Trends & issues in crime and criminal justice

Australian Government
Australian Institute of Criminology

No. 388 February 2010

Crime risks of three-dimensional virtual environments

Ian Warren and Darren Palmer

Foreword | *Three-dimensional virtual environments (3dves) are the new generation of digital multi-user social networking platforms. Their immersive character allows users to create a digital humanised representation or avatar, enabling a degree of virtual interaction not possible through conventional text-based internet technologies. As recent international experience demonstrates, in addition to the conventional range of cybercrimes (including economic fraud, the dissemination of child pornography and copyright violations), the 'virtual-reality' promoted by 3dves is the source of great speculation and concern over a range of specific and emerging forms of crime and harm to users. This paper provides some examples of the types of harm currently emerging in 3dves and suggests internal regulation by user groups, terms of service, or end-user licensing agreements, possibly linked to real-world criminological principles. This paper also provides some directions for future research aimed at understanding the role of Australian criminal law and the justice system more broadly in this emerging field.*

Adam Tomison
Director

Debate over the potential harmful and criminological impacts of virtual worlds first emerged when North American journalist Julian Dibble (1993) documented the Mr Bungle case. It involved an alleged 'virtual rape' of a female user in the purely text-based virtual world called LambdaMOO. Any connection between a virtual and real crime in this case is highly debatable, because the harm involved 'a real-time non-consensual textual description of the rape' through 'the display…of graphic and offensive…sentences' (Lastowka & Hunter 2004: 295). Nevertheless, since the early 1990s, the rapid technological evolution and global appeal of many Web 2.0 social software platforms such as *Facebook* and *MySpace* (Coates, Suzor & Fitzgerald 2007), ensures new forms of user-generated internet content and 'virtual-reality' pose various risks worthy of ongoing criminological investigation (Williams 2006).

Smith, Grabosky and Urbas (2004) define cybercrime as the use of digital technologies to commit an offence, behaviour targeting communications technologies, or the use of these technologies for the commission of other crimes. Along with improved graphic capabilities, their global reach and their immersive or 'inter-real' character, the European Network and Information Security Agency (ENISA) identify five additional characteristics of three-dimensional virtual environments (3dves) or virtual worlds:

- persistence, meaning that the virtual environment as it is seen by all users is the same and continues to host activity even when users log out (unlike video games, which shut down when the user logs off);
- central storage on a database controlled by the service provider;
- users interact in real time;
- a set of physical laws to determine how interactions take place 'in-world'; and
- participation by using an 'avatar' (de Zwart 2009).

These characteristics add to the degree of 'presence' associated with 3dve use (Boellstorff 2008). This feature is the main challenge 3dves pose to conventional understandings of cybercrime and cyber-harm.

Games and worlds

Most current generation 3dves are goal-directed multi-user games. *World of Warcraft* boasts over 11.5 million members worldwide (Blizzard 2008) within a platform containing various fictitious digital landscapes. Users pay an initial fee to purchase the gaming software, then additional monthly participation fees. Users must complete various goal-directed quests, such as slaying monsters or gathering special items, with the complexity of tasks and rewards for successful completion increasing the further one journeys through each stage. The platform also allows users to forge ongoing social ties, while receiving training for in-world roles and exchanging virtual currency to complete game-based objectives.

In contrast, *Second Life* is not a goal-directed game, although it supports many game-related activities. Abrahams (2007) describes *Second Life* as a virtual world promoting various business, educational, artistic and governmental activities.

With over 14 million users and 27,000 parcels of land, the distinctive feature of *Second Life* is a thriving market economy. Linden Lab, the platform administrator, actively encourages trade through the LindeX currency exchange. In April 2009, Linden$260 were the equivalent of US$1 and around Linden$5,851,223,689 were in circulation (Linden Lab 2009a).

Users are charged small fees to upload content into the platform. However, the bulk of trading activity involves land sales, the exchange of goods and services such as clothing, prefabricated buildings and counselling services, and the conversion of Lindens$ into real-world currency.

The initial cost of a parcel of land for private users is around $1,300, plus a further $900 each year for maintenance. Educational and charitable users are offered discounted land rates. In addition, a monthly premium membership fee of around $20 provides users with Linden$1,000. Land can only be purchased by paid members. This structure allows fee-payers to develop their own virtual environments according to their preference, imagination and technical ability.

3dves have been used to develop simulations of real-world behaviours useful in understanding crime prevention and citizenship issues (Hall et al. 2006). However, the free-market economic structure and real-world value of virtual currency blurs the boundaries between the virtual and the real.

For example, in 2007, it was estimated that up to US$75,000 was lost when the Ginko Bank in *Second Life* collapsed after offering investors 40 percent interest per annum on their Linden$ investments (Semuels 2008). This Ponzi scheme was able to flourish in the absence of any real-world regulatory scrutiny. It is therefore possible that 3dves can provide a lucrative global environment for financial scams devoid of any external regulatory oversight.

'Inter-reality' and immersion

The convergence of technical functions promotes two forms of inter-reality in 3dves. The first involves the creation of realistic 3D environments for users to navigate. The second relates to the functionality of the 'avatar', which is the medium through which users engage with the 3dve platform and other users.

Paid members or site developers create fantasy worlds or replicas of real-world environments by uploading jpeg images into the central data repository and manipulating these files to create a 3D landscape. Only fully-paid members who own an Island can construct an environment in this way.

An 'avatar' is a human-like representation of its user, which moves through the digital world by walking, flying, or 'teleporting' to new locations. The user controls avatar movements and can communicate with other avatars (users) in real time through speech, text or simulated gestures. Studies indicate that users place more trust in avatars with human characteristics and prefer to develop avatars that reflect their own gender and racial profiles (Nowak & Rauh 2005). However, with a few simple commands, users can easily alter their avatar's physical appearance, switch gender or adopt any number of fictitious or androgynous characteristics.

These immersive and synchronous elements of 3dves alter conventional notions of cyber-harm by converging text, audio and video communication methods. Therefore, offensive conduct can encompass interaction through speech, gestures, or simulated behaviours including sexual acts, assaults, gunshots and even terrorist attacks.

The reach of real-world law

The question of whether real-world notions of interpersonal harm apply to virtual assault or sexual assault is unresolved. This complicates the question of regulation within virtual worlds. Rather than developing a new realm of 'fantasy law' neatly delineated, administered and enforced solely within 3dve domains (Brenner 2008), it appears that various formal, informal and preventative social control measures will invariably co-exist to cater for the specific technical capacities of 3dves and the needs of individual users and user groups (Wall & Williams 2007).

A virtual rape?

In May 2007, a female user of *Second Life* informed Belgian police that her avatar had been raped. Reports suggested:

> ...the Brussels Court will be working together with the Federal Computer Crime Unit to 'patrol in Second Life'... There are no details at this time about what actually occurred…or under what laws these virtual actions would be prosecuted, however…'the public prosecutor was alarmed,' which may hint at how seriously this case is being taken (Weber 2007).

A person controlling an avatar that is unexpectedly raped or assaulted might experience the physical reaction of 'freezing', or the associated shock, distrust and loss of confidence in using 3dves. While civil redress for psychological harm is conceivable, the 'disembodied' character of such an incident would invariably bar liability for any crime against the person (MacKinnon 1997).

However, Australian federal criminal law imposes a maximum penalty of three years imprisonment for using an internet carriage service to ‘menace, harass or cause offence’ to another user (*Criminal Code 1995* s. 474.17). Further, US and Australian laws ban simulated or actual depictions of child abuse and pornography (Rogers 2009). Therefore, any representations of child avatars involved in virtual sexual activity, torture or physical abuse are prohibited, regardless of whether the real-world user is an adult or child (*Criminal Code 1995* Part 10.6 Division 474). Liability is imposed where a reasonable person would consider the alleged behaviour to be offensive, which could extend to any ‘socially questionable content’ (Gray & Nikolakos 2007: 105) such as depictions of drug use, sexual violence, strong language or blood and gore.

Decentralised governance

In response to the Ginko Bank incident, Linden Lab declared it unlawful for any individual or collective to offer interest or direct returns on investments ‘without proof of an applicable government registration statement or financial institution charter’ (Linden Lab 2008). In-world gambling and the use of avatars depicting child characters are also expressly banned in Second Life. However, it is rare for 3dve platform administrators to be proactive in matters of in-world regulation and governance. Indeed, the most effective in-world governance methods appear to involve ‘proximal’ techniques, such as in-group reputation or shame-management strategies, rather than ‘distal’ or external policing and criminal justice interventions (Wall & Williams 2007). The burdens of maintaining good order and resolving disputes in the numerous sites within any global multi-user 3dve platform makes stringent enforcement or dispute resolution processes impractical and unlikely.

A decentralised model of governance, where formal law plays a limited role in maintaining order, is common to most 3dves, especially where there are rules to facilitate game-related objectives. Nevertheless, all 3dve are subject to a range of informal behavioural norms and semi-formal rules with the capacity to influence the behaviour of regular users or occasional visitors. Activity within 3dves must also conform to conventional legal requirements in the host jurisdiction, although this is complicated by the lack of international harmonisation of cybercrime laws (Smith, Grabosky & Urbas 2004).

Terms of service

All 3dve users must agree to the platform’s Terms of Service (ToS) or an End User Licence Agreement (EULA) when registering an account. If the user chooses not to agree, regardless of whether or not they have read the specific terms clause-by-clause, the program will not install into the host computer.

The unilateral nature of these standardised contracts gives rise to some concern over their enforceability and the potential for the terms to be unconscionable where they restrict the right to appeal decisions of 3dve site administrators (Duranske 2008). However, these agreements are one way of ensuring users are aware that their in-world conduct can be scrutinised and subject to formal disciplinary action.

The ToS for *Second Life* include advice on how to establish an account, intellectual property rights for content developed within the platform and disclaimers absolving Linden Lab from responsibility for content developed within the platform. The ToS also contain a list of standards applicable to all *Second Life* users.

Linden Lab retains the right to suspend or terminate an account in the event of a reported breach. The community standards prohibit:

- transmitting content violating the contractual or fiduciary rights of a third party, or any law or regulation;
- impersonating or misrepresenting your affiliation with a person or entity without their consent;
- attempting to access another’s account;
- transmitting content that Linden Lab considers ‘harmful, threatening, abusive, harassing, causes tort, defamatory, vulgar, obscene, libellous, invasive of another’s privacy, hateful, or racially, ethnically or otherwise objectionable’;
- interfering with the service, servers or networks connected to the platform;
- transmitting unsolicited or unauthorised junk mail, spam, chain letters or pyramid schemes; and
- stalking, abusing or attempting to abuse or harass other users (Linden Lab 2009b: np).

A weekly Incident Report documents any action taken to enforce the terms of service, usually after a complaint from an aggrieved user (Linden Lab 2009c). Each report lists the date, nature and location of the breach, as well as the penalty imposed, which usually consists of an official warning or account suspension for one, three or seven days. Breaches and penalties listed during a two day period in May 2009 included:

- *warnings*—unauthorised gambling, harassment (land cutting), sexual harassment, assault in a safe area, verbal abuse, indecency (displaying mature content in a restricted area), disturbing the peace through unsolicited chain letters, pyramid schemes and using harmful scripted objects;
- *one day suspensions*—disturbing the peace, abuse of sandbox resources, acts of indecency (unspecified);
- *three day suspensions*—disturbing the peace (unsolicited scripting), wagering;
- *seven day suspensions*—chain letters or pyramid schemes, harassment, violence, offensive behaviour in kids-only area.

This fairly vague ‘naming and shaming’ measure demonstrates that most actionable in-world behaviours receive fairly innocuous penalties. This justifies further research on the frequency and impact of these behaviours and complainant satisfaction with current disciplinary procedures.

Site specific governance

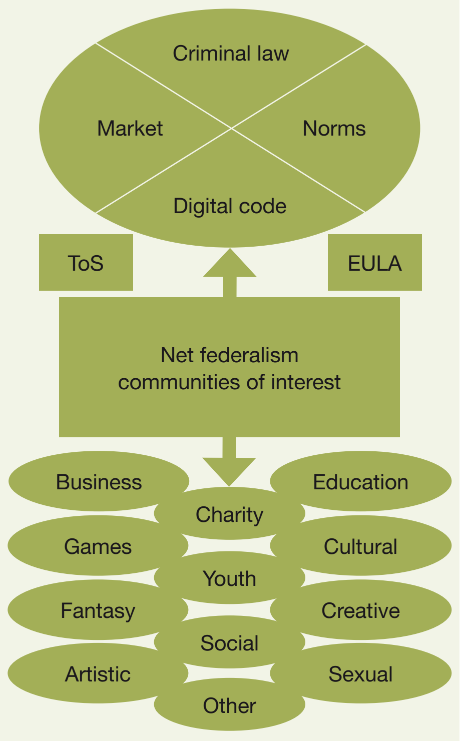
User-communities can invoke their own environment or task-specific regulatory procedures. These could incorporate any combination of market forces, digital coding, informal behavioural norms or even the establishment of site-specific policing, security and vigilante services (Wall & Williams 2007).

Net federalism

Johnson and Post (1996) used net-federalism to describe the decentralised regulatory nature of the internet. Figure 1 indicates this model can be easily adapted to explain regulatory approaches in 3dves.

Under the net-federalism model, layers of site-specific governance are developed by user communities within the 3dve platform. These are overlaid by the platform's ToS and EULAs which, in turn, co-exist with four generic forms of regulatory control to promote good conduct and site security: formal law, market forces, informal norms and digital code (Lessig 1999).

Figure 1 Net federalism and bubbles of governance in 3dves



Recent law enforcement literature indicates decentralised policing and security arrangements exist in all realms of contemporary social life. This tends to occur when conventional forms of centralised policing no longer meet the crime prevention needs of diverse communities (Shearing & Wood 2003), or where 'opportunistic' forms of third-party policing evolve to support specific interests of the state or concerned social groups (Mazerolle & Ransley 2006).

The sheer technical sophistication and variety of digital coding mechanisms and site-specific conduct norms to identify and prevent harmful activity also ensure considerable levels of 'responsibilisation' are actively promoted by the very structure of 3dve platforms (O'Malley & Palmer 1996). This means individual users or user-groups do not require extensive scrutiny or intervention by formal justice agencies or site administrators in response to the majority of 3dve harms. Provided they have the technical knowledge, user groups are arguably best situated to develop viable forms of digital coding or site-specific norms to prevent harm to digital infrastructure or other users (Wall & Williams 2007).

A typology of 3dve harm

In a decentralised and highly technical environment with high levels of user 'responsibilisation' for harm identification, prevention and the development of appropriate norms of good conduct, there is considerable uncertainty surrounding role of the criminal law in these multi-user platforms. This uncertainty is compounded by the wide range of regulatory choices available to users, confusion over the real-world implications of much of the behaviour within 3dves, the transnational appeal and jurisdictional uncertainties associated with these emerging media and the broader lack of empirical research documenting how 3dve users perceive issues relating to harm, risk, safety and governance.

The body of knowledge on each of these issues is so recent that it is premature to speculate on the ideal role of the criminal law in this field. Nevertheless, a basic typology of harms associated with 3dve use can help to clarify the various regulatory and harm-prevention strategies available to individuals, user communities and formal justice agencies.

Table 1 outlines a graded series of harms associated with 3dve use, ranging from behaviours with purely in-world implications considered too trivial to warrant formal action, to those with clearly actionable consequences under the criminal law. Within these extremes, a grey area of inter-real harms bridges the virtual and the real. Inter-real harms differ from conventional cybercrimes due to the peculiarly immersive character of 3dve technologies. How 3dve users view the severity of these harms is the most appropriate measure of the ideal regulatory approach in any given case.

Harms mediated by the technical or coding mechanisms facilitated by the platform should remain subject to current disciplinary and complaints processes established by platform administrators or under ToS agreements. For example, while activities such as digital cloning might generate fears that 3dves facilitate widespread and persistent identity thefts, systematic frauds, obscene behaviour or predatory real-world conduct (Wall 2008; Yar 2008), these nuisances are best prevented through rigorous internal digital coding modifications or informal policing, enforcement and dispute resolution methods (Wall & Williams 2007).

Table 1 A basic typology of 3dve harms

Types of harm	Conduct	Proposed outcome
Purely in-world harm	Cloning, theft, appropriation or damage to digital property of limited value or which can be easily replaced, breach of gaming rules (cheating), innocuous harassment, obscenity (flying genitalia, bots)	Internal regulation by user groups (including eviction), ToS, EULAs or formal discipline, methods of coding to prevent harm developed by platform managers
Inter-real harm	Conduct affecting avatars or property with real world physical or economic consequences: includes virtual rape, assault, sexual harassment, fraud and deception, destruction of property, abusive or threatening speech	Real-world impact must be measurable and substantial to justify formal intervention beyond the ToS, EULA and site management complaint processes
Criminal harm	Conspiracies or threats to engage in crime against the person, property, the state, communication networks or children: includes stalking, privacy, piracy and copyright violations, money laundering, disabling or tampering with 3dve platforms	Conventional criminal laws subject to jurisdictional issues and the severity or prevalence of the conduct. Internet Service Providers or platform managers to provide evidence of real-world offending

The rape of an avatar may produce some real-world physical discomfort or shock among unsuspecting or novice users (Boellstorff 2008: 189). This could be prevented through modifying simulation codes, in- or real-world counselling to deal with psychological or emotional harms or improved education about recognised risks for new 3dve users. Formal criminal intervention would only have a place if an appreciable and measurable effect on the real-world victim could be established, or if the violation clearly falls under the established criminal provisions targeting harmful online conduct (*Criminal Code 1995* Part 10.6).

Similarly, most cases of financial deception or the purchase of faulty virtual goods in 3dves will involve a minor in-world financial penalty in the order of Linden$10. Market force and greater education for vulnerable users will play a more useful harm-prevention role than the enforcement of ToS agreements or any formal legal provisions.

In contrast, systematic and organised scams aimed at using 3dves as a means of making illicit profits or for laundering real- and virtual-world money clearly have coverage under existing criminal laws. Here, the major complexity lies in assessing the scale of harm to justify a formal criminal investigation. In such cases, Internet Service Providers and platform administrators would provide crucial support to investigators aiming to establish a successful prosecution satisfying the criminal burden of proof.

Research directions

The various strands associated with harm, safety, immersion and regulation in 3dves greatly extend our conventional understanding of cybercrime. Three pertinent issues should underscore future research in this field.

The first involves enhancing our understanding of the nature of harm within multi-user 3dve platforms. Our preliminary typology and the work of ENISA (2008) provide useful starting points. ENISA's detailed report recommended the development of industry-wide standards to prevent intellectual property violations, spamming, poor user authentication procedures, automated attacks and in-world harassment, along with greater legal clarity of each of these issues.

Future research should also assess perceptions of harm, risk and appropriate educational and prevention strategies amongst 3dve users. This is crucial, given most calls for increased regulation of new technologies are made by those with little direct experience or understanding of how they are used or how they might cause harm (Wall 2008; Yar 2008).

Second, the Internet Safety Technical Task Force (2008) at Harvard University advocates ongoing collaborative research to protect children through enhanced privacy and security mechanisms. As with any internet platform, children and parents require systematic education on how to avoid clearly predatory behaviours by those who intentionally prey on or misrepresent their identities to lure or groom children into illegal and harmful real-world activities.

The Task Force also suggested:

> Members of the Internet community should continue to work with child safety experts, technologists, public policy advocates, social services and law enforcement to:
>
> - develop and incorporate a range of technologies as part of their strategy to protect minors from harm online;
> - set standards for using technologies and sharing data;
> - identify and promote best practices on implementing technologies as they emerge and as online safety issues evolve; and
> - put structures in place to measure effectiveness (Internet Safety Technical Taskforce 2008: 6).

These principles apply to other forms of harm that might have substantive financial or physical effects on adult users, regardless of their level of 3dve expertise.

Finally, the inherently qualitative nature of current research in 3dve and Web 2.0 environments raises several challenging ethical questions. While research 'stings' supported by police agencies provide valuable insights into how unlawful encounters with children are solicited (Jayawardena & Broadhurst 2007), problems of informed consent and potential entrapment abound, and are magnified by the anonymity and pseudonymity of 3dve users. More critical discussion of these ethical imperatives (Williams 2007) is clearly warranted.

Clearly, Australian 3dve users require more knowledge to identify, manage and prevent harm. Developing a systematic approach to harmonise current knowledge on these emerging issues is perhaps the greatest research priority.

References

All URLs correct as at 25 January 2010

Abrahams N 2007. Media laws for virtual worlds. *University of New South Wales Law Journal* 30(1): 295–306

Blizzard 2008. *World of Warcraft® subscriber base reaches 11.5 million worldwide*. http://investor.activision.com/releasedetail.cfm?releaseid=355698

Boellstorff T 2008. *Coming of age in Second Life: An anthropologist explores the virtually human*. Princeton: Princeton University Press

Brenner SW 2008. Fantasy crime: The role of criminal law in virtual worlds. *Vanderbilt Journal of Entertainment and Technology Law* 11(1): 1–97

Coates J, Suzor N & Fitzgerald A 2007. *Legal aspects of web 2.0 activities: Management of legal risk associated with the use of YouTube, MySpace and Second Life*. Brisbane: ARC Centre of Excellence for Creative Industries and Innovation and Queensland University of Technology

de Zwart M 2009. The dark side of online games: Fraud, theft and privacy invasion. *Internet Law Bulletin* 11(9): 147–151

Dibble J 1993. A rape in cyberspace. *Village Voice* 38(51): 36–42

Dr Ian Warren is a Senior Lecturer in Criminology at Deakin University, Waurn Ponds, Victoria.

Dr Darren Palmer is an Associate Professor in Criminology at Deakin University, Waurn Ponds, Victoria.

General editor, *Trends & issues in crime and criminal justice* series: Dr Adam M Tomison, Director, Australian Institute of Criminology

Note: *Trends & issues in crime and criminal justice* papers are peer reviewed

For a complete list and the full text of the papers in the *Trends & issues in crime and criminal justice* series, visit the AIC website at: http://www.aic.gov.au

ISSN 0817-8542 (Print)
1836-2206 (Online)

GPO Box 2944
Canberra ACT 2601, Australia
Tel: 02 6260 9200
Fax: 02 6260 9299

Disclaimer: This research paper does not necessarily reflect the policy position of the Australian Government

Duranske BT 2008. *Virtual law: Navigating the legal landscape of virtual worlds*. Chicago: American Bar Association

European Network and Information Security Agency (ENISA) 2008 *Virtual worlds, real money: Security and privacy in massively-multiplayer online games and social and corporate virtual worlds*. Position paper. Heraklion: ENISA. www.ifap.ru/library/book388.pdf

Hall L, Padmore, K, Hodge M & Oatley G 2006. Designing a virtual learning environment to support the study of crime and its prevention for teenagers. *Lecture notes in computer science* (3942): 213–222. http://www.springerlink.com/content/mh2j387p53188848/

Gray GC & Nikolakos T 2007. The self-regulation of virtual reality: Issues of voluntary compliance and enforcement in the video game industry. *Canadian Journal of Law and Society* 22(1) 93–108

Jayawardena K & Broadhurst R 2007. Online child sex solicitation: Exploring the feasibility of a research 'sting'. *International Journal of Cyber Criminology* 1(2): 228–248

Johnson DR & Post D 1996. Law and borders—The rise of law in cyberspace. *Stanford Law Review* 48(5): 1367–1402

Internet Safety Technical Task Force 2008. *Enhancing child safety and online technologies: Final report of the internet safety technical taskforce*. Cambridge (MA): Berkman Center for Internet and Society (Harvard University). http://cyber.law.harvard.edu/pubrelease/isttf/

Lastowka GF & Hunter D 2004. Virtual crimes. *New York Law School Law Review* 49(1): 293–316

Lessig L 1999. *Code and other laws of cyberspace*. New York: Basic Books

Linden Lab 2009a. *Economic statistics (raw data files)*. http://secondlife.com/statistics/economy-data.php

Linden Lab 2009b. *Terms of service*. http://secondlife.com/corporate/tos.php

Linden Lab 2009c. *Community: Incident report*. http://secondlife.com/support/incidentreport.php

Linden Lab 2008. *New policy regarding in world banks*. https://blogs.secondlife.com/community/features/blog/2008/01/08/new-policy-regarding-in-world-banks

MacKinnon R 1997. 'Virtual rape'. *Journal of Computer-mediated Communication* 2(4). http://jcmc.indiana.edu/vol2/issue4/mackinnon.html

Mazerolle L & Ransley J 2006. *Third party policing*. Cambridge: Cambridge University Press

Nowak KL & Rauh C 2005. The influence of the avatar online perceptions of anthropomorphism, androgyny, credibility, homophily, and attraction. *Journal of Computer-mediated Communication* 11(1): 153–178. http://jcmc.indiana.edu/vol11/issue1/nowak.html

O'Malley P & Palmer D 1996. Post-Keynesian policing. *Economy and Society* 25(2): 137–155

Rogers A 2009. Protecting children on the internet: Mission impossible? *Baylor Law Review* 61(2): 323–356

Semuels A 2008. Virtual bank's Second Life scheme raises real concerns. *Los Angeles Times* (Business). http://articles.latimes.com/2008/jan/22/business/fi-secondlife22

Shearing C & Wood J 2003. Nodal governance, democracy and the new 'denizens'. *Journal of Law and Society* 30(3): 400–419

Smith R, Grabosky P & Urbas G 2004. *Cyber criminals on trial*. Cambridge: Cambridge University Press

Wall DS 2008. Cybercrime and the culture of fear: Social science fiction(s) and the production of knowledge about cybercrime. *Information, Communication & Society* 11(6): 861–884

Wall DS & Williams M 2007. Policing diversity in the digital age: Maintaining order in virtual communities. *Criminology and Criminal Justice* 7(4): 391–415

Weber A 2007. *Belgian police patrols Second Life to prevent rape*. http://www.secondlifeinsider.com/2007/04/21/belgian-police-patrols-second-life-to-prevent-rape/

Williams M 2006. *Virtually criminal: Crime, deviance and regulation online*. New York: Routledge

Williams M 2007. Avatar watching: Participant observation in graphical online environments. *Qualitative Research* 7(1): 5–24

Yar M 2008. The rhetorics and myths of anti-piracy campaigns: Criminalization, moral pedagogy and capitalist property relations in the classroom. *New Media and Society* 10(4): 605–623