AUSTRALIAN INSTITUTE OF CRIMINOLOGY

trends & issues

in crime and criminal justice

No. 54

Stealing Telecommunications Services

Russell G. Smith

Since Wheatstone and Cooke first patented their system of communication by the means of electromagnetic impulses carried over wires in 1837, crimes have been committed either through the misuse of telecommunications equipment, or against telecommunications equipment. Every technological development has provided a new opportunity for criminality which has often been utilised. Unfortunately, as we move into the twenty-first century where broadband telecommunications services such as interactive video telephony will become widely available, the opportunities for criminality will be enhanced. Now is the time to develop strategic responses to the regulatory challenges which this new technology brings.

This paper is the first of a series of papers from the Institute's research program on telecommunications and crime.

Adam Graycar
Director

Since the first telegraph service was used in Melbourne in 1854, communications technology in Australia has developed rapidly. At present, Telstra alone has some 8.6 million customers who make around 25 million calls a day.

By far the most important development in telephony in recent years has been the introduction of cellular mobile telephone services which were introduced in Sydney and Melbourne around 1987. There are now approximately 3 million mobile telephone subscribers in Australia who spend between A$10 and A$500 a month on their calls, thus creating a market estimated to be worth A$3.5 billion a year. By the end of 1996, it is estimated that approximately 1.5 million mobile telephone subscribers will be using digital technology (Crowe 1996, p. 16), while by the year 2000, Optus has estimated that some 8 million mobile telephones will be in use (O'Neill 1996, p. 22). Unfortunately, not all of these users will pay for the services they obtain.

In the field of television broadcasting, the cable industry in the United States is worth the equivalent of A$25 billion with more than 11 000 cable operators servicing over 57 million paying customers, creating considerable potential for illegally obtaining services (Schieck 1995, p. 2). Once again, this potential for criminality will pose a concern for Australia in the next century.

This paper considers how best to regulate the provision of telecommunications services so as to minimise the opportunities for theft while at the same time deterring potential offenders from embarking upon acts which use telecommunications equipment for personal gain.

April 1996

ISSN 0817-8542
ISBN 0 642 24012 4

Australian Institute
of Criminology
GPO Box 2944
Canberra ACT 2601
Australia

Tel: 06 260 9200
Fax: 06 260 9201

Extent of the Problem

Statistical information concerning the size of the problem of theft of telecommunications services is scant, particularly in Australia. Recent British Telecom (BT) statistics suggest, however, that in 1990, security failures at BT cost approximately the equivalent of A$595 million, while telephone fraud in the United States amounts to the equivalent of A$5.3 billion annually. In 1993, the cable television industry lost nearly A$6.6 billion in the United States alone (Schieck 1995, pp. 2-5). Olson (1994, p. 12) cites some recent examples of telecommunications fraud including an American chemical company which lost the equivalent of A$900 000 in three weeks and an Ohio manufacturer who lost A$400 000 over one weekend. In Australia since 1990, one international telephone fraud operation cost the Commonwealth A$400 000, while another resulted in a company losing A$50 000 in unauthorised ISD call charges (Australian Federal Police 1993, p. 16; 1994, p. 21).

Mobile telephone fraud is a more recent area of concern. In the United States, Brooks and Davis (1994, p. 67) estimate that cellular telephone fraud is costing over a million dollars a day to the industry, with the equivalent of A$900 million a year lost on illegal calls actually detected. In Britain, the Parliamentary Office of Science and Technology (1995, p. 28) estimates that between twelve and fifteen thousand analogue and up to 1000 digital mobile telephones are stolen each month while subscription fraud is estimated to amount to the equivalent of A$144 million per annum or 1 per cent of network turnover.

Legal Background

Illegal use of telecommunications services falls within various State and Territory property crimes covering theft of electricity and other forms of intangible property (*Crimes Act 1900* (NSW) s. 154C; *Criminal Law Consolidation Act* 1935 (SA) s. 154; Queensland Criminal Code s. 408; Western Australian Criminal Code s. 390; Tasmanian Criminal Code s. 233) as well as a variety of Commonwealth legislative provisions.

Sections 76A to 76F of the *Crimes Act 1914* (Cwlth) create various offences to do with computers, such as unauthorised use and damage and these may be relevant where telecommunications equipment is used to gain unauthorised access to computers connected via networks. In addition, interference with the components of a telephone (especially a mobile telephone) may infringe some of these provisions.

More specific offences relating to the improper use of telecommunications services are contained in sections 85ZB to 85ZKB of the *Crimes Act 1914* (Cwlth), the most relevant of which relate to defrauding a carrier of any rental, fee or charge or causing a service to be supplied to another person without payment of the proper rental, fee or charge (s. 85ZF—5 years' imprisonment), interfering with, or using devices to interfere with telecommunications facilities in such a way as to hinder the normal operation of the service (s. 85ZG—2 years' imprisonment), tampering or interfering with a facility belonging to a carrier (s. 85ZJ—1 year's imprisonment) and manufacturing, advertising, selling, using or possessing unauthorised call-switching devices other than for bona fide purposes (s. 85ZKA—5 years' imprisonment).

In addition, section 253 of the *Telecommunications Act 1991* (Cwlth) creates an offence of knowingly or recklessly connecting unauthorised equipment to a network and section 7 of the *Telecommunications (Interception) Act 1979* (Cwlth) creates an offence of improperly intercepting a communication passing over a telecommunications system.

Applying these provisions to offences committed in respect of mobile telephones creates problems in view of the many novel ways in which such frauds may be perpetrated. For example, the act of cloning a mobile telephone (*see* Table 1) may involve crimes of theft, various computer crimes, as well as a number of telecommunications offences.

Although this legislative armory is extensive, it is not certain that it will cover future offences involving theft of telecommunications services.

One of the main concerns involving the prosecution of individuals who steal telecommunication services is the variety of legislative provisions which operate in different jurisdictions (*see*, for example, the enormous range of offences which exist in OECD countries relating to theft of telecommunications services: OECD 1986, pp. 56-60).

In Australia, the *Crimes Act 1914* (Cwlth) expressly applies throughout the whole of the Commonwealth as well as beyond the States and Territories (s. 3A) and this provision has been used to permit the prosecution of a computer crime involving telecommunications services which took place in Victoria but which involved a number of overseas jurisdictions (*R. v Jones*, County Court of Victoria, 3 June 1993).

Thus, although it may be legally possible to prosecute offenders who make illegal use of services between various jurisdictions, even internationally, significant problems may arise in detecting such illegality and in proving allegations successfully.

How are Services Stolen?

Table 1 summarises the principal ways in which telecommunications services have been stolen throughout the world over the last thirty years, along with various control and preventive strategies. This information has been compiled from a number of sources including Clough and Mungo (1992), Delaney (1993), Brooks and Davis (1994), Sulc (1994) and Denning (1995). A number of the types of theft referred to in Table 1 relate only to services available in the United States and some are now effectively prevented by technological and other solutions.

Policies for the 21st Century

Areas of emerging crime

The Commonwealth Bureau of Transport and Communications Economics Final Report, *Communications Futures* (1995), identifies the technological developments which are likely to be influential on residential markets in the period 1995 to 2005. The Report notes the importance of mobile communications, the Internet, private data networks and the growing convergence of computing and communications technologies and products. The emergence of pay television and the subsequent evolution over the next decade into other broadband products such as video-on-demand and switched broadband services including video telephony were also mentioned as likely developments.

If such developments take place on a wide scale, new social divisions could emerge based upon access to and familiarity with the new technologies. A new environment conducive to criminality may be created in which theft of telecommunications services will become a major problem. In a recent study by Coutorie (1995) in which the opinions of various experts were canvassed in order to predict the types of crimes which would be prevalent in the future, experts from traditional law enforcement backgrounds and a parallel group of highly proficient hackers both agreed that computer system attacks via telecommunications systems would be an area of concern (1995, p. 26).

The financial implications could be astounding for business as new telecommunications services, initially, will be much more expensive than standard telephony services which, even at present, lead to substantial losses for those in the industry. The motivation to steal services will be enhanced and unless adequate precautions are taken, organised crime may emerge as a major limiting factor in further business and technological developments taking place. Put simply, customers may be reluctant to take up the new technologies through fear of falling prey to telecommunications fraudsters, while organisations may be reluctant to invest in enterprises if crime-related losses are thought to be substantial and a real possibility.

Regulatory Reform

In deciding how best to approach the problem of telecommunications crime and particularly the theft of services, policy makers may choose to proceed down a variety of paths. One is to take legislative and administrative action to deal with the problem before it becomes unmanageable.

The path of criminalisation has, however, a number of dangers. First, is the difficulty, noted by Dunning (1982, pp. 293-4), of over-codifying behaviour:

> *one does not want to enact a new provision every time a new permutation of criminal behaviour arises. Ideally, the elasticity of a common law system will supply the omissions of the legislature but there are limits to which our judiciary will, and indeed can, go.*

As we have already seen, there is a wide array of criminal offences which govern the use of telecommunications systems and although these have not been rigorously interpreted as yet, it is likely that they will encompass most situations in which services are stolen. Where omissions exist, Parliament could enact specific laws with limited effect. For example, the United Kingdom Parliamentary Office of Science and Technology (1995, p. 30) has suggested criminalising the re-chipping of mobile telephones, possession of re-chipping equipment, interception of network security data and the possession of radio scanners.

In order to prevent any negative effects of such laws on the industry, it may be preferable to focus new laws on those who manufacture and distribute goods which are utilised in carrying out illegal activities rather than enacting strict liability offences relating to the possession of illegal equipment by consumers. Any legal reforms and other regulatory strategies should be based on the results of wide community consultation and should be uniform throughout the States, Territories and Commonwealth and, hopefully, consistent with international strategies.

Alternatively, a more cautious approach to regulation may be preferable. Arguably, this could best be achieved by self-regulation in the industries concerned and by a realisation that both the providers and users of services have a role to play in protecting their own interests and in preventing illegality for the benefit of all concerned. This point was emphasised recently in relation to the regulation of computer Bulletin Boards in the Report of the Computer Bulletin Board Systems Task Force (Commonwealth of Australia, Attorney General’s Department and Department of Communication and the Arts 1994, p. 9).

Table 1. *Theft of Telecommunications Services*

Offence Type	Method	Control Strategy
Metering System		
Switching System By-Pass ("Blue Box")	Device which generates tones to by-pass switching systems	Technological countermeasures
Meter Inhibition ("Black Box")	Device which prevents metering from being initiated	Technological countermeasures
Coin Drop Simulation ("Red Box")	Device which emits tones which simulate the sound of coins dropping	Technological countermeasures
Bent Wire	Defeats call charging equipment on public telephones	Technological countermeasures
Interference with External Software	Interfering with public telephone software to get international calls at local rates	Software improvement
Free Lines	The provision of non-metering exchange lines to subscribers	Operational controls
C5 Fraud	Use of tone simulators on 0800 IDD services to obtain the destination country's network free	Operational controls
Counterfeit Debit Cards	Use of unauthorised debit cards in public telephones to obtain free calls	Technological countermeasures
Billing System		
Free COCOT Services	Using customer operated coin telephones (COCOT) to obtain access to free dial tones	Technological countermeasures
Third Party Billing	Charging calls to home accounts without authorisation	Subscriber identification and authentication
Telephone Calling Cards	Charging calls to accounts using stolen, unallocated, expired or bogus telephone calling cards	Account and card authentication
Non-Existent Account Billing	Charging calls to non-existent accounts or third party accounts	Account authentication
Telex Answer-Back	Using telex answer-back codes to pass on charges to third parties	Subscriber identification and authentication
Telex Handling Charges	Defaulting on the payment of telex handling charges	Subscriber identification and authentication
0055 Premium Services	Establishing multiple 0055 services to receive profits and defaulting on payment of service fees	Subscriber identification and authentication
Mass Pager Billing of High-Cost Calls	Engaging a high-cost-to-caller line and sending mass messages for pagers to call this number	User risk awareness education
Telephone Exchange		
Small Exchange IDD Access	Obtaining access through small exchanges for IDD services	Exchange personnel screening
IDD Call Diversion	Use of exchange-based call diversion services to obtain IDD calls for free	Technological countermeasures
Public Telephone Reverse Charge Schemes	Using automatic calling number identifiers to obtain reverse charge calls to public telephones	Technological countermeasures
Meter Registration	Causing exchange-based meters to register lower usages than actually incurred	Technological countermeasures
Private Automatic Branch Exchange		
PABX Dial-Out Billing	Improperly using a PABX dial-out code to bill outside calls to the owner of the PABX	PABX code security enhancement
Direct Inwards System Access (DISA)	Charging calls to PABX without authorisation	PABX user identification and authentication
Network Looping (Weaving)	Using PABXs to gain improper access to networks and defaulting on payment of network access fees	PABX user identification and authentication
Telephone and Cable TV Lines		
Unauthorised Teeing-In to Public Telephones	Interception of cables serving public telephones to obtain free international calls	Line surveillance and protection
Unauthorised Teeing-In to Private Subscribers' Services	Unauthorised connections to subscribers' lines to bill calls without their knowledge or permission	Line surveillance and protection
Hacking into Unallocated Lines	Obtaining access to unallocated lines to obtain calls without paying	Line information controls
Unauthorised Re-Connection	Unauthorised activation of disconnected services	Technological countermeasures
Unauthorised Teeing-In to Cable TV Lines	Obtaining Cable TV services without being a subscriber	Line surveillance and protection
Unauthorised Cable TV De-Coding	Obtaining Cable TV services without the use of subscriber decoding devices	Subscriber identification and authentication
Telecommunications Equipment		
Theft of Telecommunications Equipment	Stealing any telecommunications equipment	Traditional theft prevention strategies
Mobile Telephones		
False Subscriptions	Taking out a subscription using false identification details and failing to pay fees incurred	Subscriber identification and authentication
Counterfeiting (Cloning)	Identifying an analogue telephone Electronic Serial Number/Mobile Identification Number (ESN/MIN) combination and reproducing this in another telephone to bill calls to another subscriber	Security of numbers, software analysis of call patterns and usage, making scanners illegal
Roaming Fraud	Frequently changing analogue telephone ESN/MIN combination to obtain calls prior to billing (not in Australia)	IS-41 and IS-54 call validation technology
Network and Billing Weaknesses	Utilising similar network weaknesses as with wired telephones	Technological countermeasures
Non-Payment of International Accounts	Subscribing in one country and making calls in another without settling account in home country	Subscriber identification and authentication
Theft of Mobile Telephones	Using a stolen mobile telephone until the owner reports it stolen	Restricted access using PINs and early reporting
Telecommunications Employees		
Test Desks	Improper use of test desk facilities to connect third party IDD calls for profit	Personnel screening and operational controls
Exchange Test Line Interception	Obtaining access to test lines in exchanges to permit IDD calls to be made at a local rate or for free	Personnel screening and operational controls
Exchange Trunk Test Line Interception	Using exchange-based trunk line testing facilities to connect third party IDD calls at a local rate or for free	Personnel screening and operational controls
Faultman's Ring-Back System	Using automatic test equipment to gain improper access to trunk networks for free	Personnel screening and operational controls
Improper Operator Connections	Operators improperly connecting third-parties for profit without charging or allowing extended time calls	Personnel screening and operational controls

The Role of Crime Prevention

Traditional strategies

Traditional crime prevention strategies will continue to offer many opportunities for combating the activities of offenders who operate in the high-technology world of telecommunications and who are motivated by greed and a desire for personal gain. Applying Clarke's (1995, p. 109) categories of situational crime prevention to the present context yields the techniques shown in Table 2 which may be utilised to prevent the theft of telecommunications services.

Table 2. *Traditional Crime Prevention Strategies* (based on Clarke 1995)

Increasing the effort	
Target hardening:	Tamper-proof telephones and lines
Access control:	Passwords, PINs, tokens,biometrics and encryption
Deflecting offenders:	Use of computer games and the Internet
Controlling facilitators:	Registration of telephones facilitators and service users, caller identification
Increasing the risks	
Entry/exit screening:	Checks on use of passwords and PINs
Formal surveillance:	Computerised auditing use of services and billing
Surveillance by employees:	Public telephone, location, carrier audits
Natural surveillance:	Carrier employee reporting of colleagues
Reducing the rewards	
Target removal:	Government or industry funded services, phonecards
Identifying property:	Registration of telephones and equipment
Removing inducements:	Restricted publicity of crimes and criminal gains
Rule setting:	Clarification of telephone billing procedures

While these traditional responses may be appropriate to deal with existing forms of theft of telecommunications services, policy makers may need to be more imaginative in the crime prevention strategies they consider and look to various alternative controls to deal with offences of the future. Some of these are as follows.

Opportunity reduction

Telecommunications carriers are well placed to reduce many of the opportunities for offending and, indeed, sub-section (1) of section 47 of the *Telecommunications Act 1991* (Cwlth) requires carriers

> *to do their best to prevent telecommunication networks and facilities . . . from being used in, or in relation to, the commission of offences against the laws of the Commonwealth and of the States and Territories.*

For example, carriers should conduct reasonable identification checks on new subscribers by requiring readily verifiable information to be provided.

In the United States, where obvious fraud prevention steps have not been taken by carriers, some subscribers have argued in civil proceedings that they should not be held personally liable for fees incurred by reason of telecommunications fraud where the carrier has acted negligently in failing to ensure that systems operate securely.

In relation to mobile telephone offences, some carriers have refused to permit subscribers to use Subscriber Identification Module (SIM) cards on other countries' networks without first having undergone special credit checks, while others have argued that the SIM card system should be abolished and that all SIM data should be anchored in the circuit boards of mobile telephones (Purton 1994, p. 24). Systems are also in place which enable cellular telephones to be locked by the use of a Personal Identification Number (PIN) when the telephone is not in use allowing incoming calls still to be received but if the telephone is stolen outgoing calls will not be able to be made (Cellular One 1994).

Some of the target hardening strategies which manufacturers, carriers and providers have adopted to control mobile telephone fraud include the use of software to detect calls being transmitted from a counterfeit telephone at the same time as another legitimate source (call collisions), to block the receipt of calls from cloned telephones altogether, velocity checks which are able to determine whether a telephone has moved too fast between serving areas to be legitimate, toll access restrictions to prevent unauthorised access to international dialling, unusual activity analysis to detect unusual usage patterns as an indication of fraud, dialled-number analysis which allows the carrier to block out high-risk countries or individual numbers, analysis of time of day, minutes of usage or credit activity for abnormal patterns of usage, radio frequency fingerprinting which measures the characteristics in a telephone's signal, and voice print matching which compares the subscriber's voice print with that recorded at the cell site (*see* Sulc 1994, p. 65; Walters & Wilkinson 1994, p. 7; Young 1995, p. 35).

Elsewhere, it has been reported that mobile telephone security numbers are being protected by viruses which will infect systems which gain unauthorised entry into a chip (Anonymous 1993). New digital telephones which adopt the Cellular Industry Standard IS-54 will also be much more difficult to clone (Walters & Wilkinson 1994, p. 6). Finally, various systems are being trialed to identify mobile telephone transmissions by the use of digital signatures (Brooks & Davis 1994, p. 68).

Human resource industry controls

Although accounting for only a relatively small proportion of illegal activities, conduct committed through internal security breaches or by the conduct of industry personnel may be prevented by ensuring that reliable and trustworthy staff are employed and that staff are adequately remunerated and have good working conditions, thus making them less desirous of engaging in illegal conduct. Internal controls such as separation of duties and rotation of duties should enable misconduct by employees to be more easily identified. Specific training and education in ethics for staff may also alert employees to the fact that security arrangements are in place within organisations.

Self-help and user education

Education has long been considered as one of the most effective ways of reducing the threat of criminality. Both children and adults need to be educated in the ethical use of high technology and the undesirability of manipulation of technological systems for entertainment or financial gain.

In addition, users are able to take many steps to detect illegality before it becomes a major problem or to avoid victimisation completely. Some fraud prevention strategies which are recommended for customers to adopt include checking bills for unusual calls, keeping network security numbers confidential, locking telephones with a PIN when not in use, not leaving telephones unattended in cars, using only authorised technicians and eliminating international dialling capabilities of telephones when not in use.

These few directions for future policy may assist in ensuring that the full potential of global telecommunications developments will be realised while at the same time providing both service providers and users with some expectation that their property rights will be respected.

References

Anonymous 1993, "Phone fraud crack-down not enough", *Mobile Asia-Pacific*, December, p. 15.

Australian Federal Police 1993, *Annual Report 1992-93*, AGPS, Canberra.

----------- 1994, *Annual Report 1993-94*, AGPS, Canberra

Brooks, T. & Davis, M. 1994, "Are your phone bills fraud free?", *Security Management*, vol. 38, no. 4, pp. 67-8.

Cellular One 1994, "Cellular fraud facts", paper presented at the International Crime Stoppers Conference, Hawaii, September.

Clarke, R.V. 1995, "Situational crime prevention", in *Building a Safer Society: Strategic Approaches to Crime Prevention*, eds M. Tonry & D.P. Farrington, University of Chicago Press, Chicago, pp. 91-150.

Clough, B. & Mungo, P. 1992, *Approaching Zero: Data Crime and the Computer Underworld*, Faber and Faber, London.

Commonwealth of Australia, Attorney General's Department and Department of Communication and the Arts 1994, *Report of the Computer Bulletin Board Systems Task Force: Regulation of Computer Bulletin Board Systems*, Attorney General's Department, Canberra.

Commonwealth of Australia, Bureau of Transport and Communications Economics 1995, *Communications Futures: Final Report*, AGPS, Canberra.

Coutorie, L. E. 1995, "The future of high-technology crime: A parallel Delphi study", *Journal of Criminal Justice*, vol. 23, no. 1, pp. 13-27.

Crowe, D. 1996, "Wrong numbers", *Financial Review*, 15 February, p. 16.

Delaney, D. P. 1993, "Investigating telecommunications fraud", in *Criminal and Civil Investigation Handbook*, ed. J.J. Grau, 2nd edn, McGraw-Hill Inc., New York.

Denning, D. E. 1995, "Crime and crypto on the information super-highway", *Journal of Criminal Justice Education*, vol. 6, no. 2, pp. 323-36.

Dunning, M. 1982, "Some aspects of theft of computer software", *Auckland University Law Review*, vol. 4, no. 3, pp. 273-94.

Olson, B. 1994, "Phone Hacking", *Your Computer*, December, pp. 12-13.

O'Neill, J. 1996, "The great mobile phone rip-off", *Independent Monthly*, April, pp. 20-5.

OECD (Organisation for Economic Co-Operation and Development) 1986, *Computer-Related Crime: Analysis of Legal Policy*, OECD, Paris.

Purton, P. 1994, "Fraudsters check card revolution", *The European*, 8-14 July, p. 24.

Schieck, M. 1995, "Combating fraud in cable and telecommunications", *IIC Communications Topics No. 13*, International Institute of Communications, London.

Sulc, L. B. 1994, "Communicating cellular security needs", *Security Management*, vol. 38, no. 4, pp. 63-5.

United Kingdom, Parliamentary Office of Science and Technology 1995, "Mobile Telephone Crime", *Science in Parliament*, vol. 2, no. 6, pp. 27-30.

Walters, D. & Wilkinson, W. 1994, "Wireless fraud, now and in the future: A view of the problems, some solutions", *Mobile Phone News*, 24 October, pp. 4-7.

Young, T. H. 1995, "Wireless Bandits", Police, May, pp. 32-5.

ACKNOWLEDGMENTS

This research was funded in part by a grant from the Telstra Fund for Social and Policy Research in Telecommunications. I am grateful to Greg Williams of Telstra Corporate Security and Dennis Challinger of Coles Myer Ltd for their helpful comments on an earlier draft of this paper.

NOTE

A fully-referenced extended version of this paper is available from the Australian Institute of Criminology and will be published subsequently.

Dr Russell G. Smith is a
Senior Research Officer with the
Australian Institute of Criminology

Submissions for consideration for the Trends and Issues series should be forwarded to:
Dr Adam Graycar, Director
Australian Institute of Criminology
GPO Box 2944
Canberra ACT 2601 Australia