County, Florida, involved the leak of a confidential computer disk which contained the names of almost 4,000 individuals suffering from AIDS (United States, General Accounting Office 1997).

Intercepted communications may also be used for commercial purposes. In one case in the United States, for example, a Bank Manager paid a health official to check computerised health records of loan applicants, thus requiring the official to breach confidentiality (Anonymous 1996). In another case, a banker on a state health commission obtained access to a list of all the patients in the state diagnosed as suffering

from cancer and cross-referenced it with the bank's client list. He then arranged for these patients' loans to be called in (Anonymous 1993).

Risks of corruption also arise in connection with the payment of health care providers. Risks relate to the possibility of electronic claim forms being counterfeited or manipulated electronically, digital signature keys being compromised, and electronic funds transfers being altered or diverted away from legitimate recipients (Smith 1999a). In Australia in 1997, for example, two former employees of the Health Insurance Commission (which provides health and medical benefits to doctors and the public) were convicted of defrauding the government by creating false provider accounts and making illegal claims to the combined value of more than A$45,000 (Health Insurance Commission 1997, Professional Review Supplement, p. 23).

Sometimes, misuse of electronic information can take place by accident. For example, data on thousands of patients of the University of Michigan health system were inadvertently made available on the Internet for a period of at least two months, until a student discovered the error by chance in February 1999 (Upton 1999). The lapse occurred when the hospital was developing a new patient-scheduling system. The company installing was given access to what was thought to be a secure server, but the data were discovered by a student seeking to locate a physician.

Electronic Extortion

Digital technologies are also being used to carry out acts of criminal extortion, which can have substantial consequences. In one case, two individuals from Kazakhstan were arrested in London on 20 August 2000, for allegedly having broken into the computer network of Bloomberg LP, in Manhattan, in an attempt to extort money from the company. The arrest was made following a joint operation between the FBIs New York Field Office, the Metropolitan Police in London and authorities in Kazakhstan (Federal Bureau of Investigation 2000).

Another Australian case involved a 27 year old male, known as 'Optik Surfer', who was sentenced to three years' imprisonment (with 18 months' suspended) on 27 March 1998 in Sydney, for eight counts of obtaining unlawful access to a computer and one count of unlawfully inserting data into a computer. The offender, who was a computer networking consultant, had been refused employment with an ISP in January 1994, and in March 1994 took revenge by illegally obtaining access to the company's computer network using the user account and password of the company's technical director. He then gained access to the company's database of 1,225 subscribers and publicised their credit card account details by disclosing them to various journalists and also by altering the company's Home Page on 17 April 1994 by including a message that the company's security system had been compromised. The publicity resulted in the company losing more than A$2 million in lost clients and contracts. It was required to change its business name and sold the Internet access part of its business to another ISP (R. v *Stevens* unreported decision of the NSW District Court, 27 March 1998; appeal to the NSW Criminal Court of Appeal dismissed on 15 April 1999 [1999] NSWCCA 69).

In a United States prosecution, two Russian computer hackers, Vasily Gorshkov and Alexey Ivanov allegedly stole large numbers of credit card details and attempted to extort money from account holders (*United States* v *Gorshkov* 2001 WL 1024026, No. CR-550C (W.D. Wash 23 May 2001).

Finally, in one case in England, information passing over a Bank's computer network was stolen through the use of electromagnetic radiation scanning techniques, and even though the information was encrypted, the code was broken and the bank and various customers blackmailed by threatening to disclose information to the taxation authorities unless the sum of £350,000 was paid (Nicholson 1989).

Electronic Stalking

Communications technologies have also been used to stalk or to harass people, often in other countries. In such cases, the theft of an E-mail address lies at the heart of a sometimes lengthy period of harassment.

A recent case that illustrates this question concerned a resident of Melbourne in Victoria who was accused of stalking a woman in Canada by sending letters and E-mail messages and using the telephone and the Internet. The Canadian woman complained to police in Toronto who referred the case to the Victoria Police. When the case came before a Magistrate in Melbourne, the accused argued that the effect of his activities, if any, was in Canada and not in Victoria and so the court had no jurisdiction to hear the charges. The Magistrate agreed and dismissed the charges deciding that the fear or apprehension had to be experienced in Victoria for Victorian law to apply. The Director of Public Prosecutions appealed against the decision and the Supreme Court held that the legislation did have extra-territorial effect and that the defendant could be dealt with in Victoria even though the victim was located in Canada (*DPP* v *Sutcliffe* [2001] VSC 43 (1 March 2001, Gillard J).

In another case, a man allegedly stole photographs of his naked former girlfriend and her new boyfriend and posted them on the Internet, along with her name, address and telephone number. The unfortunate couple, residents of Kenosha, Wisconsin, received phone calls and e-mails from strangers as far away as Denmark who said they had seen the photos on the Internet. Investigations also revealed that the suspect was maintaining records about the woman's movements and compiling information about her family (Spice and Sink 1999).

In another case a rejected suitor posted invitations on the Internet under the name of a 28-year-old woman, the would-be object of his affections, that said that she had fantasies of rape and gang rape. He then communicated via email with men who replied to the solicitations and gave out personal information about the woman, including her address, phone number, details of her physical appearance and how to bypass her home security system. Strange men turned up at her home on six different occasions and she received many obscene phone calls. While the woman was not physically assaulted, she would not

answer the phone, was afraid to leave her home, and lost her job (Miller and Maharaj 1999).

One former university student in California used email to harass 5 female students in 1998. He bought information on the Internet about the women using a professor's credit card and then sent 100 messages including death threats, graphic sexual descriptions and references to their daily activities. He apparently made the threats in response to perceived teasing about his appearance (Associated Press 1999).

Theft of Private Information

Finally, digital technologies have also greatly facilitated the theft of private information about individuals, whether in the form of photographic images or private communications (see Grabosky, Smith and Dempsey 2001). The advent of digital cameras, for example, allows images to be recorded clandestinely of famous as well as ordinary people going about their daily activities. Candid photographs taken with hidden cameras in public lavatories are now accessible to anyone with a computer and a modem, while the use of concealed cameras by male patrons of shopping malls in the United States has attracted police attention (Davis 1998).

Prominent people often go to great lengths to avoid photographers, whether simply because they wish to be left alone, or because they are concerned that embarrassing photos will be published. Were they alive today, Jacqueline Kennedy Onassis and Princess Diana could describe not only the harassment they experienced at the hands of paparazzi, but also the discomfort of seeing one's unflattering image on the front page of a tabloid newspaper, or a private telephone conversation broadcast publicly (Grabosky, Smith and Dempsey 2001).

Bernstein (1996) recounts a case involving inmates of a correctional facility at Lino Lakes, Minnesota, who compiled an extensive data base on children from the surrounding area. The prisoners, who had access to information technology through a prison-based computer programming and telemarketing business, scanned children's photographs and collated other information from local newspapers. The annotated files on local children contained information regarding which girls took piano lessons, who had entered children's beauty contests, and also included descriptions of children's physique. In addition there were annotations on some files referring to "latchkey kids" "cute" "Little Miss pageant winner" and the existence of "speech difficulties." The towns in which the children lived were alphabetised and coded with map co-ordinates (Grabosky, Smith and Dempsey 2001).

Whether these data were collected purely for purposes of voyeurism or fantasy, for the planning of subsequent criminal activity following release, or were compiled for sale to child molesters, one can see how ostensibly innocent public information may be gathered, collated, and subject to misuse.

Regulatory Responses

Policy Framework

In the early 1990s, the large western democracies began introducing national policy frameworks designed to enhance electronic communication and to facilitate the growth of electronic commerce (Braithwaite and Drahos 2000, pp. 340-1). In September 1993, for example, the United States government released its National Information Infrastructure Agenda for Action (NII). By February 1995, this policy framework had become the Global Information Infrastructure (GII). These initiatives have been taken up by other advanced countries globally. They have sought to liberalise telecommunications sectors globally and to harmonise regulatory measures in order to facilitate the spread of electronic commerce.

Individual countries have begun building their own policies for the expansion of information technology and the use of electronic commerce. In 1994, for example, Australia introduced its information infrastructure policy entitled *Networking Australia's Future*, while the United States released its policy paper entitled *A Framework for Global Electronic Commerce* in 1997.

In the Asia-Pacific region, the Chinese government has expressed its desire to develop the Internet as the number of users in the country doubles every six months. Over the past two years, the Chinese authorities have considerably changed their policy on controlling the Internet. The 'Great Cyber Wall' strategy, implemented in 1997, by the Ministry of Public Security and the Ministry of State Security, was abandoned in favour of selective enforcement and control carried out by ISPs and site managers themselves. Provincial governments have a certain level of autonomy in implementing Internet control policies. In the spring of 2000, for example, authorities in the Hubei province temporarily closed a site that published information about a financial scandal involving the vice-governor of the province (Reporters Sans Frontières 2001).

South Korea was one of the first countries in the world to adopt a law regulating the broadcasting and viewing of on-line information. Since 1995, the Electronic Communication Business Law has led to the creation of an Information and Communication Ethics Office—a public body that reviews sites, discussion forums and chat rooms, and can recommend that certain sites be blocked. South Korea's national security law also covers the Internet and forbids South Koreans from having any contact with their North Korean neighbours (Reporters Sans Frontières 2001).

Fraud control policies are also now increasingly being used in both the public and private sectors. In Australia, for example, the fraud victimisation survey conducted by Deakin University in 1994, found that 27 per cent of those surveyed had fraud prevention policies in place (Deakin University 1994). In November 1995, the 48 per cent of the 123 Australian respondents to Ernst and Young's fraud survey had a fraud prevention policy in place and 51 per cent had conducted fraud reviews (Ernst and Young 1996). In Ernst and Young's (1998) subsequent fraud survey, almost three quarters of the 84

Australian respondents indicated that their organisation had an explicit policy on fraud reporting (1998).

One half of the respondents to KPMGs Global eFraud survey (2001) had incident response procedures in place to deal with security breaches of their electronic commerce systems—although of those respondents who had procedures in place, 43 per cent had procedures that included computer forensic response guidelines to deal with wilful intrusions into their networks and to ensure proper gathering of evidence. Over 50 per cent of the Asia-Pacific respondents—from each of Australia, Hong Kong and India—all had procedures in place to deal with security breaches, somewhat higher than in other countries.

Various standards have been designed to assist business and government in the creation and use of fraud control measures. Australian Standard No. AS 3806-98 Compliance Programs, for example, provides guidelines for both private and public sector organisations on the establishment, implementation, and management of effective compliance programs. The Standard also provides principles which organisations are able to use to identify and to remedy any deficiencies in their compliance with laws, industry codes, and in-house company standards, and to develop processes for continuous improvement in risk management (Standards Australia 1998).

Many public sector agencies now maintain policies designed to prevent and control economic crime. The Commonwealth of Australia's *Fraud Control Guidelines*, for example, outline principles and standards of fraud control (Commonwealth Attorney-General's Department 2002). Although the policy relates only to Commonwealth Government departments, and does not encompass any enforcement function, it provides a consistent set of directions to assist departments in carrying out their responsibilities to combat internal fraud. These include agency responsibilities for fraud prevention, reporting of fraud information, investigation case handling, and training of investigators.

There has also been recognition in recent times of the need to create an ethical environment in the workplace by educating employees of all levels about the desirability of complying with laws and codes of practice.

Policies, however, need to be established to deal with specific computer-related matters such as Internet fraud. Both businesses and government agencies should establish guidelines, for example, on the allocation and use of passwords, on access to and use of the Internet for private purposes, personal use of E-mail, downloading government software, the use of copyright material, and reporting of inappropriate conduct. In Australia in March 2000, the Office of the Federal Privacy Commissioner (2000) published guidelines on workplace E-mail, web browsing and privacy. These guidelines aim to assist public sector agencies in developing appropriate workplace practices regarding the use of information technologies by employees. They generally require openness in agencies communicating with staff about what is, and what is not permitted in the workplace. They also require agencies to inform staff about the nature and extent

to which their computer-related activities are logged and who in the organisation has access to the logged information.

Codes of Practice

In addition to having fraud control policies in place as part of a general risk management strategy, codes of practice are able to provide not only a widely disseminated statement of existing laws and acceptable practices which help to create a culture of compliance within specific industries, but also often include dispute resolution procedures and sanctions for non-compliance with the rules in question.

In December 1997, the Australian Ministerial Council on Consumer Affairs released the Direct Marketing Model Code of Conduct to regulate the conduct of those involved in the direct-selling industry. The Code is administered by the Australian Direct Marketing Association (ADMA) which was established in 1966 as the peak industry body for companies and individuals engaged in direct marketing in Australia, and applies to telemarketing, mail-order and Internet sales. Membership of ADMA is open to corporations, organisations, charities and partnerships, whilst individuals are able to join as Associate members. In 1996, ADMA began providing a training program in competency-based direct marketing at certificate and diploma levels.

All ADMA members must undertake to abide by the voluntary Direct Marketing Code of Practice published by the Association which seeks to ensure that direct marketing engaged in by members complies with the highest standards of integrity. The 'Standards of Fair Conduct' within the Code govern the making of an offer, identification of the advertiser, the use of incentives, the placing of orders, fulfilment orders and the use of mailing and telephone lists. Arrangements are also made for the arbitration of disputes and members agree to comply with all legal requirements governing their activities.

The Code also specifically refers to direct marketing carried on electronically such as via the Internet. The Code states, for example:

Clear, complete and current information about the identity of businesses engaged in electronic commerce and about the goods and / or services they offer, should be provided to customers. Additional information should be provided to address particular aspects of digitised goods and services, such as technical requirements or transmission details (cl. D2).

In addition, in Australia, an Internet Code of Conduct has been created to deal specifically with business-to-consumer electronic commerce transactions. The code, *Building Consumer Sovereignty in Electronic Commerce: A Best Practice Model for Business* (Department of Treasury, Consumer Affairs Division 2000), builds on the recommendations of the Council of the Organisation for Economic Co-operation and Development (OECD, 1999) concerning guidelines for consumer protection in the Context of Electronic Commerce. These OECD recommendations include a set of general guidelines to protect consumers participating in electronic commerce without

erecting barriers to trade. They represent a recommendation to governments, businesses, consumers, and their representatives as to the core characteristics of effective consumer protection for electronic commerce.

The Australian Best Practice Model sets out the responsibilities of businesses that trade online and provides guidance to businesses to enhance consumer sovereignty by giving consumers information on what businesses should do when dealing with consumers over the Internet. The Best Practice Model aims to increase consumer confidence in business-to-consumer electronic commerce and provides guidance to industry and consumers on the elements of an effective self-regulatory framework. The Model provides guidance on fair business practices; advertising and marketing; disclosure of a business's identity and location; disclosure of a contract's terms and conditions; the implementation of mechanisms for concluding contracts; the establishment of fair and effective procedures for handling complaints and resolving disputes; adopting privacy principles; using and disclosing information about payment, security and authentication mechanisms; and the processes and policies necessary to administer a code based on the Best Practice Model.

Information and Education

Once policies have been established they need to be communicated to staff and fully explained in order to prevent misunderstandings as to their meaning and effect. Often policies are established but not adequately implemented or publicised.

Providing educational material concerning fraud prevention and reporting procedures on internal agency Websites is also now widely used in the public sector. In the survey conducted by the Australian National Audit Office (2000, p. 48) of commonwealth fraud control arrangements, approximately thirty per cent of agencies used E-mail, and thirty-five per cent of agencies used their Intranet or public databases to disseminate fraud control information to staff.

In addition, direct E-mail fraud reporting facilities can be used, although if anonymity is required then telephone hotlines or even anonymous paper-based reporting may be preferable.

Of particular importance is the need to provide information to staff on aspects of computer security along with appropriate guidelines on reporting computer misuse and abuse. Many jurisdictions now have public interest disclosure legislation which aims to ensure that those who report illegal conduct are not disadvantaged by their conduct. In the case of computer-based illegality, as in other areas of crime, severe penalties could be imposed on individuals who engage in, or attempt or conspire with others to carry out acts of reprisal against those who disclose illegality in the public interest. To date such remedies have rarely been used.

A delicate balance needs to be struck between providing information to staff about the computer security measures that have been adopted to prevent fraud, and keeping such information private so as not to alert potential fraudsters to the security measures that

they will need to circumvent in order to perpetrate fraud. Unfortunately, experience has shown that it is often upper level staff who already have knowledge of an agency's security measures who are most likely to commit computer-related fraud. This raises the need for agencies to monitor the activities of staff at all levels regularly, without unduly infringing personal privacy.

Technological Responses

In terms of target hardening, a wide range of technological solutions have been devised in order to reduce the risks of misuse of information in both the public and private sectors. Some of the key areas to consider are as follows.

Hardware Security

Agencies need to ensure that computer hardware is adequately secured by using appropriate firewalls and other technologies in order to prevent external forms of attack. In KPMGs fraud survey (1999), poor physical security over computer equipment was found to be a common factor in allowing computer-related crime to occur.

User Authentication

Authentication of one's identity is crucial in preventing computer-based fraud. At present, most authentication procedures involve the use of passwords or PINs. Ensuring that these are used carefully and are not able to be compromised represents a fundamental fraud control measure. In addition to user education, a variety of innovative ideas have been developed to protect passwords and to enhance user authentication. Systems are available which change passwords regularly, or which deny access after a specified number of consecutive tries using invalid passwords. Terminals have been devised with automatic shutdown facilities which operate when they have not been used for specified periods. Single use passwords, where the password changes with every successive login according to an agreed protocol known to the user and system operator, are also available.

In the future, many user authentication systems will make use of so-called biometric identifiers which make use of an individual's unique physical characteristics. Common examples include fingerprints, voice patterns, typing patterns, retinal images, facial or hand geometry, and even the identification of a person's subcutaneous vein structures or body odours.

Although such systems achieve much higher levels of security than those which rely upon passwords, they are expensive to introduce and raise potential problems in terms of privacy and confidentiality of the personal data stored on government computer networks. An initiative designed to reduce social security fraud in Toronto has been the enactment of legislation which would enable welfare benefit recipients to use fingerprint authentication when dealing with the Ontario government in Canada. Detailed privacy protections are built into the legislation which includes requirements for all biometric

data to be encrypted and for the original biometric to be destroyed after the encryption process has been completed (Cavoukian 1999).

Allied to the need to authenticate the users of computers is the necessity to prevent individuals from fabricating or making use of other people's identities. Identity-related crime is a substantial problem which has become easier to perpetrate through the use of so-called desk-top publishing equipment (Smith 1999b). As public sector agencies continue to make use of electronic commerce and electronic procurement, the need to authenticate users' identities will become of critical importance. A report by the House of Representatives Standing Committee on Economics, Finance, and Public Administration (2000) recommended, *inter alia*, that the Australian Taxation Office improve its internal processes for establishing identity and preventing identity fraud and that the commonwealth government formalise a process for working with other levels of government and industry to develop options for reducing and preventing identity fraud. A wide range of technological solutions are also being trialed at present to address the problems associated with user authentication, and it remains to be seen which of these, or which combination of solutions, will be most effective.

Tracking and Surveillance

Employees' use of computers and their on-line activities can be monitored through the use of software which logs usage and allows managers to know, for example, whether staff have been using the Internet for non-work-related activities, or if funds are being moved to specified accounts for unauthorised purposes. Ideally, agreed procedures and rules should be established which enable staff to know precisely the extent to which computers are able to be used for private activities, if at all. If agencies do permit staff to make use of computers for private purposes, then procedures should be in place to protect privacy and confidentiality of communications, subject, of course, to employees obeying the law.

Where certain on-line activities have been prohibited, many government agencies now monitor the activities of their employees, sometimes covertly such as through video surveillance or checking E-mail and files transmitted through servers. Filtering software may also be used to prevent staff from engaging in certain behaviours. 'Surfwatch', for example, can be customised to deny employees access to specified content. When the employee requests a site, the software matches the user's ID with the content allowable for the assigned category, then either loads the requested page, or advises the user that the request has been denied. The software also logs denied requests for later inspection by management. Although this can be an effective risk management tool for managers, it is possible to by-pass filtering software by obtaining the password of the person who installs the software.

The use of computer software to monitor the business activities of government agencies also provides an effective means of detecting fraud and deterring individuals from acting illegally. The Australian Health Insurance Commission, for example, employs artificial neural networks to detect inappropriate claims made by health care providers and

members of the public in respect of various government-funded health services and benefits. In 1997-98, this technology contributed to the HIC locating $7.6 million in benefits which were paid incorrectly to providers and the public (Health Insurance Commission 1998).

In addition, revenue authorities are able to make use of information derived from financial transaction reporting requirements to identify suspicious patterns of cash transactions which could involve illegality or money laundering. In Australia, in 1997-98, the Australian Taxation Office attributed more than $47 million in revenue assessed to its direct use of information provided by the Australian Transaction Reports and Analysis Centre. In one case, a taxpayer and associated entities had transferred more than $1.3 million to a tax haven. Following an investigation, more than $6 million in undeclared income was detected (AUSTRAC 1999).

Deterrence Through Prosecution and Punishment

Finally, theft of personal information can be dealt with through the traditional processes of prosecution and punishment.

In this often highly technological area, law enforcement agencies invariably need specially trained units to handle investigations. In some cases, forensic accountants from the private sector may be engaged by police fraud squads to carry out investigations, or part of investigations. In other cases, independent statutory anti-corruption agencies may take action; and they, too, may need to develop expertise in this area. In New South Wales, for example, the Independent Commission Against Corruption is developing a new strategy, *Project Mercury*, to deal with electronic corruption and already a number of its investigations have involved cases of electronic fraud (Bell 2000).

Taking criminal action in cases involving electronic fraud is neither simple nor quick. Financial considerations have also meant that only the most serious cases involving substantial monetary losses are likely to be fully investigated and tried, with the attendant possibility of convicted offenders receiving the most severe sanction of a term of imprisonment. The legal response to fraud control has, therefore, been severely restricted, although the possibility of criminal prosecution and sanction has always remained open.

In addition to conventional judicial punishments such as fines and imprisonment, there are a variety of other consequences which may follow the detection of fraudulent conduct. These include adverse publicity, professional disciplinary sanctions, civil action, injunctive orders and, most recently, various forms of reconciliation or community conferencing. The confiscation of an offender's assets represents an effective means of deterrence as long as such sanctions receive wide publicity. Both adverse publicity and forms of reintegrative shaming can be effective in public sector workplaces where reputations are important. One form of this which has been found to be effective in reducing the extent to which staff use the Internet for unauthorised purposes, involves

employers publicising details of Web sites visited by their staff and naming the staff in question.

Although conducted independently of any government department, in Australia, the operator of Internet sites which provided live, on-line sex shows, conducted a survey of her users and found that during business hours between 8 July 1999 and 30 June 2000, 1,186 individuals who connected to the sites had used 'gov.au' domain names. They came from a range of federal, state, and local government offices located throughout Australia. It is claimed that some 4,000 individuals have used government-provided facilities to gain access to sexually-explicit sites (see Sinclair 1999, Taylor 2000).

Conclusions

Computer technologies have greatly enhanced the ability of people to steal personal information. Many instances simply replicate traditional forms of information theft, but make use of computers to enhance the speed and efficiency with which they may be carried out. Others, are directed at computer systems themselves either through theft of hardware and software or by using computers to transfer funds illegally.

Probably the greatest source of risk lies in the area of user authentication. Identity-related crime has been a continuing problem for decades now and it is likely that it will continue, in adapted forms, in the on-line world. If passwords continue to be used to restrict access to computers then they should be protected by appropriate security devices. Biometric identifiers will, presumably, become much more widely accepted as electronic commerce develops. Less sophisticated measures should also be adopted to ensure that employees are not given passwords that permit them to gain access to parts of networks that are unrelated to their daily work.

In planning for the future, it will be necessary to ensure that the weak points in security protocols are not overlooked. As in other areas of fraud control, the weak points in information technology systems will invariably arise out of human factors rather than purely technological considerations.

Risk management and fraud prevention activities are clearly preferable to the use of criminal prosecution and punishment, although the use of the criminal justice system is still necessary in order to achieve general and specific deterrent effects. In the case of computer criminals who can be said to carry out their activities on the basis of some rational calculation, deterrence remains an important component of crime control.

The solutions to theft of information lie in a blend of risk management strategies, self help, legislative and regulatory reform, and in the appropriate use of technologies of security and crime prevention. Of key importance, however, is the need to ensure that any solutions that are adopted do not provide greater opportunities for abuse of individual and organisational integrity than existed prior to their introduction.

References

Anonymous 1993, 'RMs Need to Safeguard Computerised Patient Records to Protect Hospitals', *Hospital Risk Management*, vol. 9, pp. 16-19.

Anonymous 1996, 'Medical Records Face Hacker Risk', *Security Australia*, vol. 16, no. 10, p.18.

Associated Press 1999, 'Pyramid Schemes in Cyberspace: The Same Old Deal'. http://cnn.com/TECH/computing/9903/11/net.schemes.ap/ (visited 15 March 1999).

Australian Bureau of Criminal Intelligence 2002, *Identity Fraud Register Pilot: Final Report*, Australian Bureau of Criminal Intelligence, Canberra.

Australian Bureau of Statistics 2002, *Internet Activity*, (8153.0) March Quarter 2002, ABS, Canberra.

Australian Federal Police 1996, *Annual Report 1995-96* Australian Government Publishing Service, Canberra.

Australian Federal Police 1997, *Annual Report 1996-97* Australian Government Publishing Service, Canberra.

Australian Federal Police 1998, *Annual Report 1997-98*, Australian GovernmentPublishing Service, Canberra.

Australian National Audit Office (ANAO) 2000, *Survey of Fraud Control Arrangements in APS Agencies*, Audit Report No 47, 1999-2000, Performance Audit, Australian National Audit Office, Canberra.

Australian Transaction Reports and Analysis Centre (AUSTRAC) 1999, 'Great Tax Results', *AUSTRAC Newsletter*, Spring, p.1.

Bachner, B. and Jiang, M. 2000, 'Governing trademarks in cyberspace: A comparative study of the regulation of domain names in China', *Asia Pacific Law Review*, vol.8, no.2, pp.191-209.

BBC News 2003, 'Briton May Sue After FBI Bungle', *BBC Online* 26 February.

Bell, C. 2000, *E-Corruption: Exploiting Emerging Technology Corruptly in the New South Wales Public Sector*: Unpublished Strategic Assessment, New South Wales Independent Commission Against Corruption, Sydney.

Bernstein, N. 1996, 'On Prison Computer, Files to Make Parents Shiver', *New York Times* 18 November, A1.

Bloomberg News 2001, 'Indian Techies Arrested in Bank Hacking Case', *CNET News*, 25 January. http://news.cnet.com/news/0-1003-200-4602814.html?tag=prntfr (visited 8 August 2001).

Braithwaite, J. and Drahos, P. 2000, *Global Business Regulation*, Cambridge University Press, Cambridge.

Broughton, P. D. 2001, *The Age (Melbourne)*, 22 March.
Business Software Alliance (BSA) 2001, *Sixth Annual BSA Global Software Piracy Study* http://www.bsa.org (visited 10 August 2001).

Cavoukian, A. 1999, 'Privacy and Biometrics', Paper presented to the 21st International Conference on *Privacy and Personal Data Protection*, Hong Kong, 13 September http://www.pco.org.hk/conproceed.html (visited 17 December 1999).

Commonwealth Attorney-General's Department 2002, *Commonwealth Fraud Control Guidelines*, 13 May 2002.
http://www.law.gov.au/aghome/commprot/crjd/LECD/guidelinesmay.htm (visited 12 October 2002).

Computer Security Institute 2002, '2002 CSI/FBI Computer Crime and Security Survey', *Computer Security Issues and Trends*, vol. 8 no. 1, Spring.

Dancer, H. 2000, 'K2 uncovers GST keyhole', *The Bulletin (Australia)*, 11 July, p.76.

Dataquest 2001, 'Asia to Become Largest Net Market', *NUA*, 7 August 2001: http://www.nua.ie/surveys/index.cgi?f=VS&art_id=905357053&rel=true (visited 7 August 2001).

Davies, S. 1996, *Monitor: Extinguishing Privacy on the Information Superhighway*, Sydney, Pan Macmillan Australia.

Davis, P. 1998, 'Peeping Toms with Videocams Plague Malls', *Seattle Times*, 9 June. http://archives.seattletimes.com/cgi-bin/texis.mummy/web/ vortex/display?storyID =36d4ca92f &query=internet+and+privacy (visited 14 June 1999).

Deakin University 1994, *Fraud Against Organisations in Victoria*, Deakin University, Geelong, Victoria.

Denning, D.E. 1998, 'Cyberspace Attacks and Countermeasures', in Denning, D. E. and Denning, P. J. *Internet Besieged: Countering Cyberspace Scofflaws*, ACM Press, New York, pp.29-55.

Department of Justice, United States 2000, *Internet Fraud: Appendix B*, Report of the Criminal Division's Computer Crime and Intellectual Property Section.
http://www.cybercrime.gov/append.htm (visited 5 July 2000).

Department of Treasury, Consumer Affairs Division, Australia 2000, *Building Consumer Confidence in Electronic Commerce: A Best Practice Model for Business*, Commonwealth of Australia, Canberra.

DPP v Sutcliffe [2001] VSC 43 Supreme Court of Victoria, 1 March 2001.

Ernst & Young 1996, *Fraud: The Unmanaged Risk*, Ernst and Young, London.

Ernst & Young 1998, *Fraud: The Unmanaged Risk*, Ernst and Young, London.

eTForecasts 2001, 'Internet User Forecasts by Country, Executive Summary' http://www.etforecasts.com/products/ES_intusers.htm (visited 15 August 2001).

Federal Bureau of Investigation 2000, *Press Release*, 14 August http://www.fbi.gov/pressrm/pressrel/pressrel100/vatis08142000.htm (visited 17 January 2001).

Federal Trade Commission, United States 2002, 'Sentinel Top Complaint Categories: January 1–December 31, 2001', Federal Trade Commission, January 7. http://www.consumer.gov/sentinel/images/charts/top2001.pdf (visited 10 October 2002).

Grabosky, P. N., Smith, R. G. and Dempsey, G. 2001, *Electronic Theft: Unlawful Acquisition in Cyberspace*, Cambridge University Press, Cambridge.

Health Insurance Commission 1997, *Annual Report 1996-97*, Australian Government Publishing Service, Canberra.

Health Insurance Commission 1998, *Annual Report 1997-98*, Australian Government Publishing Service, Canberra.

House of Representatives Standing Committee on Economics, Finance and Public Administration 2000, *Numbers on the Run: Review of the ANAO Report No. 37 1998-99 on the Management of Tax File Numbers*, Parliament of the Commonwealth of Australia, Canberra.

IDC 1999, 'Asia-Pacific Development Outpaces Europe', *NUA*, 14 April 1999: http://nua.ie/surveys/index.cgi?f=VS&art_id=905354838&rel=true (visited 10 August 2001).

Internet Fraud Complaint Center 2002, *IFCC 2001 Internet Fraud Report*. http://www1.ifccfbi.gov/strategy/IFCC_2001_AnnualReport.pdf (visited 12 October 2002).

Japan Times Online 1999, 'Man Arrested Over Bogus Bank Accounts', 13 September http://www.japantimes.co.jp/cgi-bin/getarticle.pl5?nn19990913a7.htm (visited 8 August 2001).

Kennedy, l. 2002, 'A Scam to Bring the House Down', *Sydney Morning Herald*, 'A Scam to Bring the House Down', 28 August. http://www.smh.com.au/articles/2002/08/27/1030053059530.html (visited 21 October 2002).

KPMG 1999, *1999 Fraud Survey*, KPMG, Sydney.

KPMG 2001, *Global e.fr@ud Survey*, KPMG Forensic and Litigation Services.

Leary, W. E. 1997, 'Panel Cites Poor Security on Medical Records', *New York Times Fax*, 6 March.

Louis Harris and Associates Inc. 1999, *Consumers and the 21st Century: A Survey Conducted for the National Consumers League*, Louis Harris and Associates Inc, New York.

Miller, G., and Maharaj, D. 1999, 'N. Hollywood man charged in 1st cyber-stalking case', *Los Angeles Times* 22 January. http://www.cs.csubak.edu/~donna/news/crime.html#stalking (visited 12 June 1999).

New South Wales Independent Commission Against Corruption 1992, *Report on Unauthorised Release of Government Information*, Sydney, ICAC.

Nicholson, E. 1989, 'Hacking Away At Liberty' , *Times (London)*, 18 April.

Nielsen NetRatings 2001, 'South Korea Dominates Asia in Internet Use', *NUA*, 14 March 2001: http://nua.ie/surveys/index.cgi?f=VS&art_id=905356555&rel=true (visited 10 August 2001).

Office of the Federal Privacy Commissioner 2000, 'Guidelines of the Commonwealth Privacy Commissioner on Workplace E-mail, Web Browsing and Privacy' 30 March, http://www.privacy.gov.au/issues/p7_4.html (visited 15 January 2001).

Organisation for Economic Co-operation and Development (OECD) 1999, *Recommendation of the Council of the OECD Concerning Guidelines for Consumer Protection in the Context of Electronic Commerce*, 9 December 1999, OECD, Paris http://www.oecd.org//dsti/sti/it/consumer/prod/guidelines.htm (visited 19 August 2001).

Reporters Sans Frontières 2001, http://www.rsf.fr/uk/homennemis.html (visited 1 August 2001).

Ringin, S. 2000, *Report to the Winston Churchill Memorial Trust of Australia on Fellowship to Investigate Ways to Counter the Production and Use of Counterfeit Documents*, Melbourne.

Rogers, L. and Leppard, D. 1995, 'For Sale: Your Secret Medical Records for £150', *Sunday Times*, 25 November, pp. 1-2.

R. v Governor of Brixton Prison; Ex parte Levin [1996] 3 WLR 657; In re Levin, House of Lords, 19 June 1997.

R v Muir, Australian Capital Territory Supreme Court, 25 September 2001.

R. v Stevens unreported decision of the NSW District Court, 27 March 1998; appeal to the NSW Criminal Court of Appeal dismissed on 15 April 1999 [1999] NSWCCA 69

Sinclair, J. 1999, 'Sex Sites and the gov.au Connection', *The Age* (Melbourne), 8 June, p. IT-3.

Sinclair, J. 2001, 'Korean Trade Visit a Boon for Local Firms', *The Age (Melbourne)*, 31 July, p. IT1-7.

Slane, B. 2001, 'Catching the Fast Slithering Tail of E-Privacy', Address by the Privacy Commissioner of New Zealand to IIR *Web Law Conference*, Auckland, 25-26 June http://www.privacy.org.nz/news5.html (visited 9 August 2001).

Smith, R. G. 1999a, 'Electronic Medicare Fraud: Current and Future Risks', in *Trends and Issues in Crime and Criminal Justice*, No. 114, Australian Institute of Criminology, Canberra.

Smith, R. G. 1999b, 'Identity-Related Economic Crime: Risks and Countermeasures', in *Trends and Issues in Crime and Criminal Justice*, No. 129, Australian Institute of Criminology, Canberra http://www.aic.gov.au/publications/tandi/tandi129.html (visited 15 August 2001).

Smith, R. G. (ed.) 2002, *Crime in the Professions*, Ashgate, Aldershot

Smith, R. G. and Urbas, G. 2001, *Controlling Fraud on the Internet: A CAPA Perspective. A Report for the Confederation of Asian and Pacific Accountants*, Research and Public Policy Series No. 39, Confederation of Asian and Pacific Accountants, Kuala Lumpur / Australian Institute of Criminology, Canberra.

Spice, L. and Sink, L. 1999, 'Criminal charges sought over posting of nude photos on Web', *Milwaukee Journal Sentinel*, 20 May. http://www.jsonline.com/news/metro/apr99/990520criminalchargessought.asp (visited 12 June 1999).

Standards Australia 1998, *Compliance Programs*, AS 3806-1998, Standards Association of Australia, Sydney.

Taylor, B. 2000, 'Prairie Dog: The Cutest Internet Watchdog', http://www.prairie-dog.net/ (visited 14 June 2000).

Thompson, D. P. 1996, 'Pablo Escobar, Drug Baron: His Surrender, Imprisonment, and Escape', *Studies in Conflict and Terrorism*, vol. 19, pp. 55-91.

United States, General Accounting Office 1997, *Telemedicine: Federal Strategy is Needed to Guide Investments*, Report to Congressional Requesters No. GAO/NSIAD/HEHS-97-67, Washington, General Accounting Office.

United States v Gorshkov 2001 WL 1024026, No. CR-550C (W.D. Wash 23 May 2001

Upton, J. 1999, 'U-M medical records end up on Web', *Detroit News* 12 February. http://detnews.com/1999/metro/9902/12/02120114.htm (visited 18 June 1999).

Yankee Group 2001, 'E-commerce Thriving in South Korea', *NUA*, 3 May http://nua.ie/surveys/index.cgi?f=VS&art_id=905356724&rel=true (visited 10 August 2001).

Young, T. H. 1995, 'Wireless Bandits', *Police*, May, pp. 32-5.