

CRIME AND TECHNOLOGY IN THE GLOBAL VILLAGE

P.N. Grabosky
Australian Institute of Criminology

*Paper presented at the conference: Internet Crime
held in Melbourne, 16-17 February 1998, by the Australian Institute of Criminology*

1. Introduction.

This paper can be encapsulated in two quotations:

The first is from Willie Sutton, a notorious American bank robber of a half century ago, who was asked after one arrest why he persisted in robbing banks. "Because that's where the money is," he is said to have replied.

The second is from a former Governor of California, who was asked at his inaugural press conference what he was going to do about the state's rising crime rate. His reply was "Well, personally, I'm going to keep low, move fast, and not carry a lot of cash."

It would be trite to suggest to this audience that technology is changing the way we live. It may perhaps be somewhat less trite to suggest that technology is changing the face of crime, in Australia and around the world.

This is not to suggest that we are about to see the end of murder, rape, robbery, and housebreaking as we know them. Quite the contrary. The basic risk factors for these conventional crimes exist in abundance in Australia, and are not likely to diminish in our lifetime.

What has changed, and will continue to change in our lifetime, as sure as night follows day, is technology. This has, and will, generate new opportunities for crime. In the words of Willie Sutton, "That's where the money is." Fortunately for us honest folks, technology will also create new opportunities for crime control.

It has also become trite to suggest that the world is a shrinking place. On the one hand, this shrinking is highly beneficial. Australians now enjoy economic, cultural and recreational opportunities which were previously not accessible. On the other hand, the global village has its dark alleys. Once shielded by vast distance from some of the more unpleasant aspects of life elsewhere in the world, Australia is now subject to dangerous influences emanating from around the globe. In this regard, it is perhaps now appropriate to speak of "The tyranny of proximity."

The rapid mobility of people, money, information, ideas, and commodities generally, has provided new opportunities for crime, and new challenges for law enforcement agencies. Linkages between events and institutions at home and abroad are inevitable, and will inevitably proliferate. This has profound implications for many Australian institutions, law enforcement among them.

Those issues which lie at the intersection of crime, technology and globalization and which form the basis for this conference, are nothing, if not timely. If they are not already high on the policy agenda, they are destined to find their way there soon. This conference will focus on the criminal applications of what we refer to as the internet, or more broadly the convergence of computing and communications. Let us look just briefly at what lies in store for us over the next two days.

Internet Vandalism and Terrorism.

In today's world, where computers and communications systems are linked, it can truly be said that "everything depends on software." It is bad enough that this has proven irresistibly seductive to pranksters. The potential damage which can be inflicted on our infrastructure-- systems such as air traffic control, power, telecommunications, and the like, by a malicious person sitting at a keyboard on the other side of the planet, is mind-boggling. So significant, in fact, that considerable attention is being given around the world to its military applications.

Offensive content.

Content of every conceivable variety may be found in cyberspace. Erotica, racist propaganda, information relating to the manufacture of drugs and explosives, and instructions on how to commit suicide, now lie at one's fingertips. How to protect children and those who are easily offended, while allowing the emerging medium of the internet to flourish, has become a challenge to most governments, and to many parents, in the developed world.

The protection of intellectual property.

Possibilities for forgery, plagiarism, and other offences against intellectual property have been significantly enhanced by the advent of digital technology. Piracy has become a growth industry, so much so, that it may strain the capacity of governments to control it. Here again, a fundamental policy question is whether state enforcement is preferable to self-help on the part of the individual. Are private precautions and private remedies sufficient in most cases?

Private legal solutions are likely to be more effective within jurisdictions than across them. One would not expect Microsoft, for example, to receive a great deal of comfort from the legal process of the People's Republic of China. Organisations with access to considerable resources, may, however, pursue telecommunications offenders across the globe. A recent example involves the protracted litigation being taken by the Church of Scientology in respect of alleged copyright infringements on the Internet. In a series of actions taken in various jurisdictions in the United States as well as in the Netherlands, the church has sought interim orders restraining the publication of materials on the Internet which are said to infringe its copyright. Such remedies do not come cheaply, however, and one of the problems of private remedies is that they are only available to those who are able to afford them.

Commercial crime.

It seems only a matter of time before most commerce will be electronic. Then, to invoke the ghost of Willie Sutton, that's where the money will be. The proliferation of electronic funds transfer systems will enhance the risk that such transactions may be intercepted and diverted. How to facilitate commerce in the digital age, and how to obtain a competitive advantage, while ensuring the security and integrity which is essential for commerce to flourish, has become the question of the hour.

The above forms of illegality are not necessarily mutually exclusive, and need not occur in isolation. Just as an armed robber might steal an automobile to facilitate a quick getaway, so too can one steal telecommunications services and use them for purposes of vandalism, fraud, or in furtherance of a criminal conspiracy.

International legal controls.

The global nature of information technology enables criminal activity to be truly transnational. That is, a person sitting in Spain can disable a computer in Singapore, or disseminate child pornography in Swaziland. Additional problems arise from the difficulty of exercising national sovereignty over capital and information flows. Jurisdictional issues may arise from transborder online transmission. If an online financial newsletter originating in Albania contains fraudulent speculation about the prospects of a company whose shares are traded on the Australian Stock Exchange, where has the offence occurred?

The globalization of crime poses further problems, as the cost of investigating and prosecuting transnational crime may be prohibitive in all but the most serious cases. Sovereign governments are finding it difficult to exercise control over online behaviour at home, not to mention abroad. A resident of Chicago who falls victim to a telemarketing scam originating in Albania, for example, can expect little assistance from law enforcement agencies in either jurisdiction. As a result, regulation by territorially-based rules may prove to be inappropriate for some types of offences.

Of equal concern is the lack of international consensus on what constitutes criminal behaviour. What is treasonous in Tibet, or blasphemous in Bangladesh, is protected in Philadelphia. New international arrangements are being crafted to address these issues. Will they be adequate to meet the challenge?

Local Legal Controls

Even without a transnational dimension, tasks facing law enforcement in the digital age are formidable. Emerging technologies of encryption may reduce the extent to which criminal communications are vulnerable to interception. Will this require new technologies, new laws, or rather increased reliance on labour intensive undercover investigations? The collection of electronic evidence is still a novel experience for many law enforcement officers. Proof of possession of illegal materials or of criminal intent may be more difficult to achieve than would be the case with conventional criminal prosecutions.

Ironically, it would appear that some aspects of crime involving high technology will be best addressed by relatively low tech solutions. One thinks, for example, of the use of undercover investigative methods.

Meanwhile, there remains the challenge of balancing the public interest as articulated by law enforcement, with the public interest as articulated by advocates of privacy rights. Under what circumstances should service providers disclose subscriber information to law enforcement authorities? Short of this, the very transparency of much traffic on the information superhighway may cause concern to some.

Consider, for example, navigational data, the figurative “footprints” which one leaves as one traverses cyberspace. Accessible to commercial institutions, such data have become a powerful marketing tool. One can, for example, receive personalized advertising based on one’s previous online usage. If I were a football enthusiast, for example, and a frequent visitor to AFL websites, I might be pleased to be notified of a special promotion, or an offer to buy a St Kilda jersey. But as you might imagine, this is not necessarily an unmitigated good. Just last month, I did some web surfing in response to a request from my Director to prepare some briefing notes on the subject of sex slavery. I cringe to think what one might be inclined to infer from my navigational data!

On the brighter side, the information superhighway does have benefits for law enforcement agencies. Although its potential has yet to be realized, the use of technology for general public relations, for the communication of basic information for crime prevention, and for the exchange of information in furtherance of criminal investigation may be expected to increase dramatically in years ahead. Already photographs displayed on the Internet have led to the arrest of fugitives. The activities of pornographers and software pirates (as well as innocent criminologists) may be traced effectively using information available on the Internet.

On-line crime prevention.

This raises the question about prevention of internet crime, and the extent to which the principles of terrestrial crime prevention may be applied in cyberspace. Opportunity reduction and target hardening, which have become key elements of situational crime prevention, would appear to be as applicable to information systems as to residential dwellings. Whether principles of developmental crime prevention will be similarly generalizable is open to question.

Technological Controls.

It does in any event appear that technological solutions will play a significant role in ensuring security and prosperity in cyberspace. I am reminded of the film “The Graduate,” now three decades old. The scene in which an older man took the young Dustin Hoffman aside and said, with a view towards pointing him towards a prosperous career, “Son, I have one word for you--Plastics.” Today, I would say, “Son, I have two words for you--computer security.” Few would argue that this will be one of the growth industries of the next century. In addition to more rigorous management practices and the introduction of more sophisticated password and verification procedures, new technologies such as biometric security devices and anomaly detection computer software help alert users to system weaknesses and enhance the security of computer systems themselves. I look forward to learning more about this during tomorrow afternoon’s session.

One topic conspicuous in its absence from this conference is gambling. The challenge of regulating gambling in cyberspace is considerable. In part it will be addressed in the panels dealing with content regulation and commercial criminality. But it will also be the subject of a special AIC conference in a few weeks’ time. As our Deputy Prime Minister would say, “Watch this Space.”

So these are some of the themes which will be addressed over the next two days. Let me touch briefly on just a couple of threads which may run through them.

Technological leap-frog.

First is what might be called technological leap-frog-- the ongoing contest between the state and the offender to gain the technological edge. New technologies, most notably those relating to telecommunications, have great impact on both sides of the crime control effort. It is no secret that some of the more sophisticated offenders today are able to afford state of the art technology. Indeed, it has long been said that "Criminals have got all the money and no rules, while Cops have got all the rules and no money." Keeping abreast of developments in technology will remain an ongoing challenge to law enforcement agencies in Australia and around the world.

New opportunities for democratic participation in the control of internet crime.

New technologies provide new opportunities for citizenship. Opportunities for a citizenry to inform itself are unprecedented. Opportunities to communicate with government are unprecedented.

Perhaps one of the most important developments is the availability of facilities by which a citizen can report suspected illegality to service providers or to authorities. So-called "hotlines" encourage the private monitoring and surveillance of cyberspace, and the reporting of suspicious activity, including consumer fraud, racist propaganda, and child pornography. This can be healthy, as long as it does not degenerate into a field-day for busybodies and an impediment to legitimate communication. Moreover, well meaning amateurs can violate the privacy of innocent citizens and contaminate legitimate criminal investigations.

For some time now, we have been encouraged to think in terms of self-reliance and decreased dependence upon the state. Limited resources available to governments now require that careful thought be given to the nature and amount of services which it is appropriate for governments to deliver.

Recall the quote attributed to the former Governor of California "Keep low, move fast, and not carry a lot of cash."

What is the relevance of this? The first line of protection against internet crime is self help.

Given the limited capacity of governments to control crime in cyberspace, the first line of defence lies in the exercise of prudent behaviour by prospective victims. Just as the first step in the control of burglary is to lock one's doors and windows, so too the basic principles of information security should be honoured.

Market forces may also exert controlling influences of their own. As large organizations begin to appreciate their vulnerability to electronic theft or vandalism, they may be expected to insure against potential losses. It is very much in the interests of insurance companies to require appropriate security precautions on the part of their policyholders. Indeed, decisions to set and to price insurance may well depend upon security practices of

prospective insureds. Subcontractors may also be required to have strict IT integrity programs in place as a condition of doing business.

Counterproductive interventions.

The last theme on which I would like to dwell is that of counterproductive interventions, whether they originate from public or from private sources.

It is an understandable reaction to any perceived social evil to attempt to legislate it away. Early efforts to regulate internet content are illustrative. In some instances, these efforts have been grounded jointly in cynicism and realpolitik. I recall one discussion I had with a policymaker who had presided over the development of a piece of legislation which criminalized depictions of indecency. As respectfully as I could, I surmised that the law would be difficult, if not impossible to enforce. With complete candour, he intimated that enforcement was not the object. The real goal was to be seen to be doing something, and thereby to mollify the vocal minority which had become increasingly agitated about some of the more sordid corners of cyberspace.

Similarly, attempts to prohibit anonymous online communications may discourage legitimate expression such as that involving whistleblowers or human rights advocates residing within the jurisdiction of repressive regimes.

Although the rush to regulate, or to criminalize, may have political resonance, it may have downside consequences. “Burning the house to roast the pig” may be an awkward metaphor, but it fits here.

Even private remedies may be excessive. Already one sees criticisms of blocking and filtering software which automatically deny access to breast cancer support groups.

The risk, or indeed, the fact, that freedom of speech will be abused by some, is insufficient justification for “pulling the plug” on telecommunications. One must always bear in mind that excessive constraints on freedom of expression and communication may inhibit the realization of competitive advantage.

Conclusion

Over the past few minutes, I have raised more questions than I have answered. I make no apology for this, for the speakers scheduled to present over the next two days are better suited than I for this latter task. Let me leave you with a message which will be no news to you, but which you yourselves may wish to assist in disseminating more widely.

Don't shrink from a new technology just because it may be subject to criminal abuse. Exploit its strengths, while controlling its weaknesses. This will be the way to survive in an increasingly competitive world.