AUSTRALIAN INSTITUTE OF CRIMINOLOGY

trends & issues

in crime and criminal justice

No. 206

Crime Reduction through Product Design

Andrew Lester

The concept of crime reduction through product design (CRPD) has recently evolved to provide security of physical objects and data against criminal activity. It is argued that protective measures incorporated into products (for example, vehicle immobilisers, tracking systems and even simple locking devices) can prevent these items from becoming targets or instruments of crime.

This paper explores CRPD principles, technologies and issues. It examines crimes which can be reduced, current and future designs for crime control, and considerations such as user acceptance, design effectiveness and crime displacement. The potential for increasingly widespread use of CRPD is also discussed.

Crime reduction through product design offers a new way of thinking about crime prevention. Technological developments will only enhance the capacity of protective designs to act as successful crime reduction tools in the future.

Adam Graycar
Director

Principles of Crime Reduction through Product Design

Crime reduction through product design (CRPD) involves integrating protective features into products in order to reduce their potential to become targets of criminal activity (such as theft, fraud and damage), as well as preventing their use as instruments of crime. The term "product" encompasses any physical property and forms of currency, as well as electronic information and computer software.

Grabosky (1998) has previously examined applications of technological crime control in a number of fields. This paper focuses specifically on measures incorporated into products for security, regardless of the environment in which they are placed and of the persons by whom they can be accessed.

In most cases, the design features are distinct from the core product and are not required for it to perform its intended function(s). As such, security technology may either be combined with goods at their time of production (such as digital watermarks embedded in computer software) or obtained separately and added at a later time (such as encryption methods for data protection). In either case, CRPD emphasises integration between a product and its protective features, which is a more effective and efficient approach than later relying on standard target-hardening measures for security (Clarke 1999, p. 35).

Depending on the particular product and its design features, CRPD is instrumental in either or both of the following:

- prevention of offences; and
- facilitation of an effective and efficient response following an offence.

Most desirably, emphasis is placed upon the first aim, although the second may have a significant role in the deterrence of crime and the apprehension of offenders.

May 2001

ISSN 0817–8542
ISBN 0 642 24233 X

Australian Institute
of Criminology
GPO Box 2944
Canberra ACT 2601
Australia

Tel: 02 6260 9221
Fax: 02 6260 9201

For a complete list and the full text of the papers in the Trends and Issues in Crime and Criminal Justice series, visit the AIC web site at:

http://www.aic.gov.au

Reduction in the Potential of Products as Targets of Crime

In terms of products becoming targets of crime, CRPD primarily provides counter-measures against the following offences:

- theft;
- fraud, counterfeiting and copyright infringements;
- tampering; and
- graffiti and vandalism.

This facet of CRPD is largely limited to offences against property, although designs reducing the attractiveness of items may indirectly avert violent confrontations such as robbery or home invasions.

Reduction in the Use of Products as Instruments of Crime

Protection against products becoming instruments of crime can impact considerably on offences both against the person and against property, as demonstrated by the following examples.

Technology that renders firearms inoperable by anyone other than their intended user(s) can reduce instances of homicide, robbery, hostage-taking, sieges, gang warfare, suicide and criminal operations such as dealing in drugs or even arms themselves. Additionally, this can prevent police officers' weapons being used against them (Grabosky 1998) as well as linking firearms used in offences to a small number of possible operators.

Computers and telecommunications equipment can be used for:

- fraud and other white-collar crime;
- hacking; and
- malicious damage to networks, computer systems and data.

Motor vehicles are employed for a range of illegal activities, such as anonymous and disposable transport to and from crime scenes, ram raids, drive-by shootings and joyriding. It is self-evident that limiting the potential for illegal use of any of these items can reduce the occurrence of the corresponding offences. Counter-measures that diminish the market for stolen goods of any kind can also cut the level of criminal activity in general.

Protection against misuse such as product tampering can also avert further offences. As an example, tampering counter-measures can indirectly prevent crimes with political (such as terrorism), financial (such as extortion) or personal (such as revenge) motives. The need for effective protection against tampering can be demonstrated by the recent Panadol poisoning extortion bid, in which the headache pill's manufacturer, SmithKline Beecham, suffered a loss of $90 million following a massive product recall (Chulov 2000).

Reduction in CRAVED Attributes

Since property theft is the most common offence reported to police in Australia (Australian Institute of Criminology 1999), and because its reduction can prevent further offences, it is appropriate to consider many designs in terms of the acronym "CRAVED". This states that some items are attractive as targets of theft because they are Concealable, Removable, Available, Valuable, Enjoyable and Disposable (Clarke 1999). It is suggested that protective features that decrease or negate any of these product characteristics would significantly lessen its likelihood of being stolen. Some CRAVED aspects are also applicable to designs that prevent counterfeiting and unauthorised firearm use, making it a worthwhile reference when examining CRPD.

Current Product Design Technologies

Designs to Reduce Theft and Unlawful Use

There are many theft counter-measures that are now widely accepted and used, such as electronic or ink tags attached to retail merchandise, car alarms, engine immobilisers, and vehicle stereos with detachable faces and security code requirements. In addition, innovations are continually emerging as technology and production practices improve. One example is in the protection of portable computers, where several companies offer a tracking method using a small program that can be embedded in the machine's hard drive. This software, which is undetectable and cannot be removed once installed, regularly dials into a monitoring centre when the machine is connected to the Internet, supplying identification information and the telephone number of its calling location. When informed that a computer has been stolen, the monitoring centre begins a scan and alerts appropriate parties once it has been located (Evans 2000; Computer Security Products Inc 1998).

A new means of protecting mobile telephones involves software that monitors use patterns based on the time of day, duration and numbers called. This establishes a profile for the regular user. Upon detection of any deviations, the telephone is locked unless a personal identification number is entered (Meredith 2001). Because this software is operated by the network and not the mobile telephone itself, it can be used to protect any model of phone.

Electronic Article Surveillance (EAS), which is the attachment of electronic tags to products to deter and detect retail theft, was introduced in 1968 and has experienced widespread use since the mid-1980s (DiLonardo 1996). A recent development in this area is "source tagging", which entails applying the tag at the point of manufacture rather than at the sales outlet. This has numerous benefits in the form of increased productivity and merchandising opportunities (Source Tagging Council 2001) and makes EAS more likely to be adopted and implemented by retailers. Because EAS is a proven method of reducing theft (DiLonardo 1996), increased usage has the potential to further diminish such offences.

Many developments in car design have been implemented to control vehicle theft. These include:

- increased security for immobilisers, such as in the use of "code hopping" technology (Design News 1997a; Hogan 1997);
- car batteries that can themselves be immobilised remotely (DeMeis 2000);
- fluid-based tilt switches to detect attempts at towing or lifting vehicles (Design News 1996); and
- high-security keys that require cutting by laser.

There is also a sophisticated system available that automatically contacts the owner when the vehicle is being broken into, allows remote operation of the windows, door locks, lights, horn, alarm and immobiliser, and facilitates tracking via the Internet (Elite Logistics Services Inc 1999).

In addition to safeguarding complete products, there is also the need to protect individual components within the product, which may in themselves be valuable (Foresight Crime Prevention Panel 2000, p. 7). The protective designs in car audio systems mentioned previously provide two examples. Another that has been adopted is the distribution of new vehicle parts in unique packaging featuring a holographic seal (discussed below) and a barcoded label (DaimlerChrysler Australia / Pacific Pty Ltd 2000) which can diminish the market for repackaged (and also counterfeit) components and lessen the potential for them to be stolen. Also, while it has been dismissed by some manufacturers as too costly, some makers label major parts with their corresponding vehicle identification number (Turk 1996); this can significantly reduce the parts' value in illegal operations. Clarke (1999) discusses the fact that North American manufacturers are required to label the parts of cars facing a high theft risk under the *Motor Vehicle Theft and Law Enforcement Act 1984*, and that the cost of doing so is less than US$5 per car.

Design features are also available to inhibit vehicles being used for driving offences. One example is a limiting device that prevents cars from travelling at excessive speeds, while another is a breathalyser that immobilises the vehicle if the driver gives a blood-alcohol reading above the legal limit (LifeSaver Interlock 2000).

For some products, protective designs need not be sophisticated to reduce theft. One example is a bicycle in which the frame itself forms a locking device that would need to be cut for the bicycle to be stolen, hence decreasing its value (Cyclic Systems 1995). Another example is a bolt design that can only be removed using special tools (Design News 1997b) and has a range of applications in preventing theft, tampering and other malicious damage. Similarly, a product has been developed for securing cargo containers that functions both as a locking device and a seal to protect against theft and tampering (Omni Security Consultants Inc 1998).

Several design possibilities exist in the field of firearm-user authentication to restrict operation only to designated persons. These include simple locks that are deactivated by key, combination, or a magnetic ring on the user's finger (Public Health—Seattle & King County 2000), although more effective and reliable designs are present in sophisticated "smart guns". In this field, two technology types have been identified:

- radio frequency authentication; and
- biometric authentication.

Firearms employing radio frequency authentication operate only when a coded radio signal is received from a short-range transponder worn by the user. In the absence of this signal, the weapon locks and cannot be used until the transponder is in range (Schofield 1997). Biometric technology authenticates users by scanning their hand and comparing it to existing patterns in an electronic database. The firearm will only unlock if a match is found between scanned and stored images (Advanced Biometrics Inc 2000a).

Designs to Reduce Fraud, Counterfeiting and Copyright Infringements

One form of protection against counterfeiting is the use of holographic images, which are extremely difficult to reproduce. These images are usually incorporated into labels that are affixed to products, and their absence or incorrectness enables detection of illegally produced items. Holograms have a range of applications, including credit cards, vehicle parts, alcoholic beverage containers, computer software, pharmaceuticals and packaging of all kinds (Lowe 2000). Other techniques, such as sub-surface laser marking and optical imprints that are authenticated using scanning devices, can also be included in labels (Mikoh Corporation Limited 2000; Design News 1997c). Laser-engraved photographs and signatures can also be used to protect credit and debit cards (Levi & Handley 1998).

Digital watermarking offers a means of safeguarding software, web pages and other electronic data against copying, unauthorised access and tampering, and involves the insertion of imperceptible identifying code into digital information (Watermarking World 2000). Hardware and software design that causes degradation of digital data upon repeated copying is also a possibility (Lessig 1999). For user authentication in computer system access control and security in e-commerce via the Internet, a mouse is available that features an in-built hand scanner employing the same principles as biometric "smart gun" technology (Advanced Biometrics Inc 2000b).

Despite rapid increases in the global use of digital technology, however, it is important to recognise that paper-based fraud remains a growth area (Chapman & Smith 2001) and should not be ignored. As an example, there are many security features that can be incorporated into cheques, including (Goldstar Business Forms Ltd 1999):

- a warning band stating the cheque's security features for deterrence;
- an authentication band advising that the cheque should not be cashed unless certain features appear elsewhere on its surface;
- a unique serial number which is visible at room temperature and disappears when heated by friction;
- areas on the back of the cheque coated in a substance that verifies that the correct paper has been used when rubbed by a coin;
- embedded "VOID" watermarks that appear on photocopied or scanned cheque images;
- background colours that are resistant to laser scanning and cause noticeable differences in copies;
- text microprinting that verifies originality when viewed under a microscope;
- high resolution microprinting that causes distortion when copied on low or medium resolution devices;
- fabrication that causes damage to the cheque upon attempts at the removal of toner and ink by chemical washing or abrasion;
- reactive paper that causes void messages to appear in multiple languages if the cheque touches any chemicals used in cheque forgery; and
- a patterned background to visibly indicate attempts at physically swapping characters' positions to increase a cheque's value.

Any combination of these techniques may be designed into cheques to provide the desired level of protection.

In terms of currency, polymer banknotes also offer excellent counterfeit protection resulting from design and production that includes shadow marks and a clear window which can incorporate holographic images, vignettes, embossing and diffractive optical variable devices (James 1995; Note Printing Australia 2000). These elements make the notes very difficult and costly to reproduce, and allow identification of fraudulent copies. The "self-authenticating banknote" concept is another counterfeit detection feature, where the window can be designed to reveal hidden printing elsewhere on the note (Securency Pty Ltd 2000).

Designs to Reduce Tampering

Protection against tampering is enabled primarily by preventing access to a product, or facilitating detection if its packaging has been opened. Some designs previously discussed in relation to other offences are also applicable here, including special bolt designs, cargo seals and optical devices (such as holograms and sub-surface laser marking) incorporated into sealing devices. Other mechanisms employed in tamper-proof seals include powerful bonding agents or fastening ribbons that require destruction for removal, tiny partial cuts that cause the seal to rip upon removal attempts, and features that cause the display of warning messages upon being interfered with (CGM Security Solutions 2000). Most tamper-evident seals are uniquely numbered to prevent their replacement following a surreptitious attack. On a basic level, tamper protection is also present in the form of safety buttons used in airtight packaging for foods.

Designs to Reduce Graffiti and Vandalism

Product designs for graffiti and vandalism protection primarily involve physical measures, such as graffiti-resistant substances, which are continually being improved. Paints and film coatings for walls, signs and other public surfaces are now available which require minimal effort and no abrasive chemicals for removal of graffiti from a range of marking materials (Eccotech Inc 1997). Another older concept that has been enhanced over time is window laminating to resist scratching and breakage. Lamination techniques now exist where the outer coating can be completely removed if it becomes damaged, further increasing the window's lifetime (Design News 1995a). Other physical vandalism counter-measures usually involve integrating strengthening properties into the design, such as in public seating, bins, sprinklers (Pioneer Midwest Inc 2000) and even ATM keypads (Design News 1995b). Vandal protection can also be achieved by electronic means, for example in vending machines featuring devices to generate alarms upon the removal of power, tilting, tampering and other damage (CEPCO Products 2000).

Future Directions

The following trends in electronic components are significant from a CRPD perspective:

- decreasing cost;
- reducing size;
- improving capability; and
- increasing availability, public use and acceptance.

These projections suggest that electronic devices will be increasingly used for protection of products, including those that do not ordinarily have electronic components, such as firearms. One example is biometric technology, where methods exist for uniquely identifying someone in over a dozen different ways, many of which could be incorporated into products to make them of value only to their legitimate users.

Telecommunications technology, particularly wireless applications, may also be included in products more frequently in the future. Some examples include remote control of security systems, more efficient transmission of alarm signals from security devices, as well as global tracking becoming feasible for a wider range of items.

Growing emphasis on the integration of many functions into a single unit, such as in mobile telephones, has made it likely that people will own a smaller number of more powerful electronic products in future. In this case, incorporation of protective designs may become simpler because fewer items overall will require security.

Another future trend is the focus on electronic services such as pay television, communications and the Internet. It has been argued that protective design efforts will need to concentrate on these services instead of the hardware products themselves which will merely become a means of access and of little use in their own right (Davis & Pease 2000).

Smart cards are a further technological development that may combat crimes involving cash and credit facilities. Hardware and operating system security techniques are currently being developed (Saunders 1999) for integration as standards in smart cards prior to their widespread use. The trusted system concept also promises protection of electronically stored intellectual property, and involves computer designs that prevent access to data unless the user abides by rules governing the data's use, modification and distribution. This means, for example, that persons would be prevented from making unlimited duplicates of information unless granted permission by the copyright owner. The concept also facilitates payment for access and allows copyright to be enforced by technological rather than legal means (Lessig 1999).

CRPD is currently in its infancy, although significant potential exists for technology in future protective designs, even to the point where artificial intelligence can distinguish between legal and illegal activities and secure products accordingly. In the meantime, however, there is little to suggest that CRPD will not experience steady implementation in a society that is becoming increasingly accepting of technology and aware of the need to reduce crime.

Issues

User Acceptance

User acceptance of a protective design is of prime importance in determining its success. Because security features are supplementary to a product's intended function, they may be questioned if they are not sufficiently transparent to the user. Factors affecting this transparency include the additional costs, privacy infractions and possible inconvenience that the design may cause.

The cost of incorporating protection must be balanced against the product's value and its risk of becoming a target or instrument of crime. Users will usually only be willing to pay up to a certain proportion of its value for the inclusion of security features. In some cases, however, costs may be offset by third-party incentives, such as insurance premium discounts and government rebates for vehicle immobilisers (Safer WA 2001).

Privacy is a significant issue with electronic technology, particularly in tracking and monitoring personnel and their activities. While there are advantages in doing so from a crime perspective, people are generally highly protective of their right to privacy and may disagree with these practices (particularly in future designs for Internet use and information transfer).

In terms of convenience, security features should not:

- require a significant amount of additional effort to be overcome by a legitimate operator;
- malfunction so that a legitimate operator is denied use of the product;
- cause an excessive increase in product size or mass; or
- contribute to any other factors likely to make the product unattractive to a user.

Since product designers and manufacturers primarily exist to make profit via sales, they are highly attuned to consumers' preferences; hence, user acceptance is paramount to CRPD's success.

Effectiveness and Endurance of Design

Another central CRPD issue is how well a design protects its corresponding product, and for how long it is capable of doing so. Any security feature that cannot suitably reduce an item's risk of becoming a target or instrument of crime will not be considered worthwhile. Similarly, technology that becomes obsolete within a short time frame due to offenders' increasing knowledge and sophistication faces a similar outcome. For this reason, many older concepts continually require improvement to remain effective, such as the use of "code hopping" techniques in wireless vehicle immobilisers to combat car thieves replicating the transmitter's signal using scanners. Highly secure designs with a significant lifetime are a key contributor to CRPD.

Crime Displacement

Displacement is an underlying issue in most crime reduction strategies, and can occur in a variety of forms including time, space, nature of offence and target of offence. The extent to which any of these occur in response to CRPD measures will depend on the specific situation. Hence, while the potential for displacement exists, it is not necessarily a guaranteed CRPD outcome. In one example discussed by Clarke, Kemper and Wyckoff (2001, pp. 11–12), technology combating cellular telephone fraud in the United States did not result in displacement to any other types of fraud. With a broad implementation of protective designs and attention to the potential occurrence of displacement, CRPD therefore represents a viable crime counter-measure.

Conclusion

A broad variety of designs and technologies can be incorporated into products to reduce their potential as targets of crime in the major areas of theft, fraud and damage. In addition, protective features that negate the value or operability of stolen goods can also interrupt the precursory relationship between theft and more severe offences. Underlying these design technologies, however, are several issues for consideration, including user acceptance of protected products, effectiveness and endurance, and crime displacement. The limitations of CRPD measures should also be recognised in that they cannot combat all types of crime and are ideally complemented by other strategies. However, the rapid pace of technological development and innovation, and decreasing cost of hardware devices suggests that CRPD has a promising future. It is likely that product design will become an increasingly widespread means of protecting assets and reducing crime.

References

Advanced Biometrics Inc 2000a, "GunLock 'Smart Gun' technology", http://www.livegrip.com/gunlock.htm.

—— 2000b, "eCommerce Trackball", http://www.livegrip.com/trackball.htm.

Australian Institute of Criminology 1999, *Australian Crime: Facts and Figures 1999*, Australian Institute of Criminology, Canberra.

CEPCO Products 2000, "Vending machine anti-theft, anti-vandalism, and anti-tamper monitoring systems uses CEPCO Powerline Carrier Modules", http://www.cepcoproducts.com/A19.html.

CGM Security Solutions 2000, "Transport Security Tape", http://www.tamper.com/cgm01.htm.

Chapman, A. & Smith, R.G. 2001, "Controlling financial services fraud," *Trends and Issues in Crime and Criminal Justice*, no. 189, Australian Institute of Criminology, Canberra.

Chulov, M. 2000, "Poisoning victims the suspects", *The Australian*, 6 December, p. 1.

Clarke, R.V. 1999, "Hot products: Understanding, anticipating and reducing demand for stolen goods", *Police Research Series,* no. 112, Home Office, London.

Clarke, R.V., Kemper, R. & Wyckoff, L. 2001, "Controlling cell-phone fraud in the US: Lessons for the UK 'Foresight' prevention initiative", *Security Journal,* vol. 14, no. 1, pp 7–22.

Computer Security Products Inc 1998, "CompuTrace theft recovery software", http://www.computersecurity.com/computrace/index.html.

Cyclic Systems 1995, "Patented, award-winning, self-locking bicycle technology", http://www.ihpva.org/com/CyclicSystems/.

DaimlerChrysler Australia/Pacific Pty Ltd 2000, "New parts packaging", http://www.mercedes.com.au/default.asp.

Davis, R. & Pease, K. 2000, "Crime, technology and the future," *Security Journal*, vol. 13, no. 2, pp. 54–64.

DeMeis, R. 2000, "Relay open-circuits car thieves", *Design News,* 2 October, http://www.manufacturing.net/magazine/dn/archives/2000/dn1002.00/new.html.

Design News 1995a, "Laminate tackles transit vandals," *Design News*, 6 February, http://www.manufacturing.net/magazine/dn/archives/1995/dn0206.95/03news.htm.

—— 1995b, "ATM keypads resist vandals," *Design News*, 25 September, http://www.manufacturing.net/magazine/dn/archives/1995/dn0925.95/18news.htm.

—— 1996, "Telltale fluid system discourages vehicle thefts," *Design News*, 5 February, http://www.manufacturing.net/magazine/dn/archives/1996/dn0205.96/03tech.htm

—— 1997a, "Code hopping foils car thieves," *Design News*, 22 January, http://www.manufacturing.net/magazine/dn/archives/1997/dn0122.97/enginews.htm.

—— 1997b, "No-theft fastener," *Design News*, 3 February, http://www.manufacturing.net/magazine/dn/archives/1997/dn0203.97/dcorner.htm.

—— 1997c, "Tagging technology to help companies battle piracy," *Design News*, 1 December, http://www.manufacturing.net/magazine/dn/archives/1997/dn1202.97/24tech.htm.

DiLonardo, R.L. 1996, "Defining and measuring the economic benefit of electronic article surveillance", *Security Journal*, vol. 7, pp. 3–9.

Eccotech Inc 1997, "Wearlon anti-graffiti coatings", http://www.capital.net/com/eccotech/Eagraffiti.html.

Elite Logistics Services Inc 1999, "PageTrack™ 2 System", http://www.pagetrack2.com/.

Evans, J. 2000, "Anti-theft technology emerges", *InfoWorld*, http://www.infoworld.com/articles/hn/xml/00/08/11/000811hnstolen.xml.

Foresight Crime Prevention Panel 2000, *Just Around the Corner*, United Kingdom Department of Trade and Industry, London.

Goldstar Business Forms Ltd 1999, "Anatomy of a secure cheque", http://www.goldsec.com/Anatomy_of_a_Secure_Cheque.html.

Grabosky, P.N. 1998, "Technology and crime control", *Trends and Issues in Crime and Criminal Justice*, no. 78, Australian Institute of Criminology, Canberra.

Hogan, B.J. 1997, "Electronics enhance security", *Design News,* 23 June, http://www.manufacturing.net/magazine/dn/archives/1997/dn0623.97/12news.htm.

James, M. 1995, "Preventing the counterfeiting of Australian currency", *The Promise of Crime Prevention: Leading Crime Prevention Programs*, Research and Public Policy Series, no. 1, Australian Institute of Criminology, Canberra, pp. 12–13.

Lessig, L. 1999, *Code and Other Laws of Cyberspace*, Basic Books, New York.

Levi, M. & Handley, J. 1998, "The prevention of plastic and cheque fraud revisited" *Home Office Research,* no. 182, Home Office, London.

LifeSaver Interlock 2000, "Welcome to LifeSaver Interlock", http://www.lifesafer.com/.

Lowe, P. 2000, "Security holograms and counterfeiting", *Intersec*, January, vol. 10, no. 1, pp. 20–22.

Meredith, H. 2001, "'Sentinels' help guard against mobile phone fraud", *The Australian Financial Review*, 9 February, p. 28.

Mikoh Corporation Limited 2000, "Mikoh Corporation Limited", http://www.mikoh.com/index.html.

Note Printing Australia 2000, "The world standard in security", http://www.noteprinting.com/sc03_world/sc03_1/.

Omni Security Consultants Inc 1998, "Sealock Security System", http://www.sealock.com/.

Pioneer Midwest Inc 2000, "Rainbird R50 Rotor", http://www.shopworks.com/pioneer/index.cfm.

Public Health—Seattle & King County 2000, "Handgun locking devices", http://www.metrokc.gov/health/firearms.htm.

Safer WA 2001, "Immobilise for a Safer WA", Government of Western Australia, http://202.0.108.22/info/index.html.

Saunders, K. 1999, "Securing smart cards", *Intersec*, September, vol. 9, no. 9, pp. 276–8.

Schofield, J. 1997, "Electronics personalize guns", *Design News*, vol. 52, p. 13.

Securency Pty Ltd 2000, "Self-authentication features", http://www.securency.com.au.

Source Tagging Council 2001, "What is source tagging?", http://www.synergy-stc.com/.

Turk, M. 1996, "Bravada packs a punch", *Design News,* 7 October, http://www.manufacturing.net/magazine/dn/archives/1996/dn1007.96/19news.htm.

Watermarking World 2000, "Short biography of digital watermarking", http://www.watermarkingworld.org/intro.html.

Andrew Lester is a student at Edith Cowan University and a former intern at the Australian Institute of Criminology

General Editor, Trends and Issues in Crime and Criminal Justice series:
Dr Adam Graycar, Director
Australian Institute of Criminology
GPO Box 2944
Canberra ACT 2601 Australia

Note: Trends and Issues in Crime and Criminal Justice are refereed papers.