AUSTRALIAN INSTITUTE OF CRIMINOLOGY

**trends & issues**

in crime and criminal justice

No.78

# Technology & Crime Control

Peter Grabosky

*As we approach the 21st century, our efforts to tackle the challenge of crime will be assisted significantly by developments in technology. From improvements in locking and alarm systems, to new devices for location, identification, and surveillance, to means of restraining individuals who pose a risk to themselves or others, the crime control tasks confronting both the community and our police services will be made easier. Technology can assist us in making optimal use of finite resources.*

*Along with these new technologies, however, come certain downside risks. Some systems are vulnerable to excessive or inappropriate use, while others may have unintended adverse consequences, such as potential for harm to third parties. This Trends and Issues paper reviews some of the emerging technologies which may be applied to crime control. Recognising that new technologies should not be embraced uncritically, it discusses some of the principles which might accompany their introduction in a democratic society.*

**Adam Graycar**
**Director**

The application of science and technology to criminal justice is nothing new. Since the invention of modern policing and corrections in the 19th century, progress has often been measured in terms of technical innovation. Thus we have seen the advent of fingerprinting, wireless communications, the motor car, and other devices which have long since become mundane. The adaptability, and the malign creativity of criminals, however, requires the ongoing development of means to prevent, or at least to minimise, their harmful activity.

The following pages provide a brief overview of some current and emerging technologies for crime control. We first discuss mechanisms for surveillance and detection, then blocking devices, and finally, technologies of restraint and incapacitation. Acknowledging that few innovations are completely free of problems, some of the adverse consequences of these new systems are identified, and basic principles suggested to ensure that their development and implementation can be accomplished in a manner consistent with human rights in a free society.

## Technologies of Surveillance and Detection

Some applications of technology to crime prevention have become a fact of life in Australia. Few airline travellers remember the days before metal detectors became a fixture at airports; most motorists have grown up since the advent of radar to detect speeding. The Australian introduction of red light cameras, which help enhance safety at traffic intersections, has received international recognition (*see* http://www.nlectc.org/techhed.html#UNBLINK). Home alarm systems appear to be contributing to reduction in the prevalence of

January 1998

ISSN 0817-8542
ISBN 0 642 24058 2

Australian Institute
of Criminology
GPO Box 2944
Canberra ACT 2601
Australia

Tel: 02 6260 9200
Fax: 02 6260 9201

For subscription information together with a complete list 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
or send an email to:
aicpress@aic.gov.au

break and enter. At least one Australian insurance company offers premium discounts for policyholders who have a home alarm system installed (NRMA Insurance 1996, p. 3) and car alarms and immobilisers are often required by insurance companies.

Research in the United Kingdom has demonstrated that improved street lighting can contribute to public safety by improving visibility, and by increasing the risk that offenders will be detected and recognised. Enhanced lighting has helped reduce crime and fear on the part of local residents (Painter 1994).

Closed circuit television (CCTV) in confined public places, as well as in commercial establishments, can also deter crime and facilitate the identification of offenders. CCTV evidence is often very convincing, and its availability can thus serve to increase the likelihood of a guilty plea, with consequent savings in court time and costs. Infra-red and light intensifying technologies may be adapted in order to enhance the capacity of CCTV, or applied to other observation devices. These can be used not only to locate suspects, but for the identification of persons lost or missing in certain areas (Hook 1997).

Developments in technology will lead to new applications for surveillance and detection, and these may be expected to become more widespread. Portable personal alarm systems are now available which enable the user to contact a friend, relative, or security service when in need of assistance. Such technologies are increasingly accessible to older citizens, whose freedom might otherwise be constrained by fear of crime or of other mishap. Such technologies offer reassurance, independent of any objective risk.

An entire new industry relating to information security has developed in recent years to provide safeguards against various forms of illegality involving telecommunications and information systems (Grabosky & Smith 1998). Maintaining the integrity of the many computer and communications systems on which all modern institutions now depend means that IT security will become one of the growth industries of the next century. Beyond this, information technology has given rise to new methods for the detection of crimes such as fraud and money laundering. Anomalous transactions can be instantly identified through applications of artificial intelligence.

A variety of technologies for location and tracking have begun to emerge as well. The LOJACK system involves a concealed transmitter in the chassis of an automobile, which may facilitate the vehicle's recovery if stolen (Clarke & Harris 1992). Global positioning systems, once the monopoly of defence institutions, have become more widely accessible (Worthman 1997). The technology now extends to cellular phones and to automobiles, enabling one to identify their precise location in the event of theft. It can also enable law enforcement to determine the exact location from which an emergency call is made, or to locate suspects, as was the case with the fugitive Pablo Escobar. The decreasing cost of this technology may well see it incorporated into the design of consumer electronics, or indeed other products, lessening their attractiveness to prospective thieves (*Policing Today* 1997).

They can also be used to track the location of questionable import and / or export shipments, as well as individuals, such as children or patients with Alzheimer's disease, who may be at risk of becoming lost (Schor 1995). Personal location systems may also be useful in monitoring the movement of persons on bail or probation, or individuals who may be subject to restraining orders.

The detection of explosives and firearms has taken on new urgency in many nations threatened by crime or terrorism. Canadian authorities use vapour detectors for bomb detection at airports (*Aviation Week and Space Technology* 1991); X-ray analysis of luggage is now routine at airports around the world.

New technologies currently under development for the detection of concealed weapons include Low-Level Scattered X-Rays and Computer Image Processing, Millimeter Wave and Long Wave Infrared Receivers, Radar and Ultrasound, and Low Frequency Magnetic Imaging (US National Institute of Justice 1996). All of these would permit law enforcement officers to detect concealed weapons at a distance, without the necessity of "frisking" a suspect.

Drug detection has also become a fertile area for technological development. Technologies of drug detection, from specially bred and trained "sniffer dogs" to infrared spectroscopy, permit the identification of illicit substances or ingredients used in their manufacture. Beyond the conventional testing of specimens such as urine, blood or hair, magnetic resonance imaging (MRI) is a non-invasive means of identifying contraband which has been ingested (Shaw et al. 1995).

Devices for the security of retail merchandise include products designed to self-destruct, or otherwise become readily identifiable if removed illegally— "ink tags" on apparel products designed with a four digit activation code are one example (Felson 1997, p. 91). Exploding dye packs have been commingled with cash to thwart bank robberies. On a more subtle level, copyright protection of a variety of information products can also be enhanced by embedded signatures and other software.

Another application of technology to criminal justice is the use of the Internet in furtherance of community policing. Police are now able to communicate more efficiently with the public; ease of public communication with the police is commensurately enhanced. Fugitive suspects have been apprehended as a result of their identifying details having been posted on the Internet. Online hotlines now facilitate the reporting of activities as diverse as fraud and child pornography.

One of the more significant developments in forensic science since the fingerprint is DNA testing. Not only has this technology been used to conclusively establish the guilt of a suspect, but it has also served to exonerate subjects of investigation and even persons who have been convicted of crimes which they did not commit (Connors et al. 1996).

Ballistocardiogram technology has given rise to "heartbeat detectors" which can find persons hiding in vehicles. Such technology can be useful in the prevention of escapes from lawful custody.

## Target Hardening: Technologies of Blocking and Access Control

Various methods have been developed which make crime more difficult to commit by impeding access to a target. Figuratively and sometimes literally speaking, these, together with surveillance, have come to be called "target hardening."

The era of the formidable padlock is giving way to "smarter" locking technologies. Howe and Blanchard (1994) describe a new motor vehicle security system that uses a wireless electronic link between the starter key and the car's computer system to allow or prevent ignition of the car. Retinal imaging, voiceprints, hand geometry readers, and other biometric technologies permit authentication of individuals with a precision not previously considered possible.

Packaging technology has developed special seals for "tamperproofing" a product, an important consideration given the recent history of extortion in a number of western industrial societies. So, too, have technologies been developed which make counterfeiting of currencies and other documents much more difficult than in the past. Australia's polymer notes are an example (James 1995).

Over and above what is simplistically termed "computer crime", applications of IT security to anti-theft systems have far-reaching potential. Consider, for example, a car radio designed not to operate once removed from the vehicle in which it has been installed. Similarly, the design of a television or VCR can require that a pin number be entered whenever the unit is disconnected from mains power for a prescribed period in order for it to function properly (*Policing Today* 1997). In the future, PIN numbers are likely to be replaced by biometric authentication and identification devices.

New technologies are also contributing to the development of "smart" guns—firearms engineered to prevent discharge by a person other than the authorised user. Activation of a firearm would depend upon radiofrequency identification or other type of authentication system (Schofield 1997). This can help prevent criminals from disarming, then shooting law enforcement officers. The application of this technology to privately-owned firearms can also lessen the risk of some forms of accidental or intentional misuse.

Technologies can also help protect law enforcement officers whose job may at times place them in situations of considerable risk. Soft body armour, for example, has saved the lives of more than 1500 police officers in the United States (Institute for Law and Justice 1995).

## Technologies of Restraint

One of the most frequently broadcast images over the past decade was the videotape of Rodney King being beaten by Los Angeles Police. Of less global notoriety, but of substantial public concern, is the relatively small number of Australians killed each year in encounters with law enforcement officers, not to mention death and injury sustained by police and prison officers in the course of their duties.

A free society will inevitably experience circumstances in which a few individuals, whether under the influence of alcohol or drugs, or who are otherwise violent or unruly, pose significant threats to themselves and / or others. Ideally, these threats would be addressed by policies directed at the fundamental causes of the dangerous behaviour in question, whether they involve mental illness, situational and social circumstances, or other factors. But realistically, acute threat situations will persist, and means of dealing with them must not be neglected. Put somewhat bluntly, the goal is to devise more benign alternatives to shooting someone to death, beating them into submission, or restraining them in such a manner as to risk positional asphyxia.

In addition to the various circumstances of those individuals who may be in a state of extreme agitation and aggressiveness, the settings in which technologies of incapacitation might be applied can differ widely. These can include high-speed pursuits in motor vehicles, to incidents involving fugitives on foot, to hostage and siege situations.

Among the basic technologies which may be applied to incapacitation are the following.

### *Vehicle interdiction*

High-speed pursuits are dangerous, posing significant risks to fugitives, law enforcement personnel, and innocent third parties alike. In Australia, 43 people died in police pursuits between 1 January 1990 and 30 June 1997 (Dalton 1997). A variety of technologies are under development for the incapacitation of motor vehicles.

One such method involves transmitting a short electromagnetic pulse which can damage the electronic components of a vehicle's ignition system and cause it to stall. The effect is similar to that which occurs when a car runs out of petrol.

A mechanically based alternative is the retractable spiked barrier strip which can be activated remotely prior to being driven over, and which can puncture and deflate the vehicle's tyres in a manner which allows the vehicle to be brought to a controlled stop. Both of the above technologies can be deployed on a roadway on either a temporary or, in designated security areas, a permanent basis, and activated as required.

Another device entails a tagging system for fleeing vehicles. This would involve a small adhesive projectile containing a radio-frequency transmitter which will permit identification of the vehicle's location.

### *Personal restraints*

**Vehicle airbags**. Under normal circumstances, it can be difficult to control suspects who become unruly when being transported in a police vehicle. A technology has been developed which allows a police officer to activate a rear-seat airbag from the front seat of a vehicle. The airbag inflates in such a manner that it restrains the rear seat passenger until he or she can be properly subdued.

**Nets**. Ensnarement nets may be launched from specially modified firearms to assist in the capture of attacking or fleeing offenders. Nets can be modified to incorporate adhesive properties, making it all the more difficult for the subject to extricate him or herself.

**Foams and Adhesives, and Lubricants**. Aqueous foam is water-based and can be sprayed in confined spaces. It suppresses sound, impairs vision, and can be disorienting. Sticky foam is a more viscous, nontoxic substance which may be used to immobilise an attacker from a distance of up to 15 metres. When directed at the legs, it can literally stop a person in his or her tracks.

By contrast, **anti-traction fluids** help constrain mobility in a different manner. When applied to certain surfaces, these substances make it extremely difficult for a subject to maintain his or her footing.

**Sound**. Acoustic weapons are under development for use in crowd control. Noxious aural stimuli can be used to disperse threatening crowds, or to guide them to prescribed locations.

**Light**. Portable lighting sources can be activated to deploy pulsed bright white light. These strobe lights can distract or disorient the suspect, and may cause temporary visual impairment.

**Chemical incapacitants**. So-called "tear gas" has been used for riot control for many years. Oleoresin capsicum, or pepper spray, can be introduced more effectively into a barricaded structure, with less risk of penetration into adjoining areas. It can also be used to temporarily disable an attacker by inducing a burning, tearing, and swelling of the eyes, and by restricting breathing.

**Electrical incapacitants**. Electric current may be transmitted to a suspect by direct contact with a special baton, or by a dart-like device fired from a distance.

**Pharmacological substances** with tranquilising properties may also be administered by dart.

A number of the above technologies are complementary. Pepper spray may be used with foam or water cannons; acoustic devices may be used with high intensity light, as in stun grenades, and / or with chemical agents (*U.S. News & World Report*, vol. 123, no. 1, pp. 38-46, 7 July 1997).

## Downside Risks

It is only realistic to suggest that over the past half century, the stresses of modern life have increased the number of persons who pose substantial risk to themselves or others. The development and implementation of social policies to alleviate these risks is not always feasible. As a consequence, this has created a demand for technologies for the more humane control of dangerous persons.

But the various technologies discussed above are not without risk. First among these is that they might be vulnerable to excessive use or use in circumstances where they are not warranted. The inappropriate use of force has been a familiar theme throughout the history of law enforcement. "Low-tech" methods for the repression of legitimate political expression are as old as the state itself. Technologies of surveillance, which were the stuff of science fiction not long ago, now pose significant risks to individual privacy.

Recent history is replete with examples of excessive and inappropriate use of many new technologies. Surveillance technologies have been deployed for voyeuristic purposes, rather than for purposes of public safety. Technologies of restraint have been used for purposes of punishment, indeed, torture, rather than for humane incapacitation in legitimate circumstances.

Under some conditions, they may in fact be injurious, if not lethal. Rubber bullets fired at an inappropriate range or velocity may damage organs. Pepper spray may be unsuitable for use on suspects with illnesses such as heart and respiratory disease (Granfield et al. 1994). Tranquilisers may suppress respiration, in a manner which can seriously compound the effects of alcohol or drugs. Microwaves may disturb brain waves, and heart rate, and cause burns and fevers (*U.S. News & World Report*, op. cit.).

New technologies for crime control can have adverse social impacts as well. Whatever the circumstances of their use, it should be borne in mind that these instruments are prone to be employed disproportionately against members of disadvantaged groups.

The use of "high-tech" means of restraint might well lead to changes in police practice. Easily available technological fixes may tempt one to rely on them to the extent that some of the traditional law enforcement skills become neglected. There is a real risk that community relations will be overlooked, and the art of interpersonal communications will be eroded if not lost.

Another risk which may accompany the introduction of new technologies for crime control involves the exploitation of technologies by the very persons against whom they are intended — criminals themselves. Already numerous accounts have begun to emerge of criminals using sophisticated communications and surveillance technology, as well as other devices such as body armour.

Perhaps less tangibly but no less importantly, the accumulation of various technologies of surveillance and control is regarded by some as imposing intolerable constraints on individual privacy and freedom. The metaphor of "Big Brother" is even more apposite in 1997 than it was in 1984. The balance between freedom and security in a democratic society is not one which can be struck lightly; it requires regular and open discussion.

It is not difficult to imagine circumstances in which citizens, whether or not they may have previously experienced acoustic disorientation or pepper spray, might be disinclined to exercise their democratic rights. Used excessively, some technologies may have a chilling effect on one's freedom of association and freedom of protest. It is likely that developments in law enforcement technology will be accompanied by evolution in civil liberties and human rights law.

Crime displacement is another unintended consequence of some technologies, especially those involving target-hardening. For example, more sophisticated vehicle anti-theft devices have lead to an increase in car hi-jackings — much more violent crimes than simple motor vehicle theft. There is also the risk that the burden of crime will be shifted to those prospetive victims who are unable to afford target-hardening devices.

## Principles for the Application of Technology to Crime Control in a Democratic Society

Despite their downside risks, new technologies for crime control should not be dismissed out of hand. Indeed, one could argue that every new technology, beginning with the wheel, has been accompanied by inherent risk and / or possibility of misuse. This is hardly justification for its outright rejection.

Criteria for the application of technology for crime control should include:

- **legality** — the technology and its use should be consistent with prevaling standards of human rights
- **cost-effectiveness** — the technology should be affordable and offer a fair return on investment
- **technical integrity** — the technology should suit the purpose for which it is used, and be safe and maintainable
- **accountability** — the use of the technology should be transparent and subject to rigorous oversight.

The development and refinement of new technologies should, to the greatest extent possible, "engineer out" risks, that is, minimise their potential to inflict collateral damage, and their vulnerability to tampering or exploitation by criminals.

It could perhaps be said that a new technology is only as good as the person or organisation using it. In the end, there is no substitute for careful recruitment, training and supervision of those law enforcement officers whose responsibility it will be to use new technologies for the ultimate benefit of the community.

If some of the new technologies of crime control are appropriate for wider use in our society by skilled and authorised criminal justice professionals, what additional principles might govern their introduction? First and foremost, it is essential that they not be introduced by stealth. The development and deployment of crime control technology should be based on thorough consultation. To do less would run the risk of bringing the entire criminal justice system into disrepute.

It is not sufficient to assume that new technologies of crime control will automatically lend themselves to responsible use. Some may be prohibitively expensive, or logistically cumbersome to deploy. Extensive testing should precede their operational use. As is the case with any weapon, those who use them should be given appropriate training and supervision. Policies and procedures for the use of new instruments should be no less rigorous than those relating to the use of force.

Mechanisms of accountability must be as strong as ever.

As a general principle governing the use of technology in furtherance of criminal justice, one could hardly improve upon the work of Braithwaite and Pettit (1990). They would argue that interventions which curtail individual autonomy should be deployed no more than necessary, and only to the extent that they maximise the overall level of freedom in society. The public should be the ultimate beneficiaries of new crime prevention technologies.

New technologies, most notably those relating to telecommunications, have great impact on both sides of the crime control effort. There is significant potential for access to and exploitation of technology by criminals (Smith forthcoming). Indeed, it has been said that "Crims have got all the money and no rules, while Cops have got all the rules and no money." Ongoing assessment is necessary to ensure that new technologies prevent more crime than they facilitate.

Technology, therefore, is by no means a panacea. Nevertheless, for all their inherent risks, new technologies for criminal justice can lead to greater security for citizens, and reduced hazards for criminal justice professionals.

## References

*Aviation Week and Space Technology* 1991, "Transport Canada uses vapor detection with other steps to ensure security", *Aviation Week and Space Technology*, 25 March, vol. 134, no. 12.

Braithwaite, John & Pettit, Philip 1990, *Not Just Deserts: A Republican Theory of Criminal Justice*, Oxford University Press, Oxford.

Chenery, Sylvia, Holt, John & Pease, Ken 1997, *Biting Back II: Reducing Repeat Victimisation in Huddersfield*, Police Research Group, Crime Detection and Prevention Series Paper 82, Home Office, London.

Clarke, Ronald V. & Harris, Patricia M. 1992, "Auto theft and its prevention" in *Crime and Justice: A Review of Research*, ed. M. Tonry, vol. 16.

Connors, Edward, Lundregan, Thomas, Miller, Neal & McEwen, Tom 1996, *Convicted by Juries, Exonerated by Science: Case Studies in the Use of DNA Evidence to Establish Innocence after Trial*, National Institute of Justice, Washington.

Dalton, V. 1997, *Australian Deaths in Custody: Deaths Resulting From Police Pursuits 1 January 1990 to 30 June 1997*, Australian Institute of Criminology, Canberra.

Felson, Marcus 1997, "Technology, business and crime" in *Business and Crime Prevention*, eds M. Felson & R.V. Clarke, Criminal Justice Press, Monsey, NY, pp. 81-96.

Grabosky, P.N. & Smith, R.G. 1998, *Crime in the Digital Age: Controlling Telecommunications and Cyberspace Illegalities*, The Federation Press, Sydney.

Granfield, John, Onnen, Jami & Petty, Charles S. 1994, "Pepper spray and in-custody deaths", *Science and Technology*, International Association of Chiefs of Police, Alexandria, VA.

Hooke, Patrick 1997, "Night vision", *Police Review*, 22 August, pp. 30-1.

Howe, Harlan & Blanchard, Christine 1994, "Special report: Wireless technology for automobile theft prevention", *Microwave Journal*, vol. 37, no. 1, p. 24.

Institute for Law and Justice 1995, *Law enforcement options: Newsletter on less-than-lethal technology development*, vol. 1, no. 1, Institute for Law and Justice, Alexandria, VA.

James, Marianne 1995, "Preventing the counterfeiting of Australian currency", in *The Promise of Crime prevention*: *Leading crime prevention programs*, Australian Institute of Criminology, Canberra, pp. 12-13.

NRMA Insurance Limited 1996, *Household Burglary in Eastern Australia, 1995-96*, NRMA Insurance Limited, Sydney.

Painter, Kate 1994, "The impact of street lighting on crime, fear, and pedestrian street use", *Security Journal*, vol. 5, no. 3, pp. 116-24.

Pilant, Lois 1997, "Research: Applying it on the front lines", *Science and Technology*, National Institute of Justice, Washington.

*Policing Today* 1997, "Smart chips to foil TV thieves", *Policing Today*, Sept, p. 8.

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

Schor, M. J. 1995, "Miniaturized global tracking device for law enforcement applications", in *Counterdrug Law Enforcement: Applied Technology for Improved Operational Effectiveness International Technology Symposium*, Part 2; Proceedings, pp. 15-19, 15-23. Office of National Drug Control Policy, Washington.

Shaw, J.D., Magnuson, E. E., Sheldon, A.G. & Burnett, L.J. 1995, "Screening System for Detection of Contraband Swallowed Narcotics" in *Counterdrug Law Enforcement: Applied Technology for Improved Operational Effectiveness, International Technology Symposium, Part 2; Proceedings*, Office of National Drug Control Policy Washington, DC, pp. 17-33.

Smith, R.G. (forthcoming), "The Technologies of Crime", Trends and Issues in Crime and Criminal Justice Series, Australian Institute of Criminology, Canberra.

United States, National Institute of Justice 1996, "Hands off frisking: High-tech concealed weapons detection", *Technology Beat*, June, pp. 1-4.

United States, National Institute of Justice 1997, "Applying technological advances to criminal justice", *National Institute of Justice Journal*, June, pp. 11-15.

Worthman, Ernest 1997, "Global positioning systems", *Mobile Radio Technology*, vol. 15, no. 5, p. 58.

ACKNOWLEDGEMENTS:
The author is indebted to Mr David Boyd of the (US) National Institute of Justice, Dr Barend Taute of the Council on Scientific and Industrial Research (South Africa), Professor John Murray of the Australian Graduate School of Police Management, and Dr Russell Smith of the Australian Institute of Criminology for their comments on earlier drafts of this paper.

Dr Peter Grabosky is
Director of Research, 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