Crime Online

WILLAN
PUBLISHING

Edited by
Yvonne Jewkes

Crime Online

Edited by

Yvonne Jewkes

WILLAN
PUBLISHING

Published by

Willan Publishing
Culmcott House
Mill Street, Uffculme
Cullompton, Devon
EX15 3AT, UK
Tel: +44(0)1884 840337
Fax: +44(0)1884 840251
e-mail: info@willanpublishing.co.uk
Website: www.willanpublishing.co.uk

Published simultaneously in the USA and Canada by

Willan Publishing
c/o ISBS, 920 NE 58th Ave, Suite 300,
Portland, Oregon 97213-3786, USA
Tel: +001(0)503 287 3093
Fax: +001(0)503 280 8832
Website: www.isbs.com

First published 2007

Hardback
ISBN 13: 978-1-84392-198-1
ISBN 10: 1-84392-198-7

Paperback
ISBN 13: 978-1-84392-197-4
ISBN 10: 1-84392-197-9

Brtish Library Cataloguing-in-Publication Data

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

Project managed by Deer Park Productions, Tavistock, Devon
Typeset by TW Typesetting, Plymouth, Devon
Printed and bound by TJ International Ltd, Trecerus Industrial Estate, Padstow, Cornwall

Notes on contributors

Carol Andrews is Research Assistant at the University of Sheffield working on a Cyberprofiling project. She has previously worked as an Analyst with the Department of Internal Affairs in New Zealand profiling convicted censorship offenders. Her publications include 'Policing the Filth: The Problems of Investigating Online Child Pornography in England and Wales' in *Policing and Society* (2005) with Yvonne Jewkes, and 'Internet Traders of Child Pornography and Other Censorship Offenders in New Zealand' published by DIA in 2004.

Susan W. Brenner is NCR Distinguished Professor of Law and Technology at the University of Dayton School of Law. She has spoken at numerous events, including Interpol's Fourth and Fifth International Conferences on Cybercrimes, the Middle East IT Security Conference and the Yale Law School Conference on Cybercrime. She has published many articles and book chapters dealing with cybercrime, such as 'Cybercrime Metrics', *University of Virginia Journal of Law and Technology* (2004) and 'Toward a Criminal Law for Cyberspace: Distributed Security', *Boston University Journal of Science and Technology Law* (2004).

Rinella Cere lectures in Media and Cultural Studies at Sheffield Hallam University. She is author of articles on Italian media culture, on media representations of women, and more recently on gender and the Internet. She was one of the contributors to *Dot.cons* edited by Y. Jewkes (2003, Willan) with a chapter on 'Digital Counter-cultures and the Nature of Electronic and Social Movements'. Recent publications include a chapter on the Internet and gendered poverty: 'Bank Online for the Poor: The Internet, NGOs and Gendered Poverty', in *The Ideology of the Internet: Concepts, Policies, Uses* edited by K. Sarikakis and D. K. Thussu (2006, Hampton Press).

Stefan Fafinski is currently conducting research into the criminalisation of computer misuse at the University of Leeds. He is a Chartered Fellow of the British Computer Society and a Freeman of the Worshipful Company of Information Technologists. He recently won the BA 2006 Joseph Lister

Award for his lecture 'Computer Says No: the Social Aspects of Computer Misuse'. He is the co-author of *Identity Theft* with Emily Finch (forthcoming, Willan) as well as a regular contributor to Reading FC's premier shoddy fanzine *The Whiff*.

Emily Finch is a part-time Lecturer in Law at Brunel, Middlesex and the Open University. She has conducted research into the criminogenic potential of the Internet and other new technology and has published widely on this topic, including a chapter – 'What a Tangled Web We Weave: Identity Theft and the Internet' – in *Dot.cons* edited by Y. Jewkes (2003, Willan). Her work on identity theft was the subject of the Joseph Lister Award Lecture at the British Association Festival of Science in Dublin in 2005 and she is the co-author of *Identity Theft* with Stefan Fafinski (forthcoming, Willan)

Katja Franko Aas is Senior Researcher at the Institute of Criminology and Sociology of Law, University of Oslo. She has written extensively on the use of information and communication technologies in contemporary penal systems, including *Sentencing in the Age of Information: from Faust to Macintosh* (2005, Cavendish/Glasshouse Press). She is currently working on a project on ICTs and border controls and completing a book entitled *Globalization and Crime* (forthcoming, Sage).

Yvonne Jewkes is Reader in Criminology at the Open University. She has published several articles and chapters on the problems of policing cybercrime, as well as more generally about the relationship between new technologies, crime and deviance. Her books include *Dot.cons: Crime, Deviance and Identity on the Internet* (2003, Willan) and *Media and Crime* (2004, Sage). She is also Editor of *Crime, Media, Culture: An International Journal.*

Robert Moore is an instructor of Criminal Justice at Delta State University in Cleveland, Mississippi, USA. He has published several articles and chapters dealing with the interaction between crime and technology. His books include *Cybercrime: Investigating High-Technology Computer Crime* (2006, Anderson) and *Search and Seizure of Digital Evidence* (2005, LFB Scholarly). He is also a certified law enforcement officer who assists in the investigation of computer-assisted crime.

Russell G. Smith is Principal Criminologist at the Australian Institute of Criminology where he heads the Global, Economic and Electronic Crime Program. He has carried out research and published extensively on aspects of computer crime, fraud control, and professional regulation. His latest book *Cyber Criminals on Trial* (2004, Cambridge University Press), jointly authored with Peter Grabosky and Gregor Urbas, was awarded the

Distinguished Book Award of the American Society of Criminology's Division of International Criminology in 2005.

Maggie Wykes is Senior Lecturer in the Law School, University of Sheffield. She teaches in the areas of criminological theory, gender and Internet crime and her research focuses on issues of representation, identity, criminalisation and power. Her book publications include *News, Crime and Culture* (2001, Pluto Press) and, with Barry Gunter, *The Media and the Body* (2005, Sage).

Majid Yar is Senior Lecturer in Criminology at Keele University. He has published a number of journal articles dealing with cybercrime issues such as computer hacking and media piracy, as well as broader theoretical issues around online offending. He is the author of *Cybercrime and Society* (2006, Sage).

Contents

Chapter 1

'Killed by the Internet': cyber homicides, cyber suicides and cyber sex crimes

Yvonne Jewkes

Introduction

In recent years a number of high-profile, salaciously reported Internet offences have come to public attention, leading to calls for greater self-regulation, tougher legislation and even censorship. Anxiety about the power of the Internet to influence dangerous or vulnerable users reached an apotheosis in early 2004. The headline 'Killed by the Internet' appeared in the *Daily Mirror*, a British tabloid, on 5 February 2004. There were a number of stories in circulation at the time that this blunt and sensational headline could have referred to. Less than a week earlier, a self-confessed cannibal who killed, cooked and ate a man he had met over the Internet was sentenced to eight and a half years in prison by a German court. The relatively lenient sentence was imposed because he was found guilty, not of homicide, but of the less serious crime of manslaughter, following evidence that the victim had given his consent to being killed and eaten. According to a newspaper report, the offender's willingness to cooperate with the police had 'helped shed light on the murky world of online cannibals' estimated to number in excess of 800 participants (*Guardian*, 30 January 2004).

Another story that might have been headlined 'Killed by the Internet' reported in the British press during the first week of February 2004 was the Amnesty International report that revealed that the Chinese government was becoming increasingly heavy-handed with people using the Internet to circulate anti-government beliefs. In China all Internet Service

Providers (ISPs) have to register with the police and all Internet users must sign a declaration that they will not visit forbidden sites (among those routinely blocked are news, health and education sites, although pornography sites are virtually unregulated). The Amnesty report noted that 54 individuals had been arrested, largely either for organising online political petitions or for criticising the government for policies which, it was claimed, were contributing to the spread of AIDS and SARS. Arrestees faced sentences of up to 12 years, but Amnesty reported incidents of torture and even deaths in detention (http://web.amnesty.org/web/content.nsf/pages/gbr_china_internet; cf. *Guardian*, 7 February 2004: 'China tightens net around online dissenters').

A third possible contender for the headline 'Killed by the Internet' is a story that has emerged intermittently over the last three years. According to reports, there are dozens of 'suicide sites' which are said to be responsible for the self-inflicted deaths of hundreds of people each year. A report in the *British Medical Journal* notes that some of the suicide websites are highly graphic, with copies of suicide notes, death certificates and colour photographs. There are also electronic bulletin boards, where suicide notes or suicidal intentions are posted, and one site alone has 900 postings a month, mostly from people considering suicide (http://bmj.bmjjournals.com). In Japan, 55 people reportedly took their own lives in 2004 after visiting suicide websites, and 91 people did so in 2005 (*Independent*, 10 February 2006). Many die in groups, often by carbon monoxide poisoning in sealed vehicles at secluded or scenic places, having met each other only hours before following initial contact via the Net. However, police in Japan have also investigated Internet sites that supply cyanide capsules to customers who – to use the phrase from the site – 'do not know how to obtain the right drug' (http://news.bbc.co.uk). Most of the individuals involved are in their teens, twenties or early thirties and many are drawn from the *hikkikomori* – social recluses who lock themselves in their rooms with just television and their computers for company, sometimes for years on end. While the *hikkikomori* is a phenomenon that appears to be unique to Japanese society, the use of Internet suicide sites to meet, share stories and impart advice on how to die is not confined to that country, and cases have been reported in the US, UK, Australia, Sweden, Germany, South Korea and Hong Kong, among others. One of the most infamous cases occurred in January 2003 when the naked body of a young American man, Brandon Russell, was found lying on his bed by his mother. The 21-year-old had died after taking marijuana and prescription drugs with alcohol. Disturbingly, he had taken the drugs, lapsed into a coma, and died while being watched by twelve 'friends' who he had met in a 'suicide chat room' and who observed and encouraged his actions via a live webcam feed over the Internet. Brandon Russell's last words, typed to the twelve witnesses to his death, were 'Told u I was hardcore' (*Telegraph*, 9 February 2003).

Thankfully, 'Killed by the Internet' did not refer to the use of Internet chat sites by a paedophile to groom children as a precursor to real-life abuse, abduction and murder, though a case that unfolded at the same time as this headline appeared was that of the trial of a 31-year-old American man, found after a high-profile police hunt for a twelve-year-old British girl whom he abducted after meeting her in an chat room. Following the child's safe return home it was reported that police in Toby Studabaker's home town found downloaded child pornography on his computer, and discovered that he had a previous criminal record for unlawful sexual conduct in the United States. In court, the prosecution detailed how the ex-marine had 'groomed' the child over a period of eleven months, during which their exchanges had developed into cyber-sex. He pleaded guilty at Manchester Crown Court to abduction and incitement of a child to commit an act of gross indecency. Further charges against him included transporting a child across international borders for the purpose of sexually exploiting her and using the Internet to entice a child to engage in criminal sexual activity (*Manchester News*, 13 February 2004).

Three months after 'Killed by the Internet' dominated the front page of the *Mirror* another disturbing case emerged in Manchester. Reported by the *Manchester News* under the headline 'Boy Planned Own Murder on Internet', the bizarre story unfolded of a 'gifted' schoolboy who 'brain-washed and groomed' an older boy he had met online (*Manchester News*, 28 May 2004). The 14-year-old instigator, 'John', created a series of fictional characters in chat rooms, one of which – a female spy called Mary – ordered his 15-year-old friend, 'Mark', to murder him. After exchanging 56,000 lines of email, they met up in June 2003 and travelled to the Trafford Centre in Manchester, where they bought a knife. The following day, they met again and Mark stabbed John twice in the chest and stomach, an assault that he survived. Mark admitted attempted murder and was served with a two-year supervision order and ordered to have no further contact with his friend; John admitted incitement to murder and perverting the course of justice and received a three-year supervision order. He was also banned from using the Internet unless accompanied by an adult. Although an offence such as this would normally carry a custodial sentence, the trial judge noted that these could not be described as 'normal circumstances' and that 'skilled writers of fiction would struggle to conjure up a plot such as that which arises here' (http://bbc.co.uk/news). Depicted as being from 'respectable homes' and doing well at school, the detective investigating the case is reported as saying, 'Neither . . . boy are geeky computer nerds living solitary lives. They are both perfectly normal children. No single event has ever more clearly shown the dangers of the Internet' (*Manchester News*, 28 May 2004).

Although any of the above stories arguably could have appeared under the grisly headline 'Killed by the Internet', in fact it was used in reference

to the homicide of music teacher, Jane Longhurst, who was sexually assaulted and murdered by an acquaintance who reportedly used images downloaded from the Internet to fuel his deviant sexual desires. Graham Coutts was a frequent visitor to Internet sites which featured graphic images and accounts of necrophilia and death by asphyxiation. Having killed his victim at his home in Hove, East Sussex, Coutts hired a storage unit where he kept and visited the corpse every few days until, nearly a month later he removed and set fire to it. After he had disposed of the corpse in this way, he continued to visit sites with names such as 'Necrobabes' and 'Violent pleasure', according to detectives who examined his computer hard drive. Although these sites contravene the Obscene Publications Act of 1959, the UK authorities have no powers to close them down because they are hosted by service providers in other countries. Coutts was sentenced to mandatory life imprisonment with a tariff set at 30 years.

In the first decade of a new millennium these seven cases provide a snapshot of Internet-related crimes that have resulted in the abduction, torture or death of individuals in countries around the world. Of course, there is nothing inherently sinister in the technology itself. Most cybercrimes are reasonably common offences; computer technologies have simply provided a new means to commit 'old' crimes, and it is clearly not the case that if the Internet did not exist, neither would violent and sexual crimes. What makes the role of the Internet unique in these cases, and mitigates against the argument that criminal and anti-social activities on the Internet are analogous to similar behaviour in the physical world, is its scale and reach. As John Naughton (1999) points out, it took the World Wide Web just three years to reach its first 50 million users; a feat which eluded television for 15 years and which took radio 37 years to achieve from its point of inception. A mere decade after it became a domestic, as opposed to military, technology, the number of Internet users was estimated at around 1 billion and, in the UK, a recent study found that Internet use has overtaken television as the chief non-work activity (apart from sleeping), with the average user spending around 164 minutes online every day compared with 148 minutes watching television. While these figures are disputable (the survey was conducted on behalf of the Internet search engine, Google), there is no doubt that we are witnessing a rapidly growing trend towards the broad adoption of the Internet thanks not only to changing leisure patterns and an increase in high-speed broadband connections at home, but also to increased business connectivity which allows office workers to surf the web all day (*Guardian*, 8 March 2006).

In addition to this inexorable growth in numbers of people regularly using it, if we consider the anonymity afforded by the Net, the sensation of many cybercrimes being 'underground' activities carried out in 'clubby' atmospheres in the company of like-minded individuals, and the lower risk of detection that accompanies most cybercrimes, it is little wonder

that the Internet has become a scapegoat for a series of local and global moral panics. As an editorial in the *Guardian* (6 February 2004) commented: 'for all it gives us, the Internet, it seems, cannot escape being portrayed as a terrible curse as much as a blessing'.

Of course, a link between Internet content and violent crime is difficult, if not impossible, to prove and the most that can be said with any degree of certainty is that individuals who might otherwise have been predisposed to commit suicide, murder or abduction might be drawn to the Internet to facilitate their desires, particularly if their behaviour receives support from communities of other people who are sympathetic to their thoughts, values and behaviour. Like wider debates about the effects of harmful media content, much mediated public discourse about computer-related crime is underpinned by a strong technological determinism (that is, overstating the power of the Internet and underplaying the importance of the individual actor). Where the human element *is* central to a story, it tends to be dominated by positivist notions of vulnerable offenders (frequently characterised – as the police detective in the case outlined above put it – as 'geeky computer nerds living solitary lives').

Furthermore, much of the debate about Internet regulation and censorship appears to be based on speculative notions of the anti-social and harmful impacts it may have at some point in the future. Such predictions of apocalyptic meltdown include terrorist acts intended to sabotage water, gas and electricity supplies, close all international communications, manipulate air traffic control or military systems, hack into a hospital's computer system and alter details of medical conditions and treatments, tamper with National Insurance numbers or tax codes, and paralyse financial systems. However, most 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, mercenaries or terrorists bringing down a country's infrastructure (Hamelink, 2000) and, for the time being at least, they remain hypothetical possibilities rather than perpetrated acts of aggression (Jewkes, 2003).

The book

The dual nature of the Net – its capacity to pervert and to democratise – underpinned many of the chapters in the predecessor to this volume, *Dot.cons: Crime, Deviance and Identity on the Internet* (Jewkes, 2003). *Crime Online* takes up this theme, demonstrating that, despite the Internet offering its users freedom, democracy and communication with people around the world, anxieties concerning its potential to corrupt or facilitate heinous crimes persist in the popular imagination. However, where one of the primary focuses of *Dot.cons* is gender, sexuality and notions of

sexual deviance, *Crime Online* represents a more concerted attempt to explore different constructions and manifestations of cybercrime and diverse responses to its regulation. Since the publication of *Dot.cons*, cybercrime has burgeoned into an established sub-field of criminology, and this second volume brings together some of the most renowned international scholars writing about cybercrime today.

In Chapter 2, Susan W. Brenner urges us to examine how we control the incidence of cybercrime. Historically, societies have responded to the transgression of rules and norms by creating laws to proscribe certain types of conduct 'crimes' and by employing specialists to enforce those laws by apprehending violators, who are then officially sanctioned. However, as Brenner points out, this model of reactive, police-based crime control cannot protect society from criminals who use computer technologies because cybercrime does not conform to the assumptions that structured this model. For one thing, cybercrime is transnational, which makes it difficult, if not impossible, for local law enforcement to react effectively to cybercrime. For another, cyberspace lets criminals assume impenetrable anonymity and pseudonymity, which further complicates the law enforcement process. The chapter thus proposes what some might view as a controversial new model of 'distributed security' that would supplement the reactive model (which we will still need for real-world crime) and allow us to deal more effectively with cybercrime. The new model holds users of cyberspace legally responsible for taking reasonable measures to protect themselves and others who might be affected harmfully by their actions (or inactions), and 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.

While the notion of Internet users taking responsibility for their own protection against victimisation might appear a radical suggestion, it is a theme that runs through many of the chapters in *Crime Online*, and is certainly endorsed by Emily Finch in Chapter 3. She introduces us to two similar and much-publicised 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 characterise 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.

In Chapter 4, Russell G. Smith picks up this theme and offers an analysis of some of the solutions being developed to the problems of identity fraud and identity theft described by Finch in the previous chapter. In an attempt to combat the problem of stolen identity, Smith notes that there has been a move away from knowledge-based systems and tokens towards using biometric technologies to identify people. Biometrics appears cutting edge (there is a suggestion of James Bond-style futurism about technologies such as iris recognition), and despite the significant costs involved, these technologies are attractive to governments and political parties who electioneer on issues such as illegal immigration and terrorism. Smith's chapter examines the many considerations that arise in deciding whether or not to use biometrics for logical access control. His conclusions support the views of Finch; that is, that although biometrics will reduce some of the risks associated with fraud in cyberspace, it will not solve the fundamental issue of determining whether an individual is who they claim to be.

While the call for a greater awareness of our own role and potential complicity in cybercrime is a laudable goal, there is possibly a danger that, in protecting ourselves and our own computers, we turn a blind eye to the bigger picture of Internet-facilitated, transnational, organised crime, including the growing industries in trafficking, violation and exploitation of vulnerable people. In Chapter 5, Yvonne Jewkes and Carol Andrews examine 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 (where Andrews was until recently employed at the Censorship Compliance Unit in the New Zealand government's Department of Internal Affairs), but also from Australia, Canada and the United States, they discuss the nature and content of 'child pornography' and the characteristics of offenders who download offensive material. Their analysis of content and users is set in a cultural context; they 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 fetishise youth and youthful bodies. Such cultural hypocrisy is symptomatic of a

mediatised society that perpetuates notions of 'otherness' and demonises a handful of 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. It might be argued, however, that the Internet has propelled the problem of sexual exploitation of children into the open and made public a crime that was previously confined to a privatised and exclusive environment. In theory, this might suggest that policing child sexual abuse has become a more straightforward endeavour, and 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.

One of the difficulties faced by the police and other law enforcement agents is that technology moves so quickly and they seem to be playing an endless game of 'catch-up' with a computer literate criminal elite who always seems to manage to stay one step ahead. In Chapter 6 Robert Moore provides an introductory overview of computer forensics, describing what is meant by the term and how computers store data. He offers a detailed analysis which is admirably free of baffling technological jargon, and goes on to discuss the techniques investigators and law enforcers use to recover incriminating evidence from computers and the processes they have to go through in order to bring a case to trial. His analysis concludes with a discussion of the future of computer forensics investigations, in which he highlights similar problems to those discussed in the previous chapter in relation to policing child pornography, namely, recruiting, training and adequately resourcing police officers and investigators to conduct work that is often both tedious and undervalued.

The focus of the next four chapters is the extent to which new crime problems are being socially constructed in the era of the Internet. Chapter 7 by Majid Yar explores the development of 'piracy' as a contested crime problem, tracing in particular the ways in which corporate moral entrepreneurship has attempted to create a new normative consensus around cultural copying, and the ways in which this labelling process has been received and contested by those identified as 'pirates'. Yar notes that, since the development of Napster and other Internet file-sharing services, online sharing and downloading of music, film and computer software has become one of the most hotly debated forms of online crime. The copyright industries have targeted file-sharers – more often than not young people – branding them 'criminals' and 'thieves'. Advocates of cultural copying and 'borrowing' have responded by claiming that they are being unjustly criminalised, and that the real villains are not music fans but the music industries who exploit artists in the pursuit of profit.

In Chapter 8, Stefan Fafinski explores the persistent moral panics that have been whipped up throughout history around football violence. One of the most recent manifestations of media hysteria, according to Fafinski,

concerns the use of the Net to mobilise football 'firms' and to orchestrate organised hooliganism. While it is not particularly surprising that the Internet (like mobile phones) is used as a primary means of communication by individuals planning disorder (it has also been used by coordinators of riots against the police in numerous towns and cities, including the violent disturbances on the streets of Paris in 2005, and has similarly been deployed by both fox hunters and hunt saboteurs in the UK), nonetheless, the importance of the Internet may have been greatly exaggerated by the popular press. Like all news stories, the perennial tales of anticipated football hooliganism that arise before, and during, every major soccer tournament rely on an element of novelty to breathe new life into them. The growth of the Internet has provided precisely that – a new angle on an old story. However, like much popular press coverage of new media, the red-top newspapers invariably fall back on technological determinism, 'blaming' the Internet for mobilising like-minded thugs and displacing violence from the CCTV-protected stadia to the streets outside the grounds. Meanwhile, as Fafinski demonstrates, the Internet has actually played a relatively minor part in football violence over the last decade – except in encouraging hate email to be sent to referees whose decisions on the pitch incite the ire of hooligans and 'ordinary' fans alike.

Yar's comments on the culpability of major media industries (at least as it is perceived by some music fans) and Fafinski's discussion of the role played by traditional media in 'creating' a social problem and scapegoating cybertechnologies are echoed in Chapter 9 where Maggie Wykes discusses the emergence of cyberstalking and the role of cyberspace in real-life stalking. She traces the processes by which stalking went from deviant behaviour or social harm to illegal act, and argues that the impetus for the criminalisation of stalking (both real and cyber) came from celebrities and from the beauty, fashion and media industries they support. Like other criminalised activities (Wykes briefly discusses 'mugging' and 'grooming'), stalking is regarded as an offence that the USA has exported to the rest of the world and one that has relied on sustained attention from traditional media to be brought to the public's attention. But also like those offences, media coverage has skewed the picture, in this case by overlooking or ignoring the mundane reality of crimes of harassment, including the everyday harassment experienced by many women in all spheres of life. At the same time, popular media routinely report cases of celebrity victims and their costly recourses to the law giving the impression that it is the young, wealthy and beautiful who are the most likely victims of cyberstalking. Wykes also links the emergence of stalking to the growing prominence of victimology in academic, political and popular discourses which, among other things, gives credence (frequently upheld in law) to celebrities' claims of feeling 'violated' when stalked by paparazzi and photographed in unflattering poses or career-damaging situations. Such actions not only threaten to

spoil and devalue their most precious commodity, but also undermine the carefully managed images they post on their own websites.

Like Fafinski, Rinella Cere also looks at the use and role of the Internet in enabling individuals to orchestrate group violence, but in Chapter 10 the focus is on the 2005 riots in Paris, the ongoing conflict in Palestine and the wave of Islamophobia that has intensified in the western world since 11 September 2001. Cere's contribution is, in many ways, a development of her earlier chapter in *Dot.cons*. There, she also discussed the role of the Internet in circulating information and gathering support for radical politics and alternative social movements. However, her theme was gender and the means that information and communications technologies afford women in their political struggles against neo-liberal economic forces and structural inequalities. In *Crime Online* she applies a similar analysis in a different context, and her conclusions echo those of Stefan Fafinski and Maggie Wykes in earlier chapters and pre-empt the views of Katja Franko Aas in the following chapter, namely that technological determinism underpins much discussion of new media, especially, and somewhat ironically, in the 'old', traditional media, a tendency that leads to the criminalisation of some (sometimes quite benign) online activity and makes spurious links between online 'incitement' and 'real-life' disorder.

Finally, Chapter 11 by Katja Franko Aas explores the dynamics between offline and online aspects of governance, and discusses the dichotomy between popular perceptions of the Internet as a bastion of freedom and unregulability and the increasing importance of various kinds of regulation of the Net to thwart cybercriminals. In a sophisticated analysis that draws on the work of (among others) Baudrillard, Žižek and Lessig, Aas explores the 'real' impact that virtual harms and simulations have, and the increasing centrality of the Internet in all discursive and practical aspects of crime and punishment. Given the inextricable interweaving of offline and online crime and governance of crime, Aas also criticises academic criminology for its neglect of the cyber realm, noting that the subject tends to be consigned to specialist publications dedicated solely to the topic. Perhaps this is not surprising given the inadequate, and frequently non-existent legislation covering the virtual realm, as mentioned in earlier chapters: 'if the law fails to address cybercrime, why should criminologists?' might be an anticipated response among our academic colleagues. While *Crime Online* is arguably guilty of perpetuating the ghettoisation of cybercrime, it is – like its companion volume *Dot.cons* – intended to be read by those who are less interested in 'techy' jargon and legal statutes, and more interested in new social behaviours and the evolution of crime. As Aas observes, in a post 9/11 world, information and communication technologies have become a primary locus for the construction of 'Others' and have given new impetus to contemporary strategies of social exclusion. While *Crime Online* is undeniably a book about the virtual