British Society of Criminology

The British Criminology Conference: Selected Proceedings. Volume 5. Papers from the British Society of Criminology Conference, Keele, July 2002. This volume published August 2003. Editor: Roger Tarling. ISSN 1464-4088. See end of file for copyright and other information.

Travelling in Cyberspace on a False Passport: Controlling Transnational Identity-related Crime

Russell G. Smith

Abstract

Modern communications and computing technologies have greatly facilitated identity-related crime, particularly that which crosses jurisdictional borders. This paper reviews the manner in which transnational electronic crimes involving misuse of identity take place, and considers various legislative, technological and risk-management responses available to deal with them. It is concluded that although technology will provide some of the solutions, these need to be supported by a simple and effective legal regime to ensure that instances of abuse can be prosecuted and that individual privacy is safeguarded. Rather than relying totally on the deterrent effects of criminal prosecution and punishment, those who travel through cyberspace need to be made aware of the risks they face and how best to protect themselves.

The Nature of Cross-border Identity-related Crime

Throughout history people have sought to disguise their true identities for nefarious purposes. Outlaws invariably used masks to cover their faces while pirates on the high seas sometimes flew the flag of another innocent ship in order to approach their victim without alerting them to their true identity and purpose. Murderers have used aliases and planted false evidence in order to commit crimes and incriminate innocent people-sometimes leading to wrongful arrest of those whom they have implicated-and tragically, sometimes resulting in the execution of innocent people.

More recently we have seen an escalation in such acts of deception, and particularly those involving cross-border activities.

The alleged terrorists who destroyed the World Trade Centre were said to have used other people's names when undertaking their pilot training and when boarding the aircraft prior to 11 September 2001.

In April 2001, in Tijuana, Mexico, two armed robbers ambushed a delivery van in order to steal 6,000 identity cards that were being delivered to consulates in Mexico. The cards allowed entry into the United States and were estimated to be worth more than US$1 million on the black market.

People who wish to emigrate to other countries are able to by-pass official channels by engaging criminal organisations to create fictitious identities for them. In Australia, for example, one syndicate charged around A$100,000 to establish new identities for prospective immigrants. After the new identity is created, which sometimes takes months or even years, the person then flies to Australia using either false documents or documents belonging to

someone else, and assumes life under their new name. A different person leaves the country on the same documents, so that there is no record of the person who came to Australia still being here (Australian Federal Police 2001).
In one case, it was alleged that an individual had come to Australia using the passport of his girl friend's brother. He then used the passport of another of her brothers to establish a false identity, then murdered the victim in order to prevent his true identity being revealed (R. v *Steve Lee* [1998] QCA 227 (Queensland Court of Appeal, 18 August 1998).
Those countries responsible for processing refugees from Afghanistan have been required to investigate cases in which people applying for refugee status are not, in fact, who they claim to be. Some have claimed to be legitimate refugees from Afghanistan when in fact they came from Pakistan without any legitimate claim to refugee status (McKinnon 2002).

Identity-related Crime in Cyberspace

The problem of identity-related crime also exists in cyberspace, where, as the cartoon in the *New Yorker* (July 1993, p. 61) observed, 'on the Internet, nobody knows you're a dog'!
On-line technologies make it relatively simple to disguise one's true identity, to misrepresent one's identity, or to make use of someone else's identity. Remailing services can be used to disguise one's identity when sending E-mail by stripping them of identifying information and allocating an anonymous identifier, sometime encrypted for added security. By using several re-mailing services, users can make their communications almost impossible to follow (Ellison 2001).
Anonymity can also be achieved in cyberspace using less technologically-complex means. Simply purchasing a pre-paid Internet access service from an Internet Service Provider and renting a telephone line from a carrier, each in a false name provides an easy means of achieving anonymity. Free E-mail services offered by some Internet Service Providers provide another means of securing anonymity as the user may simply register using a false name and address. In addition, the use of Internet Kiosks often permits users to send messages without disclosing their true identity. These services may be used for legal reasons associated with enhancing privacy or for illegal reasons such as evading debts or police investigation of criminal activities. At present there are few verification checks made when such services are obtained.
Even E-commerce technologies that make use of public key infrastructures and digital signatures can be manipulated. These technologies use mathematical constructs to create unique identifiers for people to use when communicating electronically. Users are issued with a public key and private key pair. Each key consists of two very long numbers (with up to 500 decimal digits) which relate to each other mathematically but which make it practically impossible to determine the private key value with knowledge only of the public key value. Even if one knew the mathematical process (algorithm) used to generate the pair, it would not be possible to reproduce the private key simply by knowing the public key. The private key is kept secret by the holder while each corresponding public key is publicly available. Any document signed using a private key is thus only verifiable through the use of the corresponding public key.
Such a system requires, however, that people identify themselves at the time the keys are issued to them. Simply by presenting fabricated documents to support a false identity when obtaining the key pair, offenders would be able to communicate securely in cyberspace - but in a false name. Although the subsequent transaction may be secure from hackers, the identity of the person holding the key may nonetheless be fictitious.
In a recent study of on-line anonymity, Forde and Armstrong (2002) argue that those Internet services that provide the highest levels of anonymity are most likely to be used for criminal purposes. Encrypted E-mail and Internet Relay Chat that provide higher levels of anonymity were found to be preferred by those engaging in on-line paedophile activity and hacking, while the use of the World Wide Web and File Transfer Protocols that provided weaker levels of anonymity tended to be avoided by serious criminals.
An illustration of the use of strong encryption by a criminal organisation was uncovered during 'Operation Cathedral' by police in 1998, which led to the largest ever global seizure of paedophile material occurring. This involved police in 15 countries who uncovered the activities of the W0nderland (sic) Club, an international network with members in Europe, North America, and Australia who used the Internet to download and exchange child

pornography including real-time video images. The Club used a secure network with regularly changed passwords and encrypted content. In Europe alone, over 750,000 images were recovered from computers, along with over 750 CDs and 1,300 videos and 3,400 floppy disks. One member of the Club cooperated with police which led to approximately 100 arrests around the world in September 1998 (Australasian Centre for Policing Research 2000, p. 126).

Another example concerns the various advance fee frauds perpetrated by a group of West Africans and others since the 1980s. The gist of these schemes is to trick prospective victims into parting with funds by persuading them that they will receive a substantial benefit in return for providing some limited payment in advance. Various offenders began working from Nigeria targeting victims across the globe using a variety of such schemes. All have entailed victims being approached by letter, or recently electronic mail, without prior contact. They generally describe the need to move funds out of Nigeria and seek the assistance of the victim in providing bank account details in an overseas country and administration fees needed to facilitate the transaction. The victim is offered a commission, which could be up to forty per cent of the capital involved. Capital sums of between US$20 to $40 million are usually mentioned thus creating a potential reward for the victim of up to US$16 million. An advance payment which could total up to $50,000 is usually required which represents the amount stolen. The mechanics of the schemes vary from the barely plausible to the unlikely, but all have met with varying degrees of success.

Confederates and other fraudsters in other African countries, the United States, Britain, Canada, Hong Kong, and Japan then began using the same techniques. The scale of these frauds increased considerably and created a global problem for law enforcement. Some prosecutions have taken place in West Africa, the United States and England although many offenders have evaded detection and punishment. The United States Secret Service estimated that since 1989, US$5 billion had been stolen from victims throughout the world. Between August and November 1998, Australia Post, in Sydney alone, confiscated 4.5 tonnes of advance fee correspondence which had counterfeit postage, amounting approximately to 1.8 million items. E-mail using untraceable accounts has proved to be an effective way of disseminating advance fee letters as the true identity of the sender is easy to disguise and original supporting documentation unable to be checked for authenticity (Smith, Holmes and Kaufmann 1999).

There is also 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 possible to choose legitimate-sounding names in order to improve one's credibility or to include domain names which are misleading. 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. It is also possible to fabricate Web pages in order to attract customers to businesses that might otherwise have been overlooked or avoided (Securities and Exchange Commission 2002).

One case which illustrates the transnational reach of extortionists, involved German hackers who compromised an Internet Service Provider (ISP) in South Florida, disabling eight of the ISPs ten servers. The offenders obtained personal information and credit card details of 10,000 subscribers, and, communicating via E-mail through one of the compromised accounts, demanded that US$30,000 be delivered to a mail drop in Germany. Co-operation between United States and German authorities resulted in the arrest of the extortionists (Bauer 1998).

Local forms of computer crime may also involve anonymous activities. In Australia 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 A$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, Australian* Capital Territory Supreme Court, 25 September 2001).

In another Australian case, a 24 year-old man who lived in a Melbourne suburb, manipulated the share price of an American company by posting information on the Internet and sending

E-mail messages around the globe that contained false and misleading information about the company.
On 8 and 9 May 1999, he sent in excess of three million E-mail messages to recipients in the United States, Australia and in other parts of the world. The messages contained a statement that share value of the company would increase from the then current price of US$0.33 to US$3.00 once pending patents were released by the company, and that the price would increase up to 900 per cent within the next few months. The effect of the information was that the company's share price on the NASDAQ doubled, with trading volume increasing by more than ten times the previous month's average trading volume. The messages were transmitted through an Internet Service Provider following the prior purchase of six prepaid Internet Access Kits under false names. The messages were relayed through nine mail servers without their knowledge or consent. Several different sender names were used, the majority of which were false.
The offender had purchased 65,500 shares in the company through a stock broking firm in Canada several days before he transmitted the information. He sold the shares on the first trading day after the transmission of the information and realised a profit of approximately A$17,000. The offender was charged with distributing false and misleading information with the intention of inducing investors to purchase the company's stock. He pleaded guilty and was sentenced to two years' imprisonment on each of three counts, to be served concurrently. The Court ordered that twenty-one months of the sentence be suspended upon his entering into a two-year good behaviour bond with a surety of $500 (R. v *Steven George Hourmouzis*, County Court of Victoria, 30 October 2000).
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, 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, he allegedly instructed an accomplice 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 individuals were arrested and charged with forgery and use of private documents (*Japan Times Online* 1999).
The common feature in each of these cases is that the offenders used other people's identities in verbal representations, used false proof of identity documents, or fraudulently gained access to computers though the misuse of passwords.

Responses to the Problem

Identity-related crime in cyberspace has created considerable problems for those seeking to regulate on-line conduct and to prosecute illegal activities. Not only are communications difficult to trace electronically-particularly if they come from an anonymous source or are encrypted-but investigations often have to take place across national borders, sometimes involving multiple countries in which services have been provided and through which communications have passed. This creates legal problems in determining jurisdiction as well as a number of practical forensic difficulties associated with gathering evidence from computers, locating offenders, and arranging extradition from foreign countries.
Legal action requires considerable cooperation between law enforcement agencies and substantial resources in terms of money, time and expertise. Providing and sharing information sounds relatively simple, although in the context of cross-border crime, many practical problems emerge. Language difficulties, geographical distance, lack of knowledge of foreign legal systems, time differences, telecommunications and technological differences, and expense are all likely to impede the effective prosecution of offenders. Unless losses are large or the nature of the activities serious, police simply may be unable to take action.
The specific responses to the problem of identity-related crime in cyberspace have focused on legislative reform, technological solutions and risk-management.

Legislative Responses

A range of different legislative responses has been used internationally in order to address the problem of identity-related crime.

The most extreme response has been to create new criminal offences proscribing identity fraud. In the United States, for example, the *Identity Theft and Assumption Deterrence Act* 1998 (United States Code, Title 18, Chapter 47, section 1028) which became effective on 30 October 1998, made identity theft a crime with maximum penalties of up to 15 years' imprisonment and a maximum fine of US$250 000. It establishes that the person whose identity has been stolen is a victim who is able to seek restitution following a conviction. It also gives the Federal Trade Commission power to act as a clearinghouse for complaints, referrals, and resources for assistance for victims of identity theft. Some 47 American states now have some form of identity theft legislation, although the Federal Act is the most comprehensive.

In May 2002 the Federal Identity Theft Penalty Enhancement Bill 2002 was introduced, for first reading, to amend the Federal Criminal Code to establish penalties for aggravated identity theft in the United States. The bill prescribes a sentence of: two years' imprisonment for knowingly transferring, possessing, or using, without lawful authority, a means of identification of another person during and in relation to specified felony violations (including felonies relating to theft from employee benefit plans and to various fraud and immigration offences), in addition to the punishment provided for such felony; and five years' imprisonment for knowingly taking such action during and in relation to specified felony violations pertaining to terrorist acts, in addition to the punishment provided for such felony. The bill also bars probation for any person convicted of such violations. In addition the Bill expands the existing identify theft prohibition to cover possession of a means of identification of another with intent to commit specified unlawful activity, increases penalties for violations; and include acts of domestic terrorism within the scope of the prohibition against facilitating an act of international terrorism.

Less draconian responses have involved the amendment of existing dishonesty laws to ensure that acts of deception involving identity can be prosecuted effectively. In Australia, for example, the criminal law relating to economic crime has recently been amended by the *Criminal Code Amendment (Theft, Fraud, Bribery and Related Offences) Act* 2000 (Cth), which commenced operation on 24 May 2001. Various offences are relevant to identity crimes including the offence of obtaining property or a financial advantage by deception, offences involving fraudulent conduct, forgery and falsification of documents.

In addition, efforts have been made to amend computer crime offences to ensure that identity-related crimes carried out electronically can be prosecuted. The Australian parliament has, for example, recently enacted the *Cybercrime Act* 2001 which commenced operation on 21 December 2001. This Act inserts a new Part into the Commonwealth *Criminal Code Act 1995* and largely follows the provisions of the Council of Europe's *Convention on Cybercrime* (2001) which was adopted by the Committee of Ministers of the Council of Europe on 8 November 2001 and opened for signature on 23 November 2001 in Budapest. Although limited in its Commonwealth focus, the *Cybercrime Act* 2001 significantly improves the scope for prosecuting cyber criminals by introducing substantive offences and procedural provisions consistent with those of the Convention. Whilst a significant improvement, there still remains some uncertainty in relation to the scope of a warrant; the ability to intercept E-mails prior to delivery; obtaining data not on premises; extra-territorial searches; and the procedures used to obtain evidence cooperatively from law enforcement agencies in other countries (see Ghosh 2002).

Some of the *Cybercrime Act* 2001 provisions could be used to prosecute identity-related frauds carried out through the misuse of computers, such as where a persons gains access to a computer by using another person's password without authorisation. The Act also provides new investigative powers that allow a Magistrate to grant an order requiring a specified person to provide any information or assistance that is reasonable and necessary to allow investigating officers to gain access to data held in, or accessible from, a computer on warrant premises, copy that data, and convert data into documentary form. The maximum penalty for failure to comply with such an order is 6 months' imprisonment.

There have also been attempts to ensure that financial services legislation adequately regulates identity-related deception. In Australia, for example, the *Financial Transaction Reports Act* 1988 (Cth), regulates the manner in which identity must be established when

accounts with financial institutions are created. It is an offence to open an account in a false name, such as by tendering a false passport or someone else's driver's licence, or to disclose only one of two names by which a person is known. This carries a maximum penalty of 2 years' imprisonment. It is also an offence knowingly or recklessly to make a false or misleading statement in advising a financial institution of a change of name. It carries a maximum penalty of 4 years' imprisonment.

A number of problems remain, however. At present, the requirements for people to identify themselves when they open bank accounts, register companies, obtain cryptographic key pairs, or engage the services of a telecommunications carrier or Internet Service Provider, can easily be circumvented simply by producing counterfeit or altered documents that support a false identity. Although such dishonesty is sometimes covered by regulatory statutes, in practice it is often difficult to detect, particularly for counter staff who are required to process applications quickly, or if applications are made on-line. Often it is not until a fraud has been committed that the misuse of identity becomes apparent and it is then usually impossible to locate the offender.

Technological Responses

The alternative response has been to adopt a target hardening approach through the use of technology. This aims to make acts of identity-related deception difficult to carry out and easy to detect.

Passwords

Almost all computer systems rely on passwords in order to authenticate those who seek to gain access to Personal Computers or networks. Passwords are, however, frequently misused and abused. It is possible to guess passwords, particularly if little or no thought has been given to their selection, or to use various forms of social engineering to trick users into revealing their passwords for subsequent improper use.

The use of brute computing force has also been used to break passwords. Password cracking programs are available by which computers are able systematically to search entire dictionaries in search of a password. Even if passwords are encrypted so as to prevent them from direct exposure, encryption keys have been broken through the use of massive computing resources (Denning 1998).

Users are, however, able to protect themselves by taking basic security precautions to ensure that access codes and other personal information are not stolen. Simple precautions such as not choosing obvious numbers, not sharing numbers, and changing numbers regularly are recommended. Studies reveal, however, that between twenty and seventy per cent of people are negligent in using access code information (Sullivan 1987).

There are various ways of enhancing access security controls through the use of technology. Systems have been devised which change passwords regularly, or which deny access after a specified number of consecutive tries using invalid passwords. Some work stations have automatic shutdown facilities when they have not been used for specified periods, such as five minutes. 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.

Challenge-response protocols may also be used as a means of carrying out user authentication. The server generates a random number which is sent to the card. In a public key system, such as that described above, the card digitally signs the number and returns it to the server. The server then validates the digital signature. Alternatively, call-back devices may be used. After the user dials into a computer through a modem and gives his or her identity, the system disconnects the user and then telephones the user on a number previously registered with the server. After the user is verified, the transaction can then proceed. Such a system is, however, able to be overcome through the use of call-forwarding arrangements (Denning 1998, p. 45).

Another user authentication system makes use of space geodetic methods to authenticate the physical locations of users, network nodes, and documents. One company, CyberLocator, involves a location signature sensor which uses signals transmitted by satellite to provide a location on earth at any given time. Users can thus be located at the time they attempt to gain access to the system, which provides a safeguard against individuals pretending to be legitimate users who are located in a different physical location (Denning 1998).

Biometrics

Biometric user authentication technologies are gradually being implemented in order to enhance security, although many difficult privacy issues arise in protecting biometric information (see Crompton 2002). Already there are a wide variety of such systems being used which make use of an individual's unique physical properties. Common biometric identifiers today 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 (Biometrics Institute 2002). Fingerprint identification systems are now being used to restrict access to keyboards and when using a computer mouse.

Although such systems achieve much higher levels of security than those which rely upon passwords, they are still relatively expensive to introduce. In terms of preventing identity-related crime they still do not solve the problem of people gaining access to databases containing biometric information that has been converted into a digital data stream, copying the digital data, and using this to misrepresent one's identity. There is also the concern that displacement may arise through an increase in crimes of duress in which people are compelled under threats of violence to present themselves for biometric scanning.

Digital Signatures

Public key encryption systems represent one of the most effective ways of authenticating computer users securely. Public key systems require that cryptographic key pairs be issued to individuals who are able to establish their identity to an appropriate degree of assurance by supplying multiple and independent sources of identification such as those required when accounts are opened with a financial institution. Primary documentation (such as a passport, birth certificate etc) along with matching secondary documentation (such as a bank statement, car registration papers etc) would be required in order to satisfy the degree of documentary evidence of identity required.

This, however, may prove to be one of the system's weakest points in terms of security as offenders may simply present false proof of identity documents when being issued with key pairs. Once questions of identification have been resolved, issues would arise in relation to the manner in which keys or hardware tokens are given to users (the string of numbers that represents keys would be held digitally on a computer-chip plastic card, known as a token). The financial world has already experienced considerable problems in transferring possession of plastic payment cards to users and similar problems could arise with respect to cryptographic keys which are stored on smartcards. Adequate security precautions would need to be used to ensure that tokens are passed securely to users from the issuing authority.

Another area of risk concerns the generation of cryptographic keys. It may be possible for the individual who generates a public and private key pair to retain a copy of the private key for later illegal use. Legislation may be needed which will hold the key generator liable for subsequent losses which arise out of the compromise of a key issued by that generator. Cryptographic keys would be kept on the hard drive of a computer with the cryptographic service activated by a smartcard or dongle inserted into a personal computer. Smartcards may also be used to sign a digital signature and to authenticate the identity of a user.

Standards would also need to be complied with for the storage and use of keys, perhaps by requiring keys to be used off-line or with a smartcard which is able to process transactions. Where keys are stored on personal computers or servers, appropriate risk management measures would need to be taken to ensure that their security cannot be compromised.

An example of the risks associated with the use of encrypted authentication systems arose recently when the Microsoft product, VeriSign, was tricked into issuing false digital certificates in Microsoft's name (Bader 2001, Markoff 2001). The certificates in question were not used for electronic commerce transactions, but for checking the authenticity of the name of the developer of software programs. The problem arose in the human verification part of the process of issuing digital certificates which could also occur in electronic commerce authentication procedures.

Document Security

All systems of user authentication require proof of identity when registering with authorities. The fundamental risk arises from proof of identity documents being presented which are counterfeit or have been altered.

There are various solutions to the problem of counterfeit identification documentation fraud. First, and perhaps most importantly, is the need to validate identification documents with the issuing source. Staff presented with a birth certificate should, for example, check if the details correspond with those held in the central office of Births Deaths and Marriages. An electricity account tendered as an identification document should be validated by checking with the electricity company concerned. This may not always solve the problem, however, as telephone answering services can be manipulated to support the creation of false employment or identity details.

Secondly, staff involved in validating documents need to be instructed as to the security features which are present on original documents, what original documents look like, and how forged documents appear.

Thirdly, modern security features should be incorporated on all documents used for identification purposes. Among these new technologies are security printing, in which colour-coded particles are embedded into the medium, 'tracer fibre' which can be woven into textile labels, and hidden holographic images which can be read with a hand-held laser viewer or machine reader, thus permitting verification of a product's origin and authenticity. The use of these technologies makes counterfeiting extremely difficult.

Data Matching

The other way in which technology can assist in preventing identity-related crime involves data-matching and sharing of identity-related information by public and private sector agencies. This enables anomalies in databases to be discovered at the time individuals first produce proof of identity documents when registering with organisations. If, for example, a counterfeit birth certificate and driver's licence are tendered as evidence of identity when opening a bank account or registering with an ISP, it would be possible to verify the authenticity of those documents with the issuing agency. Already trials are underway to facilitate this within public sector agencies.

The central problem with data matching, particularly if it involves the sharing of information between public and private sector organisations, is that this might infringe privacy and data access legislation. The response to this has been to argue that agencies are able to say whether or not a document is authentic as a counterfeit document does not relate to a legitimate person and thus that the agency would not be disclosing information about any real person. Systems need to be created, however, to ensure that only specific information is shared so that confidential information held, for example, by taxation authorities could not be shared with private sector companies such as banks. These complex issues are being examined currently by a number of national bodies.

Fraud Detection Software

If one is unable to prevent identity fraud from taking place entirely, then at least it may be possible to identify the presence of fraudulent transactions quickly in order to reduce the extent of any losses which are suffered or the occurrence of repeat victimisation. A number of organisations are now providing software for use in the prevention of Internet fraud. Software has been devised to analyse user spending patterns in order to alert individuals to the presence of unauthorised transactions and also merchant deposit monitoring techniques to detect claiming patterns of corrupt merchants. The success of such an approach depends, however, upon the extent to which the software cannot be interfered with or modified.

Tracking and Surveillance

It is also possible for technology to keep the activities of Internet users under 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 can 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.

Risk Management Responses

Technologies, such as biometric user authentication systems, cannot, however, provide a complete solution to the problem of identity-related fraud in cyberspace. Such solutions need to be used in conjunction with more fundamental fraud control measures based in identifying and minimising risks.
Companies wishing to prevent identity-related fraud need to ensure that they have in place the range of risk management and fraud control measures that apply in other aspects of their business. Sometimes, however, obvious fraud control measures are overlooked because of the speed with which electronic commerce procedures have been implemented, or simply because those in charge of fraud control do not fully understand the nature of the risks that arise.
In KPMGs Global eFraud survey (2001), 30 per cent of respondents reported not having adequate segregation of duties in place with respect to their electronic commerce systems, while 60 per cent did not perform security audits. Some 62 per cent did not carry out background checks on entities that assisted them in developing, maintaining and or administering their electronic commerce systems, while 56 per cent did not carry out background checks on entities with which they did business electronically.
Risk management can also be enhanced through the use of various services that aim to verify the credentials of on-line businesses. This helps users to know the legitimacy of those with whom they transact business. Some organisations are providing certification services to enable users to identify legal, safe Internet sites. Users are then free to decide whether or not they wish to make use of the material in question. In the United States, the Council of Better Business Bureaus carries out a certification service in which Internet business sites are given a form of approval. Sites which display the authorised and encrypted seal of approval agree to abide by the Council's truth-in-advertising standards and to adopt its dispute resolution procedures. Members of approved Internet Associations are able to display the fact of their membership and consumers are able to check to see if organisations do, in fact, have membership. The WebTrust program, which was developed by the American Institute of Certified Professional Accountants, certifies Internet sites which demonstrate sound online business practices after having undergone an extensive auditing procedure (AICPA 2001).
Certification and endorsement services have two primary benefits. First, individuals are able to rely upon the fact of a business being certified in order to have some measure of confidence in the trustworthiness of that business and in the availability of redress mechanisms if problems arise. Secondly, financial institutions involved in providing payment

facilities could be encouraged to deal only with certified businesses who have agreed to comply with a code of conduct which meets certain minimum standards. This would provide a powerful industry-based inducement for businesses to undergo certification and to act responsibly and in conformity with established codes of practice.

One of the main problems with endorsement and certification, is the proliferation of services and the determination of appropriate standards. Already, some twenty so-called 'Webseals' are in circulation in Australia with the government providing a comparative table which sets out their various attributes (see Cook 1999). Determining acceptable standards and publicising these will represent a major challenge for the future.

In KPMGs Global eFraud survey (2001), only 12 per cent of respondents stated that their Website had a seal identifying that their system had passed a security audit (similar percentages were evident for all countries except Australia and the United Kingdom where only two per cent of respondents reported having seals in place). This low level of usage of seals was said to be due to security audits not being well known or understood or not regarded as being an effective security measure.

In addition to certification services are strategies that rely on educating users as to the nature of the risks they face in cyberspace, and how they may best protect themselves. Most regulatory agencies throughout the world provide information in paper form and electronically through Websites which alert consumers to misleading and deceptive practices-the Consumer World (2001) Website has over 1,400 links to consumer protection and regulatory agencies.

Consumer groups also represent a good source of trusted information for consumers. Groups, such as the Australian Consumers Association, the Consumers Union of the United States and the Great Britain Consumers' Association, conduct their own testing of products and services and publicise the results through subscriber based magazines such as *Choice* (Australia), and *Which* (United Kingdom) *Consumer Reports* (United States). Although consumer organisations already provide consumer information by various means, including the Internet, perhaps the role of consumer groups in providing information services could be increased.

Consumer protection agencies also regularly conduct sweeps of the Internet in order to identify illegal practices and sites that contain misleading and deceptive information. For example, in 1998, a worldwide clean-up operation, involving the Office of Fair Trading in Britain and its counterparts in twenty-two other countries, identified 1,159 potential 'get rich quick' schemes being advertised on Internet sites (Office of Fair Trading 1998). One identified, these sites were then able to be investigated and, where appropriate, advice given to members of the public to avoid dealing with them. A similar sweep coordinated by the Federal Trade Commission in the United States, entitled 'GetRichQuick.Con', was conducted in 2000 (Brown and Johnston 2000).

Conclusions

The criminal misuse of identity in cyberspace has raised some far-reaching issues for contemporary societies. As electronic computing and communications technologies continue to develop and to expand, the need to identify ourselves with certainty has become a pressing issue. Unless convincing solutions can be devised, the digital age may not develop as quickly and effectively as we might wish, thus retarding commerce and delaying more efficient delivery of government services.

The problem of identifying ourselves needs to be addressed with a full understanding of the technological issues as well as an appreciation and willingness to address the privacy and security concerns that arise. Any solution that fails to convince people that their personal information will not be misused will not succeed in the marketplace.

The steps which can be taken to prevent identity-related fraud depend upon a range of considerations. These are the likelihood that the risk will be realised; the cost of the countermeasures; the effectiveness of the technologies used; the user-friendliness of systems; privacy concerns if databases are used; and possible negative consequences on the behaviour of users. It might be possible to prevent all forms of false identity-related fraud but the solutions may simply be too costly, unwieldy, and authoritarian to be acceptable. In certain high-risk areas, however, greater precautions need to be taken to check the validity of documents relied on or other more secure forms of personal identification need to be used.

Technology will provide some of the solutions but these need to be supported by a simple and effective legal regime to ensure that instances of abuse can be prosecuted and that individual privacy is safeguarded. This can only be achieved by government and business working in partnership. Government can establish policy and legal frameworks that make personal identification more effective and secure, but business, and individuals must act within those frameworks and, most importantly, must make full use of any technological solutions devised to protect themselves against abuse.

Unfortunately, the remedies which are available to those who have been victimised on the Internet are often practically unavailable as they would require offenders to be extradited from other places, or victims to take cross-border legal proceedings. Such action is often beyond the means of individual businesses or government departments and costs far in excess of the amount lost in many cases. The perpetrators of many Internet-related crimes are often not large corporations. They are able to close-down their operations quickly and easily, move assets to secure locations and use digital technologies to conceal their identities and disguise evidence. In such cases there is little likelihood of success whether civil or criminal proceedings are taken.

Much remains to be done, however, in applying new solutions to cybercrime, as law enforcement agencies continue to suffer from inadequate funding, courts are only now beginning to deal with the legal problems that have arisen in specific cases, and suitably trained forensic accountants are often in short-supply. It is also clear that the deterrent effects of criminal prosecution and punishment are limited in this area as offenders often receive relatively lenient sentences in cases of economic crimes.

The problem of cybercrime has brought home to policy makers and legislators the need to harmonise efforts globally. Already considerable achievements have been made in devising uniform approaches to dealing with computer crime internationally with a number of countries having agreed to conventions and treaties to deal with some of the more difficult problems, such as transnational and organised criminal activities that are carried out electronically.

Allied to the harmonisation of laws, however, is the need to harmonise other aspects of business practices in order to provide a global environment in which economic crime is difficult to perpetrate and yet simple to detect. Bodies such as the International Accounting Standards Committee (IASC), for example, help to promote uniform accounting practices and procedures within the business community that seek to reduce the risk of improper conduct being engaged in. Similarly, international professional bodies have a role to play in creating uniform ethical practices globally which militate against fraud (Braithwaite and Drahos 2000, p. 121).

Those who make use of the Internet need, however, to be made aware of the risks they face and informed about the nature of the various objectionable on-line practices which are present. Already there are substantial amounts of information of this nature available. The challenge lies in ensuring that users are made aware of its existence. In this regard, certification and notification systems, which permit users to identify readily businesses which have been found to be trustworthy, seem to provide the best option. Technology needs to be developed, however, to ensure that certification services are, themselves, unable to be manipulated. Fraud relating to the process of certification might also develop in the future as might the use of 'phoenix businesses' which re-establish themselves immediately they have been closed down because of improper practices.

Any system in which unique identifiers are issued to people-by the government, or by private sector organisations-would need to comply with these strict legislative privacy protections so that personal information could not be maintained in databases and used for improper or unauthorised purposes.

If the government were charged with the duty of issuing verifiable identification information, safeguards would be established to permit people to check the accuracy of the information that is kept and to obtain redress if that information were incorrect or misused in any way. Systems of accountability would also be established to protect information from unauthorised disclosure.

As we have seen, it is now relatively simple to travel through cyberspace on a false passport. Although we leave digital trails of evidence wherever we go, it is sometime simply too costly and difficult for law enforcement to follow. The challenge for the future lies in making sure that when people present themselves for identification the evidence they submit is able to be verified and that when they proceed to have their identity authenticated on subsequent occasions, checks are made to ensure that someone else has not take over their identity.

Technology may help to achieve these objectives although users who know of the risks can do much to protect themselves.

References

AMERICAN Institute of Certified Professional Accountants (AICPA) 2001 'WebTrust': http://www.cpawebtrust.org/ (visited 29 May 2002).

AUSTRALASIAN Centre for Policing Research 2000, *The Virtual Horizon: Meeting the Law Enforcement Challenges*, Scoping Paper, Australasian Centre for Policing Research, Adelaide.

AUSTRALIAN Federal Police 2001, 'Identity Fraud Trends', *Comfraud Bulletin*, No 23, pp. 1-3.

BADER, J. L. 2001, 'Paranoid Lately? You May Have Good Reason', *New York Times Online*, 24 March.

BAUER, J. 1998, Testimony to the Subcommittee on Technology, Terrorism and Government Information, Committee on the Judiciary, United States Senate, 20 May http://www.securitymanagement.com/library/bauer.html (visited 29 May 2002).

BIOMETRICS Institute 2002, 'Biometric Technologies'. http://www.biometricsinstitute.org/bi/types.htm (visited 29 May 2002).

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

BROWN, R. and Johnston, M. 2000, 'Internet fraud sweep fails to turn up any NZ sites', IDG-Net, 27 March 2000: http://idg.net.nz/webhome.nsf/UNID/35166639324F7B5DCC2568AC0010C1D3!opendocument (visited 29 May 2002).

CONSUMER World 2001, Website http://www.consumerworld.org/ (visited 29 May 2002).

COOK, V. 1999, 'Trust Me, I'm a Computer', *Communications Newsletter*, September, pp. 14-15.

COUNCIL of Europe 2001, *Convention on Cybercrime*, European Treaty Series No 185, Budapest, 23 November 2001, Council of Europe, Strasbourg http://conventions.coe.int/treaty/EN/projets/projets.htm (visited 29 May 2002).

CROMPTON, M. 2002, 'Biometrics and Privacy: The End of The World as We Know It or The White Knight of Privacy?', Paper presented at the Biometrics Institute Conference *Biometrics - Security and Authentication*, 20 March, Sydney.

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

ELLISON, L. 2001, 'Cyberstalking: Tackling Harassment on the Internet, in Wall, D. S. (ed.), *Crime and the Internet*, pp. 141-51, Routledge, London.

FORDE, P. and Armstrong, H. 2002, 'The Utilisation of Internet Anonymity by Cyber Criminals', Paper presented at the International Network Conference, 16-18 July, Sherwell Conference Centre, University of Plymouth, Plymouth. http://www.cbs.curtin.edu.au/Workingpapers/other/Utilisation%20of%20Internet%20Anonymity%20by%20Cyber%20Criminals.doc (visited 29 May 2002).

GHOSH, A. 2002, 'The Cybercrime Act 2001: Implementing the European Union's Cybercrime Convention', Paper presented at the RSA Conference, San Jose, 16-22 February.

JAPAN Times Online 1999, 'Man Arrested Over Bogus Bank Accounts', 13 September http://www.japantimes.co.jp/cgi-bin/getarticle.pl5?nn19990913a7.htm (visited 29 May 2002).

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

MARKOFF, J. 2001, 'Warning From Microsoft on False Digital Signatures', New York Times Online, 23 March.

MCKINNON, M. 2002, 'Boatpeople ID Scam', *Courier Mail (Brisbane)*, 15 February.

OFFICE of Fair Trading (OFT) 1998, 'Internet Scams Deleted, Sweep Identifies 'Get Rich Quick' Schemes', *Fair Trading Magazine*, Spring, Office of Fair Trading, London.

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

R. v Steven George Hourmouzis, County Court of Victoria, 30 October 2000, http://www.countycourt.vic.gov.au/judgments/hourmouz.htm (visited 29 May 2002).

R. v Steve Lee [1998] QCA 227 Queensland Court of Appeal, 18 August 1998.

SECURITIES and Exchange Commission 2002, 'Regulators Launch Fake Scam Web Sites to Warn Investors About Fraud'. http://www.sec.gov/news/press/2002-18.txt (visited 29 May 2002).

SMITH,R. G., Holmes, M. N. and Kaufmann, P. 1999, 'Nigerian Advance Fee Fraud', in *Trends and Issues in Crime and Criminal Justice*, No. 121, Australian Institute of Criminology, Canberra.

SULLIVAN, C. 1987, 'Unauthorised Automatic Teller Machine Transactions: Consequences for Customers of Financial Institutions', *Australian Business Law Review*, vol. 15, no. 3, pp. 187-214.

About the Author

Dr Russell G. Smith has qualifications in law, psychology, and criminology from the University of Melbourne and a Ph.D. from the Faculty of Laws, King's College, University of London. He practised as a solicitor for a number of years before becoming a Lecturer in Criminology at the University of Melbourne in 1990. In 1996 he took up a position at the Australian Institute of Criminology where he is now Deputy Director of Research. He also heads the Institute's Sophisticated Crime, Regulation and Business Program and has carried out research on aspects of computer crime, fraud control, and professional regulation. Dr Smith has written or contributed to over eighty academic publications including the following books:

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

Grabosky, P. N. and Smith, R. G. 1998, *Crime in the Digital Age: Controlling Telecommunications and Cyberspace Illegalities*, Federation Press, Sydney / Transaction Publishers, New Brunswick.

Copyright Information