CRIME AND MEDIA

VOLUME 3

SAGE LIBRARY
OF CRIMINOLOGY

SAGE LIBRARY OF CRIMINOLOGY

CRIME AND MEDIA

VOLUME 3

Emerging/New Media and Crime

Edited by

Yvonne Jewkes

SAGE

Los Angeles • London • New Delhi • Singapore • Washington DC

First published 2009

SAGE Publications Ltd
1 Oliver's Yard
55 City Road
London EC1Y 1SP

SAGE Publications Inc.
2455 Teller Road
Thousand Oaks, California 91320

SAGE Publications India Pvt Ltd
B 1/I 1, Mohan Cooperative Industrial Area
Mathura Road
New Delhi 110 044

SAGE Publications Asia-Pacific Pte Ltd
33 Pekin Street #02-01
Far East Square
Singapore 048763

British Library Cataloguing in Publication Data

A catalogue record for this book is available from the British Library

ISBN: 978-1-84787-024-7 (set of three volumes)

Library of Congress Control Number: 2008933598

Typeset by Mukesh Technologies Pvt. Ltd., Pondicherry, India.
Printed on paper from sustainable resources
Printed by the MPG Books Group in the UK

Editor's Introduction

Emerging/New Media and Crime

Yvonne Jewkes

Part 1: Crime and the Surveillance Culture

In the popular consciousness, images of CCTV and other forms of surveillance are dominated by the figure of 'Big Brother', George Orwell's all-seeing, all-knowing, invisible superpower. In academic discussions of surveillance the dominant metaphor has been that of the Panopticon, an image that lends itself especially well to discussions of surveillance technologies which allow some individuals' to monitor the behaviour of others. The Panopticon, developed by eighteenth century reformer, Jeremy Bentham, was an architectural design that could be used for schools, factories, workhouses and any other social institutions that required the management of large groups of people by a small number of individuals with authority over them. It was, however, prisons that were thought to most exemplify the benefits of panoptic design.

In brief, Bentham's model for a prison consisted of a circular building with individual cells built around its entire circumference, and a central watchtower in which the activities of the prisoners could be constantly watched. A system of lighting that illuminated the cells but kept the inspection tower in darkness made it possible for just one person to monitor many inmates, each of whom knew they were under surveillance, but did not know exactly when. They were therefore obliged to behave as if they were being monitored at all times, and conformity and passivity were assured. The mental state of being seen without being able to see the watcher induced a fear that eliminated the need for visible deterrents or overt force.

The Panopticon was subsequently appropriated by others including, most famously, Michel Foucault, who took the ideological concept behind Bentham's structure and used it to demonstrate the potential of surveillance and social control. Writing about the plague at the end of the seventeenth century, Foucault (1977) describes how certain areas of a town were cordoned off and kept under continuous vigil with guards inspecting every part of the town to ensure that no-one escaped to spread the disease further. Consequently, like the inmates in Bentham's design for a prison, the town's population were not simply observed; the surveillance of them was intended to act as a deterrent, a caution to encourage them to behave in a certain way. Thus, for Foucault, Bentham's architectural design was not only a blueprint for future surveillance technologies which would allow a small, unseen few to observe the lives of the masses; it was a means of attaining absolute control over a conforming, docile population.

Over the last 20 years, scholars have appropriated the Panopticon as a metaphor for closed circuit television (CCTV) and other surveillance technologies. All

advanced industrial societies have experienced a rapid growth in the use of surveillance, to the extent where most citizens have come to take for granted that they are observed, monitored, classified and controlled in almost every aspect of their public lives. In fact the average person living and working in a major city is filmed up to 300 times a day. However, as the readings in this section show, the Panopticon is now falling out of favour with scholars because it is a fairly crude metaphor for the complex, interrelated, technologically sophisticated surveillance society we now inhabit. Some commentators have even dismissed the Panopticon as overly deterministic, abstract and paranoid.

One of the most prolific commentators on the surveillance society is Canadian scholar, David Lyon. In article 40, taken from his most recent book *Surveillance Studies: An Overview* (2007) Lyon explains why surveillance has become a central topic of public debate and political concern, particularly since the events of 9/11. In line with Giddens' (1985) definition, he uses the term 'surveillance' to refer to two related phenomena: the accumulation of coded information (e.g. from genetic material) and the direct supervision of some individuals by others who are in positions of authority over them (e.g. via CCTV). He moves away from panoptic metaphors which, he implies, have created bad theory, and attempts to provide a theoretical framework that can illuminate the causes, the courses and the consequences of surveillance, and their interconnectedness. Taking his cue from Foucault who invited his readers to use his work as a tool-box from which to select useful analytical equipment, Lyon references theorists as diverse as Durkheim, Weber, Simmel, Orwell, Ellul, Giddens, Zureik, Dandeker, Foucault, Deleuze and Bauman to map the field and 'explain' surveillance.

In another theoretical piece, Richard Jones (article 41) employs Foucault and Deleuze to develop a model of 'digital rule'; a form of 'at-a-distance monitoring' that has become possible with the advent of certain electronic technology. Jones examines some of the most important developments in criminal justice and social control through the lens of Deleuze's theories on 'control societies', including: managerialism; electronic monitoring of offenders; electronic access, exclusion, control and punishment (e.g. via biometric identity verification technologies); technology-assisted policing of physical spaces; and exclusion via withdrawal of access to 'privileges'. Advances in technology have arguably resulted in the disciplinary gaze being extended beyond the confines of closed and controlled environments such as the prison or the factory to encompass society as a whole and Jones is broadly concerned with the overlap between punishment of those individuals who transgress society's rules and laws, and the regulation of *all* citizens which can be intrusive, exclusionary and entirely unavoidable. In contemporary industrialized societies, if one wishes to take advantage of credit, withdraw money from a bank, work for an employer, vote in an election, purchase goods, attend a football match, drive a car, catch a train, use a mobile phone or surf the Internet, it is virtually impossible to remain anonymous.

Recent years, then, have witnessed the 'disappearance of disappearance' and this is the subject of article 42 by Kevin D. Haggerty and Richard V. Ericson. They point out, however, that one of the most obvious limitations of CCTV (and, indeed, of the concept of panopticism in relation to it) is the fact that disciplinary power is only complete when one-way total surveillance is combined with additional information about the individual being monitored; as they say, such surveillance is

'often a mile wide but only an inch deep'. To put it in its simplest terms, there is not much the police can do with a recorded image of an offence that has already taken place unless further data can be gathered about the offender – name, whereabouts, address, previous convictions, etc. – hence the use that the police make of TV programmes like *Crimewatch UK* (article 31) in appealing to the public to 'fill in the blanks'. However, depth, or intensity, of surveillance can also be achieved via the connection of different technologies (for example, digitised CCTV systems and computer databases) and institutions (such as the police and private security companies). Haggerty and Ericson refer to this convergence of once discrete surveillance systems as a 'surveillant assemblage'.

Even the most mundane monitoring of 'ordinary' citizens by CCTV, then, involves a nexus of cameras, computers, telecommunications and people. For example, in his study of CCTV in a northern English city, McCahill (2002) relates how individuals known to the CCTV operators – and known, not just because of previous offences that have been observed and recorded, but because they live in the same neighbourhood, were at school together, or play on the same sports team – may be subject to more intrusive and prolonged surveillance than those who are unknown to the security team. Frequently the police will make use of this accumulated knowledge, and security guards may tip them off about a suspect's movements, or allow community police officers to hang around in their control room observing the monitors. Equally, however, the fact that watchers and watched are known to each other inevitably places limits on the disciplinary potential of the surveillance systems because some private security officers are not willing to co-operate with the police about suspects who they know personally. For example, one security officer is quoted as saying, 'I wouldn't grass... on Tommo 'cause he's all right, he's never given me any bother' (McCahill, 2002: 199).

Taken together, the networks of people and institutions described in the articles here are often said to constitute a 'carceral society' (Foucault, 1977) whereby more and more aspects of public life are becoming subject to the kind of disciplinary power that we usually associate with the prison. In other words, the alliance of formerly discrete technologies into a surveillant assemblage is designed to create systems of discipline and domination. As Haggerty and Ericson point out in article 42, a great deal of surveillance is directed towards monitoring, codifying and controlling the human body. Surveillance of specifically targeted groups can be achieved via an interface of technology and corporeality that can range from direct physical contact between flesh and technological device, to more oblique or covert methods of producing information. The former would include the various forms of 'electronic tagging' that are now commonplace, such as securing an electronic tag round new-born babies' wrists or ankles in hospital which, not only contains personal information about the child and its medical condition, but also triggers an alarm if the infant is moved beyond a secure area. The electronic monitoring of offenders and those on probation, and the use of microchips inserted under the skin of pets to monitor their whereabouts, are also examples of the diversity of applications which exploit the flesh-technology-information amalgam.

Less direct forms of surveillance that rely on distanciated monitoring of corporeality include: the computer monitoring of keystrokes to assess output and effi-

ciency in offices; the visual surveillance of shop workers' body language to ensure that they are conveying the customer service ethos of their employer; toilet bowls that automatically check for drugs and CCTV cameras in cubicles that then film the people who test positive; sensors which monitor whether workers wash their hands after visiting the washroom; smart badges that track employees' movements; and various 'Big Brother' systems that check the performance quality of staff in call centres and other telephone-based work environments – including the number of calls taken and the number of calls with a 'successful' outcome in a given time period.

When it comes to techniques of identification, body surveillance extends beyond individuals and discrete groups to entire populations. In this respect, identity verification is achieved by means of 'biometrics' which are identification techniques based on physical attributes – fingerprints, palm scans, retina identification, body fluids, and so on. In the global surveillance society, one is no longer identified by what one has (e.g. a passport or credit card), or by what one knows (e.g. a personal identification number or PIN), but increasingly by what one *is* – a collection of unique body parts. Ironically, then, we have returned to the anthropometric preoccupations of the Positivist school of criminology with their measurements of the body, skull, etc. – albeit in a more sophisticated guise.

We can conclude from this discussion that there is nothing intrinsically new about the reduction of the body into micro sets of data. Primitive forms of biometric identification have existed for centuries, and advancements in photography and fingerprinting at the end of the nineteenth century coincided with the centralization and bureaucratization of administration and record-keeping. In fact, fingerprinting is a good example of a form of surveillance that has lost a great deal of its stigma through familiarity and diversity of use. Once used uniquely by law enforcement agents to identify suspected criminals, with all the negative connotations that such an application would evoke, the use of fingerprinting has expanded to include prestige cardholders, frequent flyers, club members and library users. Most of us may barely notice the extent to which we are at the centre of a surveillance society, so easily have we internalized the changes in our conduct: using swipe cards instead of keys to access our workplaces, booking flights and checking-in online, banking by telephone or computer rather than in person, and so on. Indeed, those most subject to many forms of surveillance are the most privileged who use credit cards, mobile phones and computers; and several commentators have taken exception to the idea that the powerful are exempt from the watchful gaze. Haggerty and Ericson concede that the targeting of surveillance *is* differential, but assert that it has nonetheless transformed hierarchies of observation, allowing for the scrutiny of the powerful by both institutions and the general population. Examples of 'bottom-up' surveillance include the introduction of CCTV systems into police custody suites and cells allowing the activities of custody officers to come under just as much scrutiny as those of the inmates and the global proliferation of video cameras that has resulted in numerous recordings of police brutality and government abuses of human rights.

There are, then, persuasive arguments that surveillance can be a good thing, although such arguments run counter to the stance taken by most academic criminologists, which is that surveillance systems are bound up with wider relations of power and discipline, reinforcing existing inequalities along traditional lines of class, gender, ethnicity and age. In particular, many critical criminologists have been sceptical (if not downright hostile) to the idea that surveillance technologies liberate,

empower and comfort the general citizenry. Among them are Roy Coleman and Joe Sim (article 43) who uphold the idea of panoptic top-down scrutiny which, they say, is exemplified by closed circuit television. Their analysis focuses on CCTV in the city centre of Liverpool, in the north of England and one of their central arguments is that the gaze of the surveillance camera is turned almost continuously downward on those who are already disenfranchised. By contrast, they say, there is a virtual absence of 'upward' surveillance of the powerful, whose often socially detrimental and harmful activities remain effectively beyond scrutiny and regulation.

In article 44 Gary T. Marx develops the arguments raised so far, and considers both pros and cons of surveillance, noting that protection of privacy is paramount in most public and academic discussions of surveillance. Marx's concern is broadly two-fold: to distinguish between traditional forms of surveillance and new and emerging technologies, and to highlight what he calls 'surveillance slack'; in other words, he distinguishes between the amount of surveillance available and the extent to which a technology is actually used. He states that the application of technology is frequently confused with its existence; hence the alarm that is created about issues such as personal privacy. He doesn't adhere to the pessimistic and deterministic views of technology put forward by Coleman and Sim; in fact he draws our attention to its democratizing impact, noting that the emergence of an ethos of self-surveillance has been empowering especially in the field of healthcare (with home tests for pregnancy, high cholesterol and AIDS among the self-administered kits now on the market). His overview thus highlights positive uses of new surveillance technologies (such as monitoring babies in hospital or having hidden cameras installed in ATM machines) as well as those innovations that would be troubling to some (e.g. the monitoring of employees' whereabouts and their email and phone communications).

We might conclude from Marx's article, and those that precede it in this section, that discussions of surveillance have a tendency to flatten the terrain of power, control and the role of individuals in social systems, and that a more finely nuanced approach is required. The Panopticon has been a useful metaphor for the notion of surveillance as social control and has given rise to several theoretical developments of the original concept, including 'super-panopticism' (Poster, 1990) and 'post-panopticism' (Boyne, 2000). You may recall that Brian Jarvis employs the image of the Panopticon in the penultimate reading of Volume 2 (article 39) in his critique of the film *The Truman Show.* Jarvis argues that, while not a 'prison film' as such, *The Truman Show* offers a bleak insight into post-industrial panopticism and is the culmination of the American film and its implications for contemporary developments in disciplinary technology. However, in its representation of a media-created world in which an unwitting victim is watched by millions of viewers via thousands of hidden cameras, *The Truman Show* is arguably more accurately thought of as an exemplary representation of 'synopticism', which is the subject of the next contribution by Thomas Mathiesen.

In article 45, Mathiesen argues that Foucault's interpretation of the Panopticon must – within the context of the 'total system of the mass media' (p. 219) – be supplemented by the Synopticon. In other words, in modern surveillance-rich and media-saturated societies, panopticism is intimately fused with synopticism in a process that simultaneously permits both top-down scrutiny by authority figures and bottom-up observation by the masses. The new breed of 'reality TV'

shows such as *Big Brother* and its many imitators are examples of phenomena that combine the panoptic and synoptic. Such television programmes are designed to allow the few to see the many (the programme producers in the studio gallery who observe the activities of the contestants 24 hours a day), while simultaneously and synoptically allowing millions of viewers to watch both participants and, occasionally, the 'watchers' themselves. More seriously, for Mathiesen, television news and the popular press act as Synopticons, devouring crime and purging it of every detail other than that which can be easily digested by a mass audience. It is, then, the essentialist, the sensational and the stereotypical elements of individual criminogenic characteristics and behaviour that get hurled back into society to terrify and panic. Of course, we have to remember that Mathiesen's article was written before the latest developments in Internet technology, with the appearance of Facebook, Youtube and the like, and that it pertains particularly to traditional and still very widely used media, with television as a prime example.

Synopticism has also been accelerated by the proliferation of video cameras, which have led to a number of instances where members of the public have filmed events that were not 'meant' to be seen, and then sold the footage to national television networks for broadcast around the world. For some, this is the essence of synopticism's appeal: 'surveillance footage represents one of the crudest satisfactions of the scopophilic drive, a sense of power at being privileged to see that which was meant to remain unseen: the point at which the private... goes public' (Dovey, 1996: 127).

Part 2: Crime, Deviance and the Internet

While the study of surveillance has now become established as a sub-field of criminology in its own right, an emerging area which is still very much in its infancy is cybercrime. Until a decade ago, very few criminologists were addressing this rapidly growing global phenomenon and, even now, major criminology textbooks that claim 'comprehensiveness' still appear on the market without reference to online crime. Part of the reason for this scholarly reticence may be the sheer size and scale of the problem. It took the World Wide Web just three years to reach its first 50 million users and this potential audience, which is now estimated at around one billion users, provides limitless opportunities for those who are criminally inclined and a vast marketplace for the (knowing or unwitting) recipients and consumers of their illegal activities. Cyberspace is also largely anonymous (although see Gies' comments about corporeality and performativity; article 51) and reconfigures time and space, so that offences can be initiated, and their consequences felt, in entirely different parts of the world. All these factors make cybercrime very difficult to research or even quantify.

One of the most obvious outcomes of this new information and communications revolution is its creation and distribution of unimaginably more information-based products which, in turn, pose new legal challenges to define and protect copyright. Put simply, the electronic transmission and reproduction of information has become so easy and so commonplace that many of those who routinely transfer, copy, and store material onto their own machines may not even be alert to the fact that they are engaged in theft. Another consequence of the vast scope and

pervasiveness of digital technologies is that new areas of social vulnerability have emerged. Spamming – for too long considered to be little more than an extension of conventional junk mail – is increasingly being recognized as an insidious and illegal activity. It can encompass electronic chain letters, links to pornographic sites, scams claiming that there are extensive funds – for example, from over-invoiced business contracts or a deceased relative's will – available for immediate transfer into the recipient's bank account if he or she just provides their bank details, fraudulent pyramid investment schemes, phoney claims for cancer cures and, following 11 September 2001, fake anthrax treatments and bogus test kits for the disease.

Information security, personal security and cyber-trespass encompass another area of cybercrime that has captured the public imagination. Fears concerning unauthorized access to high-security or sensitive information have been paramount within government and commercial institutions since the birth of the Internet, an unease partially borne out of its origins in American defence strategy. Among the potential consequences of deliberate acts of sabotage perpetrated by those with the skills and inclination to hack into a state's computerized systems are the capacity to disrupt water and electricity supplies, close all international communications, manipulate air traffic control or military systems, tamper with National Insurance numbers or tax codes, and paralyse financial systems. However, many commentators believe that while these kinds of possibilities are terrifying to contemplate, the likelihood of such calamitous events occurring through human or software error is far greater than the chance of malicious hackers or terrorists bringing down a country's infrastructure. For the time being, then, they remain the stuff of Hollywood writers' imaginations (see, for example *Die Hard 4.0*, dir. Wiseman, 2007) and most private individuals are more concerned about protecting the information held on their personal computers, particularly their financial transactions.

In fact, one of the first and most notorious computer viruses demonstrated that Hollywood was somewhat behind the times: the perpetrators of the 'Love Bug' virus were not geeky white kids living in an American suburb (as portrayed in countless movies) but three men living in Manila in the Philippines (http://www.landfield.com/isn/mail-archive/2000/May/0066.html). The virus, which sent the seductive headline 'I LOVE YOU' to tens of millions of computers around the world in 2000 is discussed by Marc D. Goodman and Susan W. Brenner (article 46). The virus took two hours to spread around the world destroying computer files and data. Assessments of the financial cost of the Love Bug virus vary, but are thought to be at least $2 billion (and potentially as high as $10 billion), while an estimated 45 million users in 20 countries were victims. Virus experts from the FBI traced the Love Bug to its source, but their investigation was thwarted when it became apparent that the Philippines had no cybercrime laws, which meant that Love Bug's creator had not committed a criminal offence in that jurisdiction. The suspect was charged with theft and credit card fraud on the basis that the virus was designed to steal passwords which, in turn, could be fraudulently used to obtain Internet services and goods, but the charges were dismissed as inapplicable and unfounded. He could not be extradited to the United States which does have laws governing cybercrime because extradition treaties require 'double criminality'; in other words, they require that the act for which the person is being extradited is a crime in both the extraditing nation and the nation seeking extradition. Although the

Philippines has since adopted new legislation which would result in heavy fines and/or a custodial sentence for the creator of a computer virus, it came too late for the investigators of the Love Bug, and no one was ever brought to trial.

Goodman and Brenner not only discuss the Love Bug but also consider why it was a landmark in the history of cybercrime, its regulation and legislation. A relatively early analysis of the subject (it was published in 2002), this article remains one of the most comprehensive histories and overviews of the subject. In it Goodman and Brenner call, not only for more attention to be paid to introducing new legislation to combat the growing problem of cybercrime, but also for their to be a more coherent international stance on the problem with 'joined-up' policy and legislation so that a future catastrophe on the scale of the Love Bug virus can be avoided.

In more recent work, Susan Brenner (2007) has argued that a model of reactive, police-based crime control – even with the backing of legislation - cannot protect society from cybercriminals. She has proposed what some might view as a controversial new model which holds users of cyberspace legally responsible for their own protection, and which holds the software industry liable if they take inadequate measures to ensure their products' reliability and security. The combination of self-policing on the part of users and voluntary compliance to new industry regulations by the 'architects' of cyberspace enforced by means of criminal sanctions (primarily fines) is, according to Brenner, the way forward if we are all to be protected from becoming victims of cybercrime (Brenner, 2007).

While the notion of Internet users taking responsibility for their own protection against victimization might appear a radical suggestion, it is an opinion endorsed by Emily Finch in article 47. Finch introduces us to two similar and much-publicized cybercrimes of recent times - identity fraud and identity theft - and explains what 'identity' is, and what it means for it to be stolen. In the news media, reports regularly appear of credit card numbers and other personal information being taken from the Internet and used fraudulently. Less common, but equally newsworthy are cases of individuals who adopt another (often deceased) person's identity wholesale, several examples of whom are mentioned in the chapter. Hijacking of others' identities has been facilitated by developments in information and communications technologies which enable the cheap and easy creation or manipulation of false documents such as passports, birth certificates and drivers' licences. In particular, the burgeoning ubiquity of the Internet has facilitated an unprecedented ease of access to personal information and - given the intimacy and anonymity that may characterize online relationships - has offered false promises of trust, security, invulnerability, etc. Finch discusses these shifts in social interaction, and argues that attempts to counteract identity theft which focus exclusively on the fixity of physical identity are addressing only a partial manifestation of the problem and inevitably will result in an incomplete and imperfect solution.

While information and communication technologies (ICT) are frequently associated with lone criminals operating in isolation (for example, hackers and virus planters are often regarded as archetypal computer geeks who lack conventional social skills) the criminal exploitation of online systems by groups of organized criminals is a growing problem. They are the subject of the next contribution by Kim-Kwang Raymond Choo and Russell G. Smith (article 48). In it, they discuss three types of offenders who use ICT in the pursuit of organized crime, and five

different elements of risk involved in their activities. Like other contributors to this Volume, they appeal to both legislators and to individuals and communities to be responsive to the threats posed by organized criminals.

Choo and Smith offer observations based on an international analysis but their particular focus on online crime in Asia is interesting and important given the exponential growth in Internet use on this continent. China alone has seen its use of the Internet grow from 23 million in 2000 to 162 million at the beginning of 2007 (http:// www.internetworldstats.com/asia/cn.htm). By 2008 that figure had risen dramatically again to 210 million, just five million behind the US. However, China is adding six million new Internet users a month which is more than 10 times the pace of US growth. The world's most popular blog is Lao Xu, written by the actor and director Xu Jinglei, which boasts 137 million visitors. The biggest distributor of online video is Tudou, which has overtaken YouTube with over one billion megabytes of data transfers every day. The Mandarin search engine Baidu has more hits than Google, and Chinese entrepreneur Jack Ma has set up Taobao to compete with eBay (http://www.guardian.co.uk/technology/2008/feb/09/internet.china). These examples are all the more remarkable given the Chinese authorities' fears about the potential uses of the Internet by 'subversives' (discussed in Volume 1).

The emancipatory qualities of the Internet have been much debated in recent years, with commentators usually arguing that cyberspace is a democratic space and a great leveller of inequalities. However Susan Zickmund (article 49) takes issue with this thesis, arguing that for every subversive or alternative voice that offers a perspective which is counter to the 'official' political line, there are countless individuals who use the Internet to propagate fear and harm. The promotion of racial hatred is unfortunately widespread and the Internet is a relatively cheap and accessible means of connecting similarly minded people across the world and coalescing their belief systems. The Net is a sophisticated tool for recruitment and unification, providing links between hate movements that were previously diverse and fractured, and facilitating the creation of a collective identity. Various groups on the political far right – Neo-Nazis, skinheads and groups with ties to the Ku Klux Klan – are using the Net to target a youthful and impressionable audience with racist, anti-Semitic and homophobic propaganda with little fear of the kind of legal sanction that might accompany the circulation of such material in more 'traditional' forms. As Zickmund points out, while Germany and many other European countries have criminalized the publication and distribution of hate propaganda, the Internet remains largely unregulated.

Having covered some of the most serious and feared cybercrimes – computer viruses, identity fraud and theft, organized crime, and hate crime, we now turn our attention to arguably the most challenging and pressing cybercrime of our age; the production and consumption of abusive sexual images of children. Max Taylor and Ethel Quayle, the authors of article 50, work in the *Department of Applied Psychology, University College Cork, Ireland and are founding members of the COPINE (*Combating Paedophile Information Networks in Europe) Project. They have probably written more extensively about this issue than anyone else and here they provide an overview of the nature of child pornography, focusing on legal and psychological perspectives. This dual analysis enables them to unpick some of the complexities underlying the regulation of Internet pornography; for example, the difficulties associated with legislating against fantasy. Taylor and Quayle also provide a typology,

or taxonomy, of different kinds of child pornography which has since been adopted by police and computer forensic experts to indicate the level of seriousness that downloaded images represent (see article 57 by Jewkes and Andrews).

Just as Zickmund (article 49) takes issue with the prevailing argument that cyberspace is essentially democratizing, so Lieve Gies (article 51) seeks to challenge the commonly perpetuated view that Internet use is a form of disembodied, and thus anonymized, communication from which performativity has vanished. Gies suggests that the notion that Internet users are free to indulge in identity play (and identity theft and fraud) due to the anonymity of cyberspace is becoming less tenable as enhanced bandwidth facilitates the exchange of bodily cues and creates stronger convergence with audio-visual media. She further argues that constructing the Internet as virtual and disembodied obscures the material and embodied lived reality in which technology operates. Of course, it is precisely the Internet's domestication and its advanced integration into everyday life in the 'real' world that has precipitated the growth of crimes such as the production of images of children being sexually abused, and Gies' article is useful in underlining just how quickly communication technologies move forward in both technological sophistication and expansion.

Part 3: Crime Control in a Global, Virtual and Mediatized World

It is the rapid advancement of information and communication technologies that make their use in criminal activities so difficult to monitor, regulate and police. The focus of this final section of *Crime and Media*, then, is crime control in a global, virtual and mediatized environment, and we start with a contribution by Katja Franko Aas (article 52) which draws upon many of the concepts raised elsewhere in this Volume, including globalization, the digital divide, identity, surveillance and synopticism. In a clear and concise overview underpinned by theories proposed by Castells, as well as many of the authors represented in this Volume, Aas discusses the challenges that cybercrime presents, both for criminologists and law enforcers.

As Aas observes, although most experts agree that thorough regulation of the Internet is impossible, there can be no doubt that the Internet has itself vastly extended the scope and efficiency of regulatory practices. Technology's increasingly sophisticated capacity for monitoring, tracking down and identifying individuals raises important questions concerning the 'policing' of cyberspace: what are the implications – good and bad – of the Internet's capacity to allow widescale regulation and surveillance of its users? Because the technology *is* inherently democratic and is available to 'authorities' beyond the police and state, the issue of privacy has become increasingly salient, yet the carceral net is widening and surveillance technologies are creeping in to virtually all aspects of everyday life. Yet who defines and identifies 'miscreants' and with what consequences to notions of citizenship and civil liberties?

In article 53 Majid Yar reflects on these important questions. Technology might give us a sense of freedom and opportunity but regulation and monitoring by authorities – whether they be governments or private, commercial interests – causes unease to many ordinary Internet users and remains of concern to civil liberties groups. Frequently defended on grounds of security, state surveillance of

citizens has been brought more sharply – and more sensitively – into focus by the events of September 11 2001. In an article entitled 'Say Good-Bye to Privacy', American writer Doug Barney puts forward a patriotic view of his government's response to the act of terrorism that, in the parlance of the mass media (and Danny Schechter in Volume 1, article 13) 'changed everything':

> Now most of us are thanking our lucky stars and stripes that our government has been spying on us. Western governments have repeatedly denied the existence of the Echelon network, but it was the 'nonexistent' Echelon that provided solid evidence (like bank transfers and phone conversations) to pinpoint the mastermind behind the terrorist attacks and justify the assault on the Taliban and Osama bin Laden camp (Barney, 2001: unpaginated).

The 'Echelon' system referred to is a US intelligent search agent used to monitor the communications traffic (especially Internet and mobile phone communications) of European citizens, politicians and military personnel; a sophisticated 'eavesdropping' device that is justified on grounds of terrorism and crime but has, as Yar observes, been found to routinely intercept valuable private commercial data. In addition, listening devices called 'carnivores' have been installed at several ISPs to monitor email traffic. But not everyone feels secure in the knowledge that state authorities have this level of power to monitor the communications and movements of individuals – not least because they failed to identify and act on the threat in the first place. Furthermore, as Chomsky intimates (in Volume 1, article 16) American governments have a long and troubled history of defining deviants, miscreants and people displaying the 'wrong kind' of patriotism. The prolonged period of moral hysteria that accompanied the war on communism reached its zenith during the 1950s period of McCarthyism, by which time the FBI was spying on hundreds of organizations to see if Communists had infiltrated them. In the 1960s and 1970s the FBI added to their files the names of anti-Vietnam War protestors, black nationalists, members of the women's liberation movement and numerous other groups, and surveillance permeated the activities of every police and military organization in the country. After a short period in the late 1970s, when the dismantling of the Soviet Union and the end of the Cold War saw calls for the protection of civil liberties take priority over concerns about communism, US foreign policy turned its attention to the War on Terror, and civil liberties once again became secondary to the zeal for rooting out dissidents and dissenters.

But as increased powers are given to authorities to monitor the activities of citizens, the question is raised of why law enforcement agencies *need* new powers when they do not necessarily make effective use of the considerable powers they already have. For example, British journalist David Rose (2001) suggests that the 11 September attacks might have been averted had security chiefs in America and Britain accepted the offer of Sudan's government (made over a six-year period prior to 9/11) to acquire a vast intelligence database on the man believed to be behind the attacks, Osama bin Laden, and more than 200 members of his al-Qaeda terrorist network, including material about their financial interests and plans. They also turned down the opportunity to extradite or interview key bin Laden operatives who had been arrested in Africa on suspicion of planning terrorist atrocities.

The conclusion to be drawn seems to be that the technology is only as good as the humans making use of it – or not. The limitations of electronic surveillance

methods are further illustrated by the finding that the hijackers responsible for the attacks on the World Trade Centre and Pentagon had organized their efforts via the Internet, co-ordinating their activities – unmonitored – from Internet cafés and libraries. Following 9/11, Osama bin Laden disappeared. US Intelligence has intercepted email traffic from members of his terrorist group suggesting that he retreated to a remote area of Pakistan but, despite a sustained military and surveillance operation, they have been unable to locate him or even say with any certainty whether he is dead or alive. Meanwhile bin Laden has reportedly eschewed his laptop computer for the more 'reliable' method of using human couriers to communicate with other members of his network.

While the global threat of terrorism is ever present in late modern societies it is, once again, the more 'micro' examples of surveillance via computer and information technologies that are of greatest concern to many ordinary people, such as the monitoring and interception of phone calls and emails by employers. In July 1999, twenty workers at a Cable & Wireless call centre in the UK were sacked or suspended, and a further 29 were told they faced serious disciplinary action, when managers at the centre concluded a six-week period of electronic surveillance during which they claimed to have uncovered thousands of pounds worth of theft in the form of 'stealing' extra cable TV channels. Cases at other companies have included disciplinary action and dismissal for employees who have sent risqué emails internally, been caught taking unauthorized rests at work, and booked holidays on the Internet during office hours. However, surveillance operations are frequently far from foolproof, and employers are themselves not above suspicion of using technology for immoral purposes. Indeed, the 49 Cable & Wireless workers referred to issued counter-accusations that the surveillance operation was an elaborate ruse by the company to avoid paying redundancy.

As we have seen from Aas (article 52) and other contributors to this Volume, Manuel Castells is one of the most influential theoretical commentators on the rise of the information society (see, for example, *The Rise of the Network Society*, 2000; and *The Internet Galaxy*, 2001). While having little to say about crime *per se*, Castells' work is firmly located within discourses of risk, surveillance and social exclusion, but in his most recent work, *Mobile Communication and Society: A Global Perspective* (2007), co-authored with Mireia Fernández-Ardèvol, Jack Linchuan Qui and Araba Sey, he is broadly optimistic about the opportunities that mobile communications afford. Article 54 is taken from this book and, in it, Castells et al. describe how young people have been at the vanguard of the mobile communication revolution, not only adopting it with openness and enthusiasm but also inventing new communicative uses for the technology available. The article included here is the conclusion from *Mobile Communication and Society* and so offers a summary of the social contexts in which new technology is embedded. Elsewhere in the book, Castells et al. observe that the diffusion of wireless technology in the 1990s was 'nothing short of extraordinary' and was due, in large part, to 'the embrace of the technology by the younger generation as the density of mobile communication users reached its high points in Japan and in Northern and Western Europe' (2007: 128). Quoting Holmes and Russell (1999: 69), they note that, not only does their sophisticated grasp of the technology give young people superiority over their elders, but it has brought about a 'tectonic shift in the contemporary formation of adolescent identity' (Castells et al. 2007: 141). Unfortunately, as criminologists are

aware, it has also made young people vulnerable to new forms of victimization, including mobile phone theft, cyberbullying and 'happy slapping' (where physical assaults are filmed and shared on mobile phones).

In the final three articles, we turn our attention to policing the Internet. The Love Bug case discussed above illustrates why efforts to police cyberspace have, to date, been considered largely futile. In article 55, David Wall discusses the challenges facing both state funded public police and other groups who have responsibility for 'policing' cyberspace, including individual users, Internet Service Providers and state funded regulatory bodies and task forces. While an early contribution to the field (the article was published in 1998) many of the problems Wall describes have not altered or improved significantly in the intervening decade. For Goodman (article 56) the main obstacle to policing cybercrime is bound up with the (state funded public) police's perception of themselves and their occupational culture. In a contribution provocatively entitled 'Why the police don't care about computer crime' Goodman outlines why they *should* care and offers advice on building a police force which is comfortable and competent with new information and communication technologies. Once again, this is one of the earliest discussions of policing cybercrime (published in 1997) but, as the authors of the final article in this collection testify, many of the observations made about the police's resistance to tackling offences in cyberspace still pertain in 2009.

Yvonne Jewkes and Carol Andrews (article 57) return to the problem of abusive images of children being bought, sold, or simply circulated, around the world via the Internet. Drawing on research primarily from the UK and New Zealand, but also from Australia, Canada and the United States, Jewkes and Andrews discuss the role of the police in terms of both the progress that has been made in recent years, and the obstacles that law enforcers still face in their battle to combat the trade in abusive images of children and in securing convictions in this area. They also discuss, following Quayle and Taylor (article 50), the thorny issue of who commits these offences, and question the frequently made assertion that media reporting of those who download abusive images of children (and, indeed, child abusers generally) constitutes the moral panic of our age, given the ways in which the mainstream media and associated cultural industries fetishize youth and youthful bodies. Such cultural hypocrisy is symptomatic of a mediatized society that perpetuates notions of 'otherness' and demonizes a handful of individual known paedophiles, while at the same time turning a blind eye to the fact that 80 *per cent* of child abuse occurs within the home. We have, then, come full circle from where we started in Part 1 of the first Volume of *Crime and Media* with an article that problematizes the notion of moral panics and implicitly counsels against a faithful adherence to models of media 'effects'.

References

Barney, D. (2001) 'Say good-bye to privacy', www.networkcomputing.com, 29th October: unpaginated.

Boyne, R. (2000) 'Post-panopticism', *Economy and Society* 29(2), May: 285–307

Brenner, S. W. (2007) 'Cybercrime: re-thinking crime control strategies', in Y. Jewkes (ed.), *Crime Online*, Cullompton: Willan.

Castells, M. (2000) *The Rise of the Network Society* 2nd edition, Oxford: Blackwell.
Castells, M. (2001) *The Internet Galaxy*, Oxford: Oxford University Press.
Dovey, J. (1996) 'The revelation of unguessed worlds', in J. Dovey (ed.), *Fractal Dreams: New Media in Social Context*, London: Lawrence & Wishart.
Foucault, M. (1977) *Discipline and Punish*, London: Allen Lane.
McCahill, M. (2002) *The Surveillance Web: The Rise of Visual Surveillance in an English City*, Cullompton: Willan.
Poster, M. (1990) *The Mode of Information*, Chicago: University of Chicago Press
Rose, D. (2001) 'Resentful West spurned Sudan's key terror file', *The Observer* www.guardoam.co.uk/archive, 30th September: unpaginated.