TRENDS & ISSUES
in crime and criminal justice

Australian Government
Australian Institute of Criminology

No. 286 October 2004

Criminal Forfeiture and Restriction-of-Use Orders in Sentencing High Tech Offenders

Russell G. Smith

Courts in the United States, Europe and Australia have in recent years experimented with sanctions which require the computer of an offender convicted of high tech crimes to be forfeited, or which seek to prohibit the offender from undertaking certain, or all, computer-related activities like possessing or using computers or gaining access to the internet. Some courts have also imposed requirements that the offender's computer activities be monitored by a probation officer or that the offender's computer have filtering software installed to prevent access to certain types of content. This paper considers whether such orders are legally and practically justifiable as appropriate judicial punishments.

Toni Makkai
Director

AUSTRALIAN HIGH TECH CRIME CENTRE

ISSN 0817-8542

ISBN 0 642 53855 7

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 & issues in crime and criminal justice series, visit the AIC web site at:http://www.aic.gov.au

This paper looks at certain sanctions that have been applied in recent years to persons convicted of computer-related crimes. The kinds of crimes under consideration include gaining access to computers without authorisation (so-called 'hacking' or 'cracking'), dissemination of viruses, and possession or distribution of illegal content such as child pornography. The discussion examines whether the use of criminal forfeiture and restriction-of-use orders satisfy the various aims of sentencing, and considers whether the courts in a number of countries have acted in accordance with the law when seeking to impose these sanctions.

The methodology used follows that adopted by Smith, Grabosky and Urbas (2004). It involved the identification of 240 cases of high tech crime from Australasia, Europe and the United States in which sentences were imposed on offenders. Cases were identified from searches conducted of legal databases, media reports and secondary sources including books and government reports. In 33 cases, sentences were imposed that involved the use of criminal forfeiture and restriction-of-use orders, and it is these cases which form the basis of the following discussion. There have only been isolated cases reported in Australia:

- In one case, the offender's computer was subject to a forfeiture order to facilitate compliance with other conditions that he seek psychiatric treatment for an addiction to cybersex (*R v Burnham*, District Court of Queensland, Ipswich, 20 June 2002; see West 2003).
- In 2003, a 17-year-old was charged with the attempted murder of a man he met in an internet chat room, with whom he allegedly had sexual contact following their online meeting. Part of the bail conditions imposed on the teenager were orders that he not use the internet except for school work, that he obey a nightly curfew of 9pm, and that he report to police three times a week until his next court appearance. His computer, allegedly used to make contact with the man, was seized by police (see Milovanovic 2003).
- A further case involved a 69-year-old man in New South Wales who was charged with possession and publication of child pornography. He was originally sentenced to two years imprisonment for the publication offence and five years probation for the possession with

> conditions that he not use any computer at any time connected to the internet, and that he not be in the company of any person under the age of 18 without the specific written permission of a probation officer. On appeal the sentence was reduced to two years imprisonment with a non-parole period of 12 months (*R v Geoffrey Seaton Rooney*, Nowra District Court, 18 November 2003).

In the absence of other decisions, Australian courts will be guided by what has occurred in other countries that have experimented with such orders – especially the United States (where most such cases have been decided). Although sentencing laws differ across jurisdictions, the fundamental principles remain similar in determining whether these orders fulfill the aims of sentencing.

High tech crime and punishment

Grotius, the seventeenth century jurist and philosopher of law, defined punishment as 'the infliction of an ill suffered for an ill done.' Punishment entails something which is assumed to be unwelcome to the recipient or which, in the words of Hart (1968), invokes pain or other consequences which are considered to be unpleasant, such as loss of liberty through incarceration, disqualification from some activity, or loss of something of value such as money or time.

Over the past decade, high tech crimes have attracted the complete range of available sanctions, from the death sentence (see People's daily online [2000] for the case of a computer hacker who was sentenced to death for embezzling 1.66 million yuan [about US$200,000] from customers' accounts at the bank where he worked) to the most lenient of fines and unsupervised release orders.

Forfeiture orders seek to punish offenders by removing from them something of value, which in the case of high tech criminals is the ability to use computers and the internet. This is clearly of considerable value, both financially (in terms of undertaking gainful employment) as well as psychologically (in terms of demonstrating one's expertise and enhancing one's self-esteem). Hence, some courts have imposed orders requiring the forfeiture of computer hardware or conditional orders that seek to limit computer-based and online activities as a form of punishment.

The objectives of sentencing can be classified under two broad categories: retributivism and consequentialism. Each has particular features that sentencing needs to accommodate if it is to achieve its purpose. These include proportionality, denunciation, incapacitation, deterrence, rehabilitation and restitution. Although sentencing judges take all these considerations into account when choosing appropriate sanctions, the process tends to be intuitive rather than empirical. In the case of *R v Williscroft* [1975] VR 292, Justices Adam and Crockett in the Court of Criminal Appeal of the Supreme Court of Victoria remarked:

> ultimately, every sentence imposed represents the sentencing judge's instinctive synthesis of all the various aspects in the punitive process.

Applying these various aspects to the circumstances in which forfeiture or restriction-of-use orders have been made has raised some difficult legal issues. In the United States, Canada and Australia there have been 33 publicly reported cases decided over the past 11 years in which 58 forfeiture or restriction-of-use orders have been made involving computers (in some cases multiple orders were imposed). Almost all involved conditions placed on periods of supervised release, although in one case conditions were imposed on computer use while the offender was in prison (these conditions were set aside on appeal; see *United States* v *Ginyard* 342 US App DC 83; 215 F 3d 83; 16 June 2000). In another case conditions were imposed on computer use while the accused was on bail (which were not challenged by the offender).

As is apparent from Table 1, in approximately one-third of cases these conditional orders were not challenged on appeal; in another third of cases the conditions were challenged and set aside on appeal; and in the final third of cases the orders were affirmed. The jurisprudence remains in a period of development although it is now clear that certain orders should not be used.

Legislative authority and validity of orders

Although the legislative authority for the use of forfeiture and restriction-of-use orders varies across jurisdictions, it is generally possible for sentencing judges to order forfeiture of the implements used in the commission of an offence, or to impose conditions on periods of probation or parole that require the offender to refrain from doing certain activities or to comply with any reasonable directions of a probation officer. In most jurisdictions, the law requires special conditions to be used only where those conditions:

- are certain in their requirements;
- are necessary for the prevention of crime or the protection of members of the public;
- are practically able to be carried out;
- do not serve ulterior purposes; and
- are not contrary to public policy.

See, for example, *Neil v Steel* (1973) 5 SASR 67; *R v Conn*, Supreme Court of Victoria, 5 October 1981; *R v Harvey* (1989) 40 A Crim R 102; *Temby v Schulze* (1991) A Crim R 284. There are also in some jurisdictions statutory time restrictions on the maximum duration of such orders.

In the United States, it has been argued in some cases that the imposition of restrictions on the use of computers or monitoring of online activities infringes the first amendment of the constitution concerning freedom of speech. It has been held, however, that as long as restrictions are reasonably related to the offence and defendant's history, are primarily designed to protect the public and promote rehabilitation by preventing recidivism, are expressly related to those ends and, particularly in light of the defendant's past conduct, involve no greater deprivation of

Table 1: Restriction of possession and use cases, 1992–2003

Order	Unchallenged	Held valid	Held invalid	Total
Forfeiture	3			3
Ban/restriction on possessing computers	2	5	5	12
Ban/restriction on using computers	4	5	1 (in prison) 4 (on parole)	14
Monitoring of computer use	4	3		7
Ban/restriction on using internet	1 (on bail) 4 (on parole)	8	9	22
Total	18 (31%)	21 (36%)	19 (33%)	58 (100%)

Note: Thirty-three cases (29 American, three Australian and one Canadian) were identified during the current research. Some cases involved more than one type of order in addition to other sentences.

Source: Australian Institute of Criminology high tech crime sentencing file

liberty than is reasonably necessary to achieving those ends, they should survive a first amendment challenge (Painter 2001; *United States v Ristine*, Eighth Circuit, 2 July 2003; *United States v Mitnick*, Ninth Circuit, 14 May 1998).

Generally, it seems that restrictions on the use of computers or the internet will be appropriate as long as they are reasonably related to the statutory purposes underlying the order, involve no greater deprivation of liberty than is reasonably necessary and are not overly broad (see Painter 2001; Hyne 2002). For example, in *United States v Robb Walker Freeman* (Third Circuit, 6 January 2003) the District Court for the Eastern District of Pennsylvania had imposed a special condition on supervised release that the offender could not possess a computer at his home or use an online computer service without the permission of his probation officer for the 70-month period of his supervised release. This case involved possession of computerised images of child pornography. The Court of Appeals held it was too broad a restriction as the offender had not tried to contact minors online but had merely obtained illegal images of children. Accordingly, a complete prohibition was overly restrictive.

A number of courts have held that a blanket ban on the use of computers and the internet is now inappropriate in view of the heavy reliance that we all have on computers for daily life. In *United States v Holm* (Seventh Circuit, 4 September 2003), Judge Diane Wood, writing for the Court of Appeal, observed:

> for anyone, a total ban on all internet use would render life exceptionally difficult, given that today, the government strongly encourages taxpayers to file their returns electronically, more and more commerce is conducted online, and vast amounts of government information are communicated via web sites.

In terms of rehabilitation, it is often essential for offenders to have access to computers to secure employment on their release from prison. On occasions, however, prohibition of the use of computers or the internet could impede rehabilitation. In *United States v Robert White* (Tenth Circuit, 27 March 2001), for example, the offender pleaded guilty to receiving child pornography ordered over the internet. The District Court ordered that he should 'not possess a computer with internet access throughout his period of supervised release.' The offender, who was writing a book at the time, argued this would impede his ability to research the book and thus go against his rehabilitation. The Court of Appeals stated that although the offender could still technically possess a computer for word processing and record-keeping, most computers are now equipped with an internal modem, rendering any use of the computer a possible access to the internet. The court found the condition to be overly broad and invalid, instead suggesting that some form of monitoring of his computer use would have been adequate to prevent him from obtaining child pornography.

Similarly, in the case of *United States v Holm* (Seventh Circuit, 4 September 2003), the Court of Appeals overturned a restriction that the offender should not possess or use a computer that is equipped with a modem, that allows access to any part of the internet, email or other online service or possess software expressly used for connecting to an online service, including email. The court agreed that prohibiting the offender from use of computers with network connectivity would seriously impede his ability to find gainful employment upon his release from prison as he had previously worked as an information systems technologist.

Forfeiture of computer equipment

The earliest case in which a forfeiture order was used occurred in 1992 when the State of New York County Court ordered the forfeiture of the personal computers of four students from Cornell University after it was proved they had created and spread the MBDF computer virus which interfered with the operation of the university's computer system. One of these students had also created a false user account at the university. In addition to the forfeiture order the students were required to pay restitution of US$6,000 to the university and US$1,365 to two victims, and to perform 520 hours community service (*New York v Blumenthal and Others* Ind. No. 92-072-A, 4 September 1992).

Forfeiture of computer equipment used in the commission of offences provides a clear example of proportionality by linking the punishment for an offence with the means by which the offence was committed. Proportionality, or 'just deserts,' simply means that the severity of punishment should be commensurate with the seriousness of the wrong. Although forfeiture of personal computers

may be appropriate where they are owned by offenders and have been used to commit offences, difficulties may arise where hardware or software belongs to some other person or corporation, or where the forfeited computer contains data that belong to others. In such cases, the effect of the order may be to punish persons who were not involved in the commission of the offence. In the Queensland case of *R v Hannah* (District Court of Queensland, Ipswich, 9 April 2001), the offender was convicted of possessing a child abuse computer game and fined A$1,000. During a search of his premises, police found a number of disks containing child pornographic images. The court ordered the disks to be forfeited but not his computer because of the detriment such an order would have had on the offender's children (West 2003: 99).

In some cases in which computers have been seized in the execution of search warrants on lawyers' premises, claims of legal professional privilege have been successfully made on the grounds that the computer records contain confidential client communications (Smith, Grabosky & Urbas 2004). Forfeiture could also be viewed as a form of incapacitation in that it is seeking to prevent the offender from committing crime by isolating the individual from the online society in which the offence was committed. The ready availability of computers in public libraries and internet cafés, however, means that forfeiture of one's personal computer is unlikely to be entirely effective in preventing online access.

Restricting possession and use of computers

As an alternative to confiscating and forfeiting an offender's computer hardware – that is, physically removing them from the offender's premises – courts have made orders banning offenders from possessing computers or prohibiting them from having or using modems or gaining access to the internet. These orders have extended from complete prohibitions to specific orders that only prohibit certain types of activity, such as downloading child pornography.

The first case in which such an order was made involved an offender who had posted child pornographic images to bulletin boards from his home computer. The Ontario Provincial Court sentenced him to two years probation, with 150 hours community service, and ordered him to seek psychological treatment, not to communicate with anyone under 16, and not to download erotic material from the internet (*R v Pecciarich* (1995) 22 OR (3d) 748, [1995] OJ No. 2238, Ontario Court (Provincial Division) 20 July 1995). The obvious problem with such an order concerns its enforceability and the problems that probation officers would encounter in determining what material the offender had downloaded.

Problems have also arisen in defining exactly what 'erotic material' or 'pornography' means, although most cases have involved child pornography which is capable of more precise definition because of the age or appearance of the individuals being represented. Other courts have imposed bans on the use of computers with exceptions for work-related use, school work or where the offender's probation officer has approved of the use.

In the case involving Kevin Mitnick, in addition to being sentenced to almost five years imprisonment, being ordered to pay US$4,125 in restitution and being required to assign to his victims any proceeds he may receive from selling the story of his conduct, Mitnick was subject to stringent conditions during his three-year period of parole. These included a complete prohibition (without prior express written approval of the probation officer) on the possession or use (personally or through third parties), for any purpose, of the following:

- mobile phones;
- computers, any computer software programs, computer peripherals or support equipment;
- personal information assistants, modems or anything capable of accessing computer networks; and
- any other electronic equipment presently available or new technology that becomes available that can be converted to, or has as its function, the ability to act as a computer system.

Mitnick was also banned from accessing computer systems, computer networks or telecommunications networks. In addition, he was prohibited from acting as a consultant or advisor to individuals or groups engaged in any computer-related activity. Mitnick appealed against this order on the basis that it involved a violation of his first amendment rights and because it was said to be vague and overly restrictive. The appeal court, however, decided that the conditions were reasonable in view of Mitnick's recidivist tendencies and in order to protect the public (*United States v Kevin Mitnick*, 1998 WL255343, 9th Circuit 20 May 1998).

Monitoring computer use

The most recent cases have decided that rather than prohibit use of computers and the internet, it is preferable for some form of monitoring to take place, either through unannounced visits by probation officers, or through the installation of filtering software which would prevent the offender from visiting certain web sites – principally those relating to child pornography or paedophile activity. Of course, filtering software is not always effective in restricting access to certain content, and technologically skilled high tech criminals could well program their computers to disable the filtering software.

As suggested by Judge Wood in *United States v Holm*, monitoring computer use has previously been applied as a condition in cases involving high tech crime. In *United States v Scott Dennis* (District Court for the Eastern District of New York, 19 January 2001), for example, the offender was convicted of perpetrating a series of 'denial of service' attacks, in which the victim's computer systems were maliciously flooded with data, and was sentenced to six months incarceration to be served by three months in jail and three months in home confinement, followed by one year of supervised release. He was also ordered to perform 240 hours of community service, and was required to

allow the probation authorities to monitor his computing activity during the period of supervision.

In the first prosecution to go to trial in Los Angeles under the federal statute covering computer abuse and spamming – the *Computer Fraud and Abuse Act 1986* (18 USC §1029) – Bret McDanel, otherwise known as 'Secret Squirrel', was sentenced to 16 months in a federal prison, and ordered to submit to unannounced searches of his computer, to advise all future employers about his conviction and receive psychological counselling, for having maliciously bombarded his company's server with thousands of spam emails (*United States v McDanel*, District Court at Los Angeles, 25 March 2003).

In the case of *United States v Chance Rearden* (349 F.3d 608, United States Court of Appeals, 6 November 2003), in which the offender was convicted of using a computer to communicate information about raping children and sending graphic child pornography by email over the internet, the District Court ordered that:

> all computers, computer-related devices, and the peripheral equipment used by the defendant shall [be] subject to search and seizure and the installation of search and/or monitoring software and/or hardware including unannounced seizure for the purpose of search.

This order was upheld on appeal. The defendant argued the conditions were vague, as even a television, palm pilot or watch could be considered a computer or computer-related device. However, the Court of Appeals saw no reasonable possibility that a computer, a computer-related device and peripheral equipment would be interpreted beyond the normal accoutrements of one's personal computer such as disks and disk drives, and devices for extra storage.

The possibility of an unannounced inspection of one's computer may act as a specific deterrent to some forms of high tech crime. Problems could, however, arise in inspecting computers shared by offenders and others as the privacy of non-offenders could be infringed if an entire hard drive were inspected which contained data belonging to third parties. These questions will, no doubt, need to be addressed by courts over time as orders of this kind continue to be made.

Generally, conditional orders which require the surveillance of offenders must not be unreasonable in their potential to interfere with the offender's life. In the Northern Territory case of *Dunn v Woodcock* [2003] NTSC 24 (Supreme Court of the Northern Territory, 20 March 2003), conditions were imposed on an offender convicted of unlawfully supplying cannabis which required her to consent to any number of searches at any time during the day or night over a period of 12 months, irrespective of whether or not the police had reasonable grounds for believing there may be dangerous drugs concealed upon her premises, and even if a search warrant had not been obtained. The court considered that the condition placed an unreasonable burden on the offender as it placed her in the power of the police who could exercise very substantial control over her life by the mere threat of exercising the power to search unreasonably or unfairly. The court struck out the condition on the grounds that it was unduly oppressive.

Effectiveness of the orders

How effective, then, are forfeiture and restriction-of-use orders in reducing crime? Because these orders have only recently been employed in cases involving computer crimes, we do not have a sufficiently large sample to undertake quantitative research. There are, however, some logical barriers to the likely utility of these orders.

Use of other computers

The use of forfeiture of an offender's personal computer and modem is unlikely to stop the offender from using any one of a number of computers that are readily available to members of the public in libraries and other public places such as internet cafés. Forfeiture is, therefore, unlikely to have an incapacitating effect.

Effects on non-offenders

Forfeiture of a personal computer may affect individuals other than the offender, such as where other family members make use of the computer for school work or recreational activities. Forfeiture could, therefore, infringe the principle of proportionality in punishment.

Difficulties of enforcement

Restriction-of-use orders will only be effective to the extent that the order is capable of being enforced. This may require that probation officers be trained in computer forensics to conduct thorough inspections of the offender's computer, which is unlikely to be feasible for most probation services. Technologically adept offenders would be quite capable of concealing their activities from most probation officers who have not been fully trained in computer forensics.

Limits of monitoring software

If monitoring or filtering software is installed on the offender's computer this could be disabled by the offender, or be either inadequate to detect the full range of prohibited content or, alternatively, could be over-inclusive and prevent the offender from gaining access to legitimate content. This could impede a person's potential rehabilitation or employment during parole.

Effect on rehabilitation

Forfeiture and restriction-of-use orders could create problems in terms of rehabilitation of offenders, particularly for individuals who work in the information and communications technologies industries. A ban on computer or internet use may make them unemployable. In addition, the use of filtering software may be over-inclusive and prevent the offender from gaining access to legitimate content.

Limits on restitution/community service

Related to the problem of achieving rehabilitation, forfeiture and restriction-of-use orders may mean the offender is unable to earn sufficient money to pay compensation orders or other financial penalties. Similarly, offenders subject to

forfeiture or restriction-of-use orders could not engage in some types of constructive community service that might require the use of computers. In this sense, their skills are being wasted during the period of the order.

Future directions

From these few illustrations of sentences imposed on high tech criminals in recent years, we can see that courts are beginning to adapt sanctions to suit the novel circumstances of the cases. The difficulty which courts face in sentencing is to impose an appropriate punishment that will have some deterrent effect while at the same time devising orders that will be enforceable and not overly restrictive on the offender and third parties.

The decisions that have been imposed remain in their infancy and we are only beginning to see decisions of appellate courts being handed down which explore the boundaries and appropriateness of some of the conditional orders being imposed. Restricting access to computers or the internet can have potentially profound consequences, making punishments of this kind arguably more severe than traditional conditional orders. The simple prohibition on the use of a computer could deprive a person of the ability to find employment which could reduce, not enhance, the possibility of rehabilitation.

Rather than seeking to impose restrictions on the use of computers as a means of punishment, courts could perhaps adopt the alternative approach of requiring offenders to use their computer skills or knowledge for *constructive* purposes. This could occur in a variety of ways:

- assisting police to investigate high tech crime cases, such as in the case of *United States v David Smith*, where the author of the Melissa virus acted as a police informer and his assistance led to the convictions of Jan DeWit (author of the Anna Kournikova virus, in the Netherlands on 27 September 2001) and Simon Vallor (author of the Gokar virus, in London on 21 January 2003);
- delivering lectures to the public/schools about the dangers of computer crime, and discouraging others from engaging in similar conduct, such as in *United States v Richard W. Gerhardt* (District Court of the Western District of Missouri, 13 March 2003), which was a case involving theft of passwords; and
- performing supervised community service in the high tech field.

Although conventional punishments of imprisonment and fines are likely to remain popular with courts in cases involving serious computer crime, it is likely that some judges will continue experimenting with specifically targeted forfeiture and restriction-of-use orders. As we have seen, however, these can sometimes entail legal challenges or be counterproductive in reducing crime. Carefully framed conditional orders can, however, enhance the effectiveness of judicial punishment in certain cases.

What may be needed is for evaluative research to be undertaken to assess the impact of such orders both on the individual offender as well as others who may be affected as a consequence of sharing the offender's computer at home or at work. Only when the results of carefully controlled research are gathered will we be in a position to assess the impact of such sentences in punishing the computer criminal.

Acknowledgment

I am grateful to Neale Williams, intern at the AIC, for assisting with the research for this paper, and for the suggestions of two anonymous reviewers and an officer of the Australian High Tech Crime Centre.

References

Hart HLA 1968. *Punishment and responsibility: essays in the philosophy of law.* Oxford: Oxford University Press

Hyne D 2002. Examining the legal challenges to the restriction of computer access as a term of probation or supervised release. *New England journal on criminal and civil confinement* vol 28: 215

Milovanovic S 2003. Student banned from internet after stab charge. *The age* (Melbourne) 29 October: 3

Painter CME 2001. Supervised release and probation restrictions in hacker cases. http://www.usdoj.gov/criminal/cybercrime/usamarch2001_7.htm

People's daily online 2000. Chinese hacker sentenced to death for embezzlement. *People's daily online* 13 June. http://english1.peopledaily.com.cn/english/200006/13/eng20000613_42866.html

Smith RG, Grabosky PN & Urbas GF 2004, *Cyber criminals on trial*, Cambridge: Cambridge University Press

West A 2003. Sentencing for the possession of child abuse computer games and images. *The Queensland lawyer* vol 23: 98–101

Dr Russell G. Smith is Principal Criminologist at the Australian Institute of Criminology

General editor, Trends & issues in crime and criminal justice series: Dr Toni Makkai, Director, Australian Institute of Criminology, GPO Box 2944 Canberra ACT 2601

Note: Trends & issues in crime and criminal justice are refereed papers

The AIC is a statutory body with a Board of Management comprised of federal, state and territory government representatives, administered under the *Criminology Research Act 1971*