International Journal of Cyber Criminology
Vol 1 Issue 2 July 2007

Crime Control in the Digital Age: An exploration of Human Rights Implications

Russell G. Smith[1]
Australian Institute of Criminology, Australia[2]

Abstract

Advances in information and communications technologies (ICT) have created not only a range of new crime problems, but also facilitated prevention, detection, investigation, prosecution and punishment of crime. Although technology has assisted criminal justice agencies and offered many protections for suspects and offenders, risks of infringement of human rights have arisen from the way in which the law has responded to computer crime. This paper identifies the principal areas of human rights concern, which the digital age has created and assesses whether the achievements and benefits derived outweigh the potential and actual infringements of liberty that exist. It is concluded that policy makers have sometimes been attracted by the novelty and efficiency of technology without having due regard to the sometimes covert infringements of human rights which could and do occur.

Keywords: Communication; Technology; Human Rights; Liberty; Internet; Computer Crime;

Introduction

This paper considers the human rights implications of crime control in the digital age—that is, crime that involves information systems as instruments or as targets of illegality. 'Digital', simply refers to the fact that computerized systems operate by reducing information to streams of '1s' and '0s'. Almost every type of information is thus able to be transmitted across telecommunications networks connected either by wires or by means of radio waves. Advances in information and communications technologies (ICT) have created not only a range of new crime problems, but also facilitated the prevention, detection, investigation, prosecution, adjudication and punishment of crime. Examples include the use of encryption to ensure that data are held securely, neural networks to detect financial crime, biometric systems to identify suspects, hard drive imaging to secure data from alteration or destruction, sharing of data held in official databases to identify suspects and risks, electronic courtrooms to present evidence clearly, and electronic monitoring of offenders to enhance surveillance during periods of home detention.

Although technology has assisted criminal justice agencies and offered many protections for suspects and offenders, risks of infringement of human rights have arisen

[1] Principal Criminologist; Manager, Global, Economic and Electronic Crime Program, Australian Institute of Criminology, GPO Box 2944 Canberra ACT 2601, Australia. Email: Russell.Smith@aic.gov.au

[2] "The views expressed are those of the author alone and not the Australian Government".

from the ways in which legal reforms designed to deal with computer crime risks have been framed. As Arup and Tucker (1998: 245) observed:

> *Information technology has provided authoritarian states with capacity to monitor contain and discipline their subjects but information technology and the human rights associated with it have also done much to undermine their hold.*

This paper identifies some areas of human rights concern which legal reforms designed to address ICT-related crime have created and assesses whether the achievements and benefits derived outweigh the potential and actual infringements of liberty that exist. It is concluded that policy makers have sometimes been attracted by the novelty and efficiency of technology without having due regard to the sometimes covert infringements of human rights which could and do occur.

What are Human Rights?

At present there are no specific normative instruments that comprehensively set out human rights applicable in the digital age. Instead, developments in ICT have implications for the various existing international and local regimes that seek to protect human rights (see Weeramantry 1990). These include:

- The Universal Declaration of Human Rights (1948) (UDHR)
- The International Covenant on Civil and Political Rights (1966) (ICCPR), to which Australia is a signatory;
- The International Covenant on Economic, Social and Cultural Rights (1966) (ICESCR), to which Australia is a signatory; and
- The Optional Protocol to the International Covenant on Civil and Political Rights (1966).

The Universal Declaration sets out general principles concerning physical integrity (life, liberty, arrest, detention, torture, freedom of movement, asylum), social welfare (social security, the right to work, rest, leisure, education), health, adequate standard of living, the family, legal integrity (nationality, participation in government, recognition before the law, fair trial), and mental and moral integrity (dignity, freedom of thought, conscience and religion, freedom of opinion and expression, freedom of peaceful assembly and association). These rights are described more fully in the Covenants and Protocols.

In addition, some countries and regions have developed their own Human Rights Conventions, such as the European Convention for the Protection of Human Rights and Fundamental Freedoms, the United States Constitution and the Canadian Charter of Rights and Freedoms. There are also the British constitutional documents Magna Carta (1215), and the Declaration of Rights (1689) which, along with the common law, has created a climate of respect for individual liberty in English common law countries.

In Australia, there are numerous pieces of legislation that give effect to these human rights principles, although there is no national level Human Rights Act. At the federal level there are some twenty Acts that are relevant to the protection of human rights including the Human Rights and Equal Opportunity Commission Act 1986, which protects certain specific rights such as freedom from various forms of discrimination. There are also over 80 state and territory Acts that protect human rights in various ways dealing with principles of anti-discrimination, freedom of information, equal opportunity, adherence to the rules of natural justice, to mention a few (for a full list see http://www.hreoc.gov.au/hr_explained/hr_in_australia.html). In the Australian Capital Territory, various rights are also now protected under the Human Rights Act 2004 (ACT)

and the Human Rights Commission Act 2005 (ACT) which is based on the International Covenant on Civil and Political Rights. In Victoria, since 1, January, 2007, human rights are also protected under the Charter of Human Rights and Responsibilities Act 2006 (Victoria).

The purpose of the following discussion is not to assess whether legislation in Australia relevant to cyber crime complies with each Convention or piece of legislation, but rather to indicate some areas in which human rights concerns have been identified, and also to point to potential areas of infringement if certain technological developments occur. At present Australia can be guided by what has occurred in various overseas countries which have enacted local human rights legislation, or whose legislation has been challenged in the Human Rights Commissions or higher courts.

What Rights are at Risk from Crime Control in the Digital Age?

In the digital age, misuse of ICT can take place in relation both to government and private sector activities. Most human rights principles are directed at identifying and preventing abuses by government agencies, although recently we have seen an extension of privacy protections from the public sector to the private sector. In addition, human rights abuses can arise from the actions of individuals, which give rise to the need for governments to enact laws to protect citizens both from the acts of government agencies as well as other individuals and corporations, a point recognized by Arup and Tucker (1998), some time ago. The present discussion focuses on abuses which can occur in criminal justice contexts involving cyber crime, which increasingly are inclusive of private corporations as providers of investigative, judicial and correctional services.

Weeramantry (1983: 17-21) has identified various technological advances which could detract from basic human rights unless regulated by legislation. Over the last twenty years many new issues have arisen and Table 1 sets out those areas of concern that relate to the regulation of ICT in the context of criminal justice in the 21st century.

Table 1 - Potential Human Rights Infringement in Connection with ICT and its Regulation

Human Rights*	Sources of Possible Denigration by ICT
Human freedom and dignity (UDHR art 1, ICCPR art 10)	Electronic surveillance (listening devices, CCTV) DNA analysis Data matching by government agencies Identity smart cards Electronic tagging of offenders
Freedom from discrimination (UDHR art 2, ICCPR art 26)	Cyber racism Computer addiction
Freedom of thought and expression (UDHR art 18, 19, ICCPR art 18, 19)	Maintenance of databases Surveillance devices Spam / Denial of service attacks Online content restrictions
Right to bodily security and freedom from inhuman punishments (UDHR art 3, 5, ICCPR art 7)	Electronic tagging of offenders Embedded computer chips in humans Biometric identification
Right to a fair trial, presumption of	Disclosure of encryption keys / passwords

innocence, freedom from self-incrimination (UDHR art 11, ICCPR art 9, 14)	Use of electronic evidence in court Co-mingling of electronic evidence Juror access to online information
Right to own property and protect intellectual property (UDHR art 17, 27.1)	Digital piracy Computer hacking Electronic espionage
Right to privacy (UDHR art 12, ICCPR art 17)	Electronic surveillance Maintenance of databases Data matching by government agencies Identity smart cards e-commerce marketing and spam
Right to life (UDHR art 3, ICCPR art 6)	Cyber terrorism Capital punishment for cyber crime
Right to participate in government and vote (UDHR art 21, ICCPR art 25)	Online indoctrination Electronic surveillance Digital monopolies Invasions of privacy Surveillance of electronic voting activities

Note: Adapted from Weeramantry (1983: 17-21).
⋆ UDHR - articles of the Universal Declaration of Human Rights (1948);
ICCPR - articles of the International Covenant on Civil and Political Rights (1966).

The technologies are relevant to infringements of human rights include: the Internet, DNA analysis techniques, biometric identification technologies, CCTV and mobile phone cameras, listening devices, networked databases and neural networks for data analysis, voice recognition systems and others. Many of these technologies were developed by the military and security industry in the 1940s during the Cold War for policing and national security purposes. Since the 1990s, their miniaturization and power has increased immensely. It needs to be emphasized that potential infringements of human rights most often arise following the introduction of legislative measures designed to regulate these new technologies, rather than from the creation or usage of the technologies themselves.

With the advent of personal computers and wireless technologies in more recent times, the capacity to carry out complete surveillance of people is astounding, although the idea of the 'surveillance society' has its roots in much older times. In the late 18th century, Bentham designed his 'Panopticon' or total institution in which those in charge could monitor the activities of inmates, be they prisoners or patients in hospitals, easily through the use of specially designed buildings (Semple 1993). Foucault (1977) identified the societal implications of the power imbalance that would result in discipline and punishment. Unfortunately, technologies of surveillance have since developed, often with less than adequate controls over potential abuse.

Examples of Potential Human Rights Infringements from Crime Control in the Digital Age

Over the last thirty years during which cyber crime and its control have developed, we have witnessed many examples of the misuse of ICT, and legislative

responses to it, that could be said to have infringed human rights. The following are some illustrations that have been detected or which individuals have raised as potential infringements. Some relate to abuses of normative instruments in other countries, especially the United States Constitution, and so are not of direct relevance to Australia at present. Others relate to more universal human rights and so have particular importance in Australia. The following is not an exhaustive list, but serves to illustrate the kinds of issues that exist in the 21st century. It can be anticipated that the years ahead will see an escalation in these and other potential forms of human rights abuses.

Privacy

One particular group of rights that has relevance to ICT concerns the protection of privacy. In Australia, the legislative protection of privacy came relatively late in 1988 with the enactment of the Privacy Act 1988 (Commonwealth) and the more recent Privacy Amendment (Private Sector) Act 2000 (Commonwealth). There are also privacy laws in some states and territories, such as the Privacy and Personal Information Protection Act 1998 (New South Wales) and the Information Privacy Act 2000 (Victoria). However, Australian privacy laws are not particularly strong legislative instruments as remedies for breach of privacy are generally by way of declaration rather than criminal punishment, and private sector compliance is largely through voluntary codes of practice.

The protection of privacy in Australia arguably lags behind privacy protection in Europe, where various Privacy Directives have implemented protections under the European Convention for the Protection of Human Rights and Fundamental Freedoms. Recent measures include the Privacy Directive (95/46/EC) and the Privacy and Electronic Communications Directive (2002/58/EC) (see Smith, Grabosky & Urbas 2004).

The ability to monitor computer usage creates a number of potential human rights concerns including infringements of human freedom, freedom of thought and expression, and the right to privacy. Although the monitoring of emails and Internet usage by employers is usually undertaken with the knowledge of employees, informed and free consent is sometimes lacking.

Less certain are situations in which ISPs and telecommunications carriers monitor computer usage or provide logs to government agencies. Article 20 (real-time collection of traffic data) and Article 21 (interception of content data) of the Council of Europe's Convention on Cyber crime, for example, have been criticized as involving breaches of human rights in requiring organizations to collect traffic data and the content of communications and make this available to law enforcement agencies (Taylor 2001).

Recent moves towards the creation of electronic identity cards, e-Passports and data-matching also raise potential infringements of privacy which need to be addressed prior to the widespread implementation of such initiatives. Hong Kong, for example, has developed multi-use ID smartcards which contain basic biometric information such as thumb prints and a photograph, and are capable of multiple functions including use as drivers' licenses and as library cards (Benitez 2002). A pilot program for a biometric ID card has also been implemented in Britain, in relation to asylum seekers (McAuliffe 2002).

Some of the main privacy concerns which affect biometrically enabled identity cards include fears that information will be gathered without permission or knowledge, or without explicitly defining the purpose for which it is required; that information may be used for a variety of purposes other than those for which it was originally acquired

('function creep'); shared without explicit permission; or used to track people across multiple databases to amalgamate information for the purpose of surveillance or social control.

In addition to complying with privacy principles and privacy legislation, additional measures may be needed to enhance privacy protections in the digital age. These include mandating the use of specified levels of encryption for the capture, storage and transmission of data, limiting database matching except under close scrutiny by independent observers, preventing the reconstruction or retention of original biometric samples from encrypted biometric information, and preventing comparisons with reproductions of biometric information not obtained directly from individuals. Some of these aspects may require amendments to the Privacy Act 1988 (Commonwealth).

Search, Seizure and Criminal Trials

Computer crime legislation is expanding greatly the range of investigatory powers available to law enforcement agencies to deal with such problems as concealing electronic evidence through the use of encryption. Those countries unconstrained by a Bill of Rights have devised a simple solution to the challenge of encryption. They simply require individuals to disclose encryption keys or face criminal charges. In the United Kingdom, this can entail imprisonment for up to two years (Regulation of Investigatory Powers Act 2000 (England) ss. 49-55). In Europe, Article 6 of the Rome Convention could be a barrier to such compulsory disclosure, although the European Commission on Human Rights has restricted the scope of the article to oral statements. Nevertheless, European procedures for compulsory decryption would have to be formulated precisely in order to withstand judicial scrutiny (Smith, Grabosky & Urbas 2004: 67).

The Australian Cybercrime Act 2001 (Commonwealth), provides a maximum penalty of six months' imprisonment for failure to comply with a Magistrate's order to provide such information to investigating officials (see s. 3LA Criminal Code Act 1995 (Commonwealth) and s. 201A of the Customs Act 1901 (Commonwealth)). Arguably this could infringe article 14(3) (g) of the ICCPR which provides that a person shall not be compelled to testify against himself or to confess guilt.

The Council of Europe's Convention on Cyber crime (2001) incorporates various provisions designed to safeguard human rights norms and privileges in connection with cyber crime investigations, such as requirements for judicial or other independent supervision, proportionality, and respect for and consideration of the rights of third parties. Given the strength of the provisions allowing search, seizure and surveillance, however, these have been criticized by some privacy advocates as being inadequate (Taylor 2001).

Another particular area of concern relates to the use of 'keystroke logging' software which can be installed remotely on computers to capture information such as passwords and decryption keys typed on keyboards. Some have argued that such activities infringe the United States Constitution's Fourth Amendment right against unreasonable search and seizure. In one case, FBI agents in the United States tricked a pair of suspected hackers out of passwords and account numbers and then downloaded evidence from their computers in Russia.

The United States District Court rejected several motions filed on behalf of the defendants who sought to suppress the evidence obtained from their computers. They argued that the FBI agents had violated their Fourth Amendment right against unreasonable search and seizure by secretly obtaining the passwords and account numbers

using a '*sniffer*' program that recorded their keystrokes when the FBI agents remotely accessed the computers in Chelyabinsk, Russia.

The court found, that the defendants had no expectation of privacy when they sat down at computers at an FBI office set up to lure the suspects to the United States with offers of work in the computer security field. When they sat down at the networked computer they knew that the systems administrator could and likely would monitor their activities.

The court also found that the Fourth Amendment applied neither to the computers because they are the property of a non-resident and located outside the United States nor the data, at least until it was transmitted to the United States. The judge noted that investigators then obtained a search warrant before viewing the nearly 250 gigabytes of data. He rejected the argument that the warrant should have been obtained before the data were downloaded, noting that the agents had good reason to fear that if they did not copy the data, the defendants' co-conspirators would destroy the evidence or make it unavailable (United States v Gorshkov and Ivanov 2001 WL 1024026 W.D.Wash.).

Fairness in relation to the gathering and use of electronic evidence also can be placed in jeopardy because of the extent of electronic information that has been gathered. Often it will be necessary for police to image an entire computer's hard drive when executing a search warrant, despite the fact that much of the data copied will be irrelevant to the investigation. If the irrelevant material contains evidence of unsuspected criminal activity by other persons, their rights may be adversely affected.

In relation to criminal trials, a number of human rights implications arise. The rights to a fair trial, the presumption of innocence, and the freedom from self-incrimination are all established rights (UDHR article 11, ICCPR articles 9, 14) which could be infringed where ICT is used to gather and to present evidence. Risks could arise where electronic evidence is presented in court proceedings which may be unduly prejudicial to the accused or where jurors undertake private online research into the background of an accused contrary to directions from the judge. In both New South Wales and Queensland it is an offence for a juror to undertake investigations on the Internet or otherwise (Jury Act 1977 (New South Wales) s. 68C; Jury Act 1995 (Queensland) s. 69A). The extent of online information is such that prejudicial material could easily be discovered by jurors during a trial, with few opportunities for the judge or defense counsel to learn of this potential problem (see Spigelman 2005).

An example of this occurred recently in New South Wales. The accused had been convicted of murder of his first wife, but the Court of Criminal Appeal ordered a re-trial. He had also been tried and acquitted of the murder of his second wife. Both wives were from the Philippines and a Website called The Solidarity Philippines Australia Network contained material which was prejudicial to the accused. During the re-trial, a juror conducted Internet searches and inspected the Website and discovered that he had been tried and convicted of murdering his first wife and charged and acquitted of murdering his second wife. The Court of Criminal Appeal set aside the conviction in the re-trial because of the conduct of the juror in obtaining access to the information contained on the Internet. It ordered a further re-trial as a result of which the accused was convicted of murdering his first wife (R. v K (2002) 59 NSWLR 431; 144 A Crim R 468; [2003] NSWCCA 406).

Discrimination

Potential infringement of anti-discrimination laws in the digital age can arise in situations in which persons accused of illegal online activity claim to be acting due to some form of impairment. A Canadian civil case, for example, involved the dismissal of a University academic for using his employer's equipment for downloading child pornography (Re Seneca College and Ontario Public Service Employees Union, Local 560, 109 L.A.C. (4th) 334, 2002 L.A.C. Lexis 160, File No. MPA/Y200927 (2002). The professor, who had pleaded guilty to criminal charges, was given a suspended sentence and placed on probation for two years.

He sought to challenge his discharge from the college on the grounds that it arose from a mental disorder that could be considered a disability under Ontario's Human Rights Code. Accordingly, it was argued that he had been discriminated against on the basis of mental disability. The professor, who lived under difficult circumstances with his ageing parents, claimed to have used the Internet as an escape from the sadness and isolation that characterized his personal life. He claimed that he was unable to control his impulses.

The Court held that evidence did not support a conclusion that the professor was suffering from any form of medically recognized mental disorder. His inappropriate use of the college's computers was both selective and controlled, and the depression for which he was temporarily hospitalized was brought about by his impending dismissal from the college as a result of his misconduct. These findings served to neutralize any justification for therapeutic use, or and extenuation based on compulsive behavior. His dismissal from the college was upheld (see Smith, Grabosky & Urbas 2004: 79).

Freedom of Thought and Expression

The UDHR and the ICCPR establish rights to freedom of thought, conscience, religion and expression. In the digital age infringements could arise from both government agencies and business organizations and other individuals. In the case of organizations, surveillance of email and mobile phone communications could entail infringements of freedom of expression. In the case of individuals, the dissemination of spam, racist material or distributed denial of service attacks could infringe other people's human rights. Laws which restrict online content in various ways including obscene or defamatory materials could also involving breaches of freedom of expression.

These rights are obviously not unrestricted, and the Conventions allow for limitations in order to protect the rights or reputation on others and for the protection of national security, public order, public health and morals. Clearly, the Internet creates an environment in which these rights are difficult to balance.

In Australia, for example, several States and territories have enacted various criminal laws prohibiting racial and religious vilification, although at the Commonwealth level, as with privacy, the approach has been less punitive. In a case concerning Fredrick Toben's Adelaide Institute, for example, the Human Rights and Equal Opportunity Commission (HREOC) ordered a website questioning the historical occurrence of the Holocaust to be closed down, but there were no criminal penalties involved (Jones v Toben, 2001 / 2002, HREOC / FCA).

The issue of 'cyber racism' has also recently been addressed by the Council of Europe. In May 2001, the Council's Convention on Cyber crime was opened for

signature, together with a First Additional Protocol concerning criminalization of Racist and Xenophobic propaganda over the Internet, aimed at harmonized approach to the criminalization of such content as well as investigative issues and international assistance (Smith, Grabosky & Urbas 2004).

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 of convicted offenders 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 defendant's past conduct, involve no greater deprivation of liberty than is reasonably necessary to achieving those ends, they should survive a First Amendment challenge (Painter 2001, and United States v Ristine (Eighth Circuit, 2 July 2003) and United States v Mitnick (Ninth Circuit, 14 May 1998, 145 F.3d 1342 C.A.9 (Cal.), 1998)).

The famous case involving Kevin Mitnick who, in addition to being sentenced to almost five years' imprisonment and ordered to pay US$4,125 in restitution and to assign to his victims any proceeds he may receive from selling the story of his conduct, 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: cell phones, computers, any computer software programs, computer peripherals or support equipment, personal information assistants, modems, 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 or to access a computer system, computer network, or telecommunications network. In addition, Mitnick 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 Appeals Court held that the district court had not abused its discretion because the conditions imposed were reasonably related to legitimate sentencing goals and were no more restrictive than necessary. Conditions which restrict otherwise lawful activities are still legitimate when the defendant, by engaging in them, might be tempted to commit further crimes. Also, the fact that Mitnick may have engaged in otherwise prohibited conduct with his probation officer's approval made the conditions imposed less restrictive that an outright ban on such conduct.

The Appeals Court also rejected Mitnick's contention that the supervised release conditions impermissibly restricted the exercise of his First Amendment rights of freedom of speech. Despite the increasing pervasiveness and importance of the Internet as a communication tool, restrictions on access to such technology 'are proper if related to and reasonably necessary to promote the goals of sentencing.' As long as the conditions were expressly related to preventing recidivism and did not go beyond what was reasonably necessary, they would be valid. Mitnick also contended, that the district court erred by imposing supervised release conditions which restricted his employment in the computer and telecommunications industries as well as employment in which Mitnick would have access to computers and computer-related equipment. The district court was held not to

have abused its discretion because a reasonably direct relationship existed between Mitnick's possible occupation and his offences (United States v Kevin Mitnick, 1998 WL255343, 9th Circuit 20 May 1998).

The rights to participate in government and to vote by secret ballot or free voting procedures are specified in the Universal Declaration and ICCPR (UDHR article 21, ICCPR article 25). Where electronic or online voting procedures are used, potential infringements could arise from individuals who do not have access to computers being disenfranchised, surveillance of voting activities by citizens or from manipulation of information provided to voters. Problems of the authentication of the identity of individuals will also arise (Smith 2002).

Cruel and Unusual Punishment

Article 7 of the ICCPR provides that 'no one shall be subjected to torture or to cruel, inhuman or degrading treatment or punishment'. Capital punishment is still employed in a number of countries and in some rare instances in China, capital punishment has even been ordered for computer-related offences (see People's Daily Online 2000 – a case in which a 36 year old computer hacker in Hangzhou Province was sentenced to death for embezzling 1.66 million Yuan (about US$200,000) by counterfeiting bank paper and misappropriating funds from customers' accounts from the bank at which he was employed as an accountant).

The use of electronic monitoring as a punishment, if sufficiently invasive, could also, arguably infringe this article. Electronic monitoring is undoubtedly an invasive technology that involves the physical attachment of a device to a person. Modern technologies are also psychologically invasive in the sense that the person's every move can be tracked, other than when the device is programmed to be off. Fox (1987) reported that 'those who have experienced the regime of [electronically] monitored home detention indicate that it is psychologically wearing and more onerous in terms of self discipline than the world of prison'.

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 twelve months, irrespective of whether or not the police had reasonable grounds for believing that 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.

A more invasive development involves the use of computer chips embedded beneath the skin of offenders, albeit with their consent (The Economist 2002). Miniature tracking devices can be implanted beneath the skin and can track an individual's location as well as monitor physiological signs. Although these may be removed using a simple surgical procedure, the potential for civil action for any adverse consequences of the surgery or the implant itself, demands serious consideration before any such developments take place. Professional ethical issues also arise for doctors involved in the non-therapeutic

implantation and removal procedures. In the United Kingdom, there have been indications that the government may consider the use of surgically implanted devices for convicted pedophiles (Bright 2002).

Australia has recently enacted legislation that enables, inter alia, control orders, which may include electronic monitoring, to be made in respect of persons in situations in which such orders will substantially assist in preventing a terrorist act, or where it is suspected on reasonable grounds that a person has provided training to, or received training from, a listed terrorist organization (Criminal Code Act 1995 (Cth), Division 104).

In making an order, the Judge must be satisfied on the balance of probabilities that the order to be imposed is reasonably necessary and reasonably appropriate and adapted for the purpose of protecting the public from a terrorist act (s. 104.3(c)). Such a control order can be made for up to 12 months, except in the case of 16 to 18 year olds which can only be made for up to 3 months. Control orders cannot be made in respect of people less than 16 years of age. Failure to comply with a control order, such as by removing a tracking device, carries a maximum penalty of 5 years' imprisonment (s. 104.13). The Attorney General must provide written consent prior to such orders being sought from a Judge. Electronic monitoring is defined in the legislation as a 'tracking device' which means any electronic device capable of being used to determine or monitor the location of a person or an object or the status of an object (s. 100.1(1)).

Although the use of electronic monitoring in this context would entail similar issues to its use in correctional settings, the manner in which the legislation has been framed in Australia has raised numerous legal and human rights concerns (see, for example, Byrnes, Charlesworth & McKinnon 2005). These questions relate principally to the legal protections that govern the making of orders, their constitutionality and their compliance or otherwise with international human rights protections. Questions also arise concerning the effectiveness of such orders in enabling government agencies to gain useful information about terrorist threats. Clearly if a suspect were required to wear an electronic device, he or she would no longer be included in terrorist activities as the risks of detection would be substantial. It remains to be seen whether electronically-monitored control orders will be used, and to what extent, and whether or not these human rights concerns will eventuate. Once again, it needs to be emphasized that these potential infringements for human rights arise from the legislative measures introduced, rather than from the creation and use of the monitoring technologies themselves.

How Can We Prevent Human Rights Infringement in the Digital Age?

Ultimately, the prevention of human rights infringements in the digital age lies with individual legislatures which should ensure that new legislation complies with current international and local normative instruments. In addition, the private sector could play a part in preventing abuses by designing new technologies in ways that prevent or minimize potential human rights abuses. Thus, the protection of human rights can best be achieved through an interaction between technological innovation and policy reform.

First, hardware and software developers could be persuaded to build into new products technological solutions to problems that concern human rights when developing new technologies. An example is the use of systems which prevent illegal copying of data to protect copyright.

Second, it is important for the human rights implications of new technologies to be examined before they are introduced, not after. Fox (2001, p. 268) notes the need for academics to question the use of new technologies, while Kirby (1998: 331) has stressed the need for ongoing and informed debate about the social implications of new technologies, and the desirability of establishing global principles to guide the use of new technologies.

The following cautionary observation of Casella (2003: 92) is worth recalling in the present context:

> *The longer a technology is used, the more entrenched in life it becomes. When technologies are new, or are used in newer ways . . . their uses are easier to modify and their consequences easier to control. . . . If we wish to question the unintended consequences of these developments, now is the time to do so.*

Finally, rigorous evaluative research needs to be conducted once new technologies have been introduced in order to monitor their potential for denigration of human rights and infringements of international and national laws. The reporting requirements under international law should be taken seriously by governments and individuals and organizations should be encouraged to report infringing practices immediately they appear.

In the capitalist marketplace where corporate reputations are important, having a link to new technologies that infringe human rights may be a powerful deterrent and a useful way of ensuring that some of the more egregious developments in the digital age are avoided. At the same time, the development of technologies to protect and to enhance human rights could be a powerful marketing feature. An example would be the use of biometric user authentication technologies to protect personal identity information. Ideally, those responsible for technological innovation should work closely with human rights advocates and policy makers to prevent potential problems from arising during the development phase of new technologies, rather than devising solutions once problems have arisen and human rights have been infringed.

References

Arup, C., & Tucker, G. (1998). Information technology law and human rights. In Kinley, D (ed) *Human Rights in Australian Law.* (pp 243-66), Federation Press: Sydney.

Bright, M. (2002). Surgical Tags Plan for Sex Offenders. *The Observer* Retrieved on 24th October 2007 from http://society.guardian.co.uk/children/story/0,1074,842393,00.html

Byrnes, A., Charlesworth, H., & McKinnon, G. (2005). Human Rights Implications of the Anti-Terrorism Bill 2005. Letter of advice to Mr John Stanhope 18 October 2005. Retrieved on 24th October 2007 from http://www.chiefminister.act.gov.au/docs/_20051018.pdf

Casella, R. (2003). The False Allure of Security Technologies. *Social Justice*, 30 (3), 82-93.

Foucault, M. (1977). *Discipline and punish: The birth of the prison* (translation Allan Sheridan). Penguin Books: London.

Fox, R. G. (1987). Dr Schwitzgebel's Machine Revisited: Electronic Monitoring of Offenders. *Australian and New Zealand Journal of Criminology*, *20* (3), 131-147.

Fox, R. G. (2001). Someone to Watch Over Us: Back to the Panopticon? *Criminal Justice*, *1* (3), 251-276.

Kirby, M. (1998). Privacy in Cyberspace. *University of New South Wales Law Journal*, *21* (2), 323-333.

Semple, J. (1993). *Bentham's prison: A study of the panopticon penitentiary*. Clarendon Press: Oxford.

Smith, R. G. (2002). Electronic Voting: Benefits and Risks. In *Trends and Issues in Crime and Criminal Justice*, no 224, Australian Institute of Criminology, Canberra.

Smith, R. G., Grabosky, P., & Urbas, G. (2004). *Cyber Criminals on Trial*. Cambridge University Press: Cambridge.

Spigelman, J. J. (2005). The Internet and the Right to a Fair Trial. *Criminal Law Journal*, *29*, 331-339.

Taylor, G. (2001). The Council of Europe's Convention on Cybercrime and Australia: A Civil Liberties Perspective. *Cyber Law Research* p. 30.

The Economist. (2002). Something to Watch Over You: Surveillance. *The Economist,* 17 August.

Weeramantry, C, G. (1983). *The Slumbering Sentinels: Law and Human Rights in the Wake of Technology*. Penguin Books: Melbourne.

Weeramantry, C, G. (1990). Human Rights. In Wallace, J & Pagone, T (Eds) *Rights and Freedoms in Australia*, *(*pp 240-255), Federation Press: Sydney.