Article

CCJ

Criminology & Criminal Justice
0(0) 1–17

DOI: 10.1177/1748895811432957
crj.sagepub.com
SAGE

E-safety education: Young people, surveillance and responsibility

David Barnard-Wills
Cranfield University, UK

Abstract

This article presents the findings of an analysis of 'e-safety' education material currently made available to UK schools, and currently being delivered to children and young people between the ages of five and 18. E-safety refers to the way that young people are taught about risks online, how they can protect themselves, and to whom they should report worrying activity. The article is grounded in a political understanding of education as a political strategy, and one that is conducted by multiple actors, including policing agencies. The article therefore relates e-safety education to a broader politics of surveillance, crime prevention and governmental rationalities and techniques. Formal education does not determine, but likely influences the perceptions of young people towards the digitally mediated environment – including roles of authority, appropriate behavioural norms and risk perception (currently dominated by the threat of child sexual abuse). The most commonly used and disseminated e-safety education material is that produced by the Child Exploitation and Online Protection Centre. This article examines the role of a policing agency in delivering education, one that also functions as an agent of digitally mediated surveillance in its law enforcement functions. Education is an explicit strategy of political actors involved in the politics of digitally mediated surveillance.

Keywords

education, internet, policing, privacy, surveillance

Introduction

This article presents findings of an analysis of 'e-safety' education material currently available to UK schools, and delivered to children and young people between the ages of

Corresponding author:
David Barnard-Wills, Department of Informatics and Systems Engineering, Cranfield University, Shrivenham, Swindon, SN6 8LA, UK
Email: d.barnardwills@cranfield.ac.uk

five and 18. E-safety refers to the way young people are taught about risks online, how they can protect themselves and to whom they should report worrying activity. Education is understood as one of a range of explicit strategies enacted by actors in the politics of digitally mediated surveillance. The article therefore relates e-safety education to a broader politics of surveillance, crime prevention and governmental rationalities and techniques. The main focus of the article is on the role of a particular policing agency in delivering online safety education. This organization, the Child Exploitation and Online Protection Centre (CEOP), is also an agent of digitally mediated surveillance in its law enforcement functions. It is hoped that an understanding of the role of the police in technology education will make a contribution to criminological accounts of the police as knowledge-actors. Formed in 2006, CEOP is a cross-agency department of the Serious Organized Crime Agency (SOCA). CEOP combines police officers with staff seconded from charities such as the NSPCC, and support in kind from a range of strategic partners that includes Visa Europe and Microsoft. This makes CEOP a particular example of networked and pluralistic policing with respect to online environments (Johnston and Sheering, 2003; Loader, 2000; Wall, 2010a).

The discourse of e-safety education provides a particular representation of the online environment and information technology. This prioritizes certain threats and actors over others, and presents a very minimal account of privacy as protecting oneself from sexual predators. The debate and the educational material available are currently dominated by the threat of child sexual abuse. It is harm- and loss-based, and risks missing opportunities and limiting the capacity for structural change.

Children are a population who are constructed as both potential victims and potential offenders in online settings. They are at risk from exposure to inappropriate media and from hostile actors. However they seek to circumvent restrictions on their behaviour, and can be responsible for harmful behaviour to each other in the form of cyber-bullying. This renders them likely to be also construed as legitimate targets for surveillance and intervention by a variety of adult actors who prioritize certain educational responses to certain narrowly perceived threats. Young people are a population whose activities must be known by adults in order to protect them, but also because the population contains potential offenders – 'cyber-bullies'. At the same time, the naive or intentional visibility of children is seen as a significant source of risk. This occurs in an increasingly surveilled educational environment as schools become sites of technologically mediated surveillance (Hope, 2005; Monahan and Torres, 2010; Steeves and Jones, 2010; Taylor, 2010). This should all be considered against a background public understanding of the internet as criminogenic (Wall, 2010b). The focus of this article is primarily the role that the issue of predation, rather than bullying, plays in this discourse.

This article examines in turn the policy background for e-safety, issues of surveillance and privacy, e-safety as reassurance policing and how this education material functions to attribute responsibility to various actors and provide accounts of appropriate behaviour. This is contextualized as part of a politics of knowledge and conduct, and the article concludes with a discussion of ways to expand e-safety education and reduce its constitutive distortions. How young people are taught to stay safe online and understand a range of online threats, actors, technologies and concepts may affect how they relate to the online environment both now and in their future lives. This impacts upon

online privacy, consent and digitally mediated surveillance. Formal education likely influences the perceptions of young people towards the politics of the digitally mediated environment – including roles of authority, appropriate behavioural norms and risk perception. Education, alongside persuasion and seduction are key modalities of non-coercive government (Miller and Rose, 2008: 209). Subjects of rule become active in their own government, while institutions seek to create individuals capable of governing themselves, capable of making decisions about their self-conduct in reference to particular norms, vocabularies and warnings (Miller and Rose, 2008: 205). The police role in education might be thought of in terms of governing through crime (Simon, 2007). Online crime, particularly sexual offences against children, becomes the dominant modality for technology education, legitimating the role of a police agency intervening in education, and reframing education through forms of knowledge associated with crime control. This is received by educators and parents, who it purports to help perform socially lauded roles. Although he does not engage with e-safety, the family is identified by Simon as a particularly strong anchor for governing through crime. The predominant role of the young person is as potential victim, who is to be equipped and guided to security-consciousness. This move seems particularly powerful in moments of novelty where no existing actor has a history of securing the online environment.

Methodology

This study uses a discourse analysis methodology drawing upon the work of Fairclough (2003) and Glynos and Howarth (2007). Knowledge of the social world is constructed through language, and language in political and social texts reflects both explicit choices and deeper structures not easily accessible to those entangled in them. This methodology focuses upon the way that the social world of online safety education and young people's use of online technology is constructed and represented in texts. 'Texts' encompasses any 'readable' material and can include video and audio. This analysis therefore incorporates elements of a visual analysis where appropriate, and acknowledges the power of images and their potential emotional effect. Such an approach can be difficult in 'disciplines of words' (Banks, 2005: 3) and requires readings of both internal and external narratives. Texts are products of human action and are entangled in social relations. Multiple readings of texts are always possible, and the task is not to produce a single authoritative reading, but rather to construct a plausible reading based upon the text and the wider social context, woven together with appropriate theoretical frameworks. A discourse analysis approach to education material attempts to identify both the dominant encodings and therefore the intended message, including the representation of the social world that surrounds and permeates that message (Hall, 2006). It cannot determine all possible decoding by audiences, intended or otherwise. An examination of reception is left to further qualitative research into the experience of using this education material.

The textual sample was constructed through a search of the available e-safety education material and interviews with e-safety practitioners. These interviews identified the Child Exploitation and Online Protection Centre (CEOP) as a primary source. CEOP has trained over 11,000 child protection professionals since 2006, and CEOP education material (primarily the flagship ThinkUKnow campaign) has been delivered to nearly six

million children in the UK. This makes CEOP a very significant actor in the e-safety education field. Other education material is available (for example from Childnet International or a specialist website from the Information Commissioner) but, although mentioned for comparative purposes, this is not the focus here.[1] With permission from CEOP, all available material was downloaded in May 2010 and formed the population of texts. The 26 documents in total included a combination of short films, presentation scripts and slides, marketing documents, leaflets, fact sheets for parents and guidance for teachers. Some of these short films are now available online, but at the time required authorization to access. The core of CEOP's strategy is a set of high quality media products making use of varied soundtracks and special effects. These short films are often disturbing and shocking. They involve threatening characters with emotional framing. Many make use of a reverse filming, tracking back through time from a moment of abuse to a moment of decision.

Background

Holloway and Valentine (2003) argue that current UK public policy on children's ICT use contains paradoxical ideas about childhood and technology. They identify 'boosters' who celebrate children's command of technology and 'debunkers' who feel that technology is putting young people's emotional well-being at risk. They associate these perspectives with 'Apollonian and Dionysian' narratives of childhood and development (Holloway and Valentine, 2003: 18). Both rest upon an essentialized narrative of childhood which collapses the diversity of identity and experience and assumes diverse children have the same capacity for using technology, with a techno-determinist perspective on the effects of technology. They identify great variety in the exposure and interaction of young people with information technology across school and family life. This would suggest caution towards any account that assumes young people to be either 'digital natives' perfectly at home in a technological environment, or conversely assumes total ignorance. The *UK Children Go Online* report on nine to 19-year-olds' use of the internet, suggested that while home access is growing, and school access is nearly universal in the UK, there is a continuum in quality of use, and that many young people are not yet taking up the full potential of the internet (Livingstone and Bober, 2005: 2). Although he does not engage with online crime, Simon (2007: 209) argues that governing through crime has resulted in a conflation of virtually all vulnerabilities of children into some form of crime while Yar (2010: 151) states that concerns about online victimization are most pronounced when they involve the sexual victimization of children.

This is a changing and novel environment and many educational organizations feel they are in the middle of a learning process; coming to terms with technological change and its social elements. Hope (2005: 365) identified three types of risk from the internet as perceived by schools and policy makers: risks to children, staff and to educational institutions themselves. Sharples et al. (2009: 70) argue that a central dilemma that schools must currently address is how they can support children to engage in productive and creative social learning online while protecting them from undue harm. They also suggest that this dilemma has no obvious answer given that both learning and social

interaction necessitate an element of risk. The roots of this dilemma are for them, rooted in a more fundamental ideological division over the role of adults in child education and the proper balance between freedom to explore and protection from harm. Adolescents in particular are in liminal positions in regard to the adoption of adult risk, often mediated by institutional contexts (Miller, 2005). Sharples et al.'s (2009: 82) conclusion is that schools are currently caught between the desire (although perhaps not the capacity) to encourage creative use of web technology and parental fears about internet abuse. The *Safer Children in a Digital World* report (Byron, 2008) is also criticized for a focus upon risk over benefits from online technology (Sharples et al., 2009: 71).

However, this situation is not binary, and there are other actors intervening in this relationship. Much of the e-safety education material available to teachers is externally produced, and in many cases is already dominated by a risk averse, police-driven perspective.

Surveillance and Privacy

While surveillance pervades this field, there are three main analytic perspectives on surveillance that arise out of the e-safety material. These are the police as a surveillance agent, surveillance by predatory criminals and privacy.

Police as surveillance agents

Ericson and Haggerty (1997) provide an account of policing as increasingly an information hungry activity, and also as a risk-communication system. In line with this, CEOP performs a number of intelligence functions that can be understood as surveillance. This includes their specialist Behavioural Analysis Unit, victim identification and Most Wanted initiative. Their remit includes tracking and bringing offenders to account (www.ceop.police.uk). Surveillance of sex offenders is networked, and includes information sharing with organizations such as the Virtual Global Taskforce, Internet Watch Foundation, Internet Service Providers and credit card companies. In CEOP education material, this surveillance role is not significantly mentioned. It is however apparent in their communication, marketing documents and website aimed at adults and organizations. To young people, the police are represented in CEOP materials as somebody who can be told about concerns, and somebody who will take action.

Predators

The primary subject position that emerges from the threatening, anonymous online environment represented in e-safety texts is the paedophile, online predator or sexual abuser. This is the dominant concept in the education material, and one that drives and structures it. It is arguably a nodal point for this discourse (Laclau and Mouffe, 2001). An example from the ThinkUKnow presentation script suggests that any adult could be a paedophile, given the difficulty of identifying an adult as a person with malicious intent:

> Look at the picture, which one of these people do you think could be a paedophile? The point you are making is that a paedophile could be anybody (male, female, old, young, someone you know or a stranger, etc). A paedophile could be any of those people, you can't be sure what they look like, which is why it's so important to always protect yourself, no matter who you think you're talking to.

In contrast to this statement, in the CEOP videos child abusers are almost universally white males, with ages ranging from 20–40. This produces a tension between technical ambiguity and a distinct stereotype of the sexual abuser. Paedophiles are also constructed in CEOP discourse as being capable agents of surveillance directed at children and young people, capable deceivers and manipulators and as technologically literate. Information for teachers states: 'Paedophiles are very clever at piecing together small bits information to track children down in the real world' (CEOP, n.d.: 3). Bell (2002) examines the way that paedophiles are problematized and constructed as a particular 'type'. This occurs across multiple sites as part of the contemporary governance of child sex abuse. The paedophile is constructed as unseen and therefore potentially existing everywhere. They are also placed on the other side of healthy, rational, normal life. Their behaviour is constructed as so abnormal that they are functionally unknowable. They cannot be normalized to community norms and must therefore be managed as a high-risk category (Simon, 1998).

Grooming is a process of socialization drawn from the sex offender literature, and the concept has now spread into detection and prevention initiatives (Davidson and Martellozzo, 2008). The Sexual Offences Act 2003 makes internet grooming an offence if it can be demonstrated that following grooming behaviour, a person meets with (or travels to meet with a victim) (Edgar-Nevill, 2008). It is represented as a deceitful, intentional act of surveillance and emotional manipulation that exploits the anonymity, accessibility and visibility of the online environment. However, Holmes' (2009) review of existing research finds that risks from online communication for young people are small scale and often exaggerated. He critiques the grooming pathway from abusively motivated surveillance to harm, finding little research evidence for the paradigm setting case of online-initiated abduction that dominates the security imagination (Holmes, 2009: 1180). He also suggests that online predators are often not deceiving young people they are communicating with about either their age or their intentions. Holmes (2009: 1181) suggests that grooming is 'peripheral to the majority of young people's concerns, liable to affect older teens more able to cope and is related to social mediators of risk'. This is supported by Beech et al. (2008), Bryce (2010), Withers and Sheldon (2008) and Wolak et al. (2008).

Privacy online

Privacy is currently a politicized issue. Thought of as a legal right or as a protection against a particular set of information harms (Solove, 2008), privacy is related to the information norms of a particular context (Nissenbaum, 2010). Many CEOP texts in the online safety education discourse do not engage or utilize the concept of privacy. This occurs even in discussion of issues that might be thought of as privacy or privacy-related

by analysts. Safety is a much more prominent concept than privacy, and privacy is never articulated as a stand-alone value, but only as an instrumental methodology or tactic for ensuring broader personal safety. There is no discussion of privacy in the CEOP videos. A working theory of privacy can however be extrapolated from CEOP discourse on exposure and personal information. One of the problems identified by CEOP discourse is the way that young individuals can, through internet use, be exposed to a much wider world, containing more hostile actors. This expanded world is globalized – 'going online can be a world of fun, but don't forget you're talking to everyone' (CEOP, 2011). Young people may not be aware of this level of exposure, putting themselves at risk: 'Imagine if someone wanted to find you or learn stuff about you to bully you. Would the information on your profile make this pretty easy? Your personal information may be more public than you think' (ThinkUKnow leaflet). This unstated privacy theory includes an attitude towards knowledge: that certain categories of knowledge should not be known by all people; that the individual should have some choice over this; and that failure to manage this can be harmful. Privacy is most frequently explicitly mentioned in relation to privacy settings on social networking sites. Privacy settings are constructed as an important tool for protecting personal information, and setting them correctly is seen as essential, but also as achievable and relatively non-controversial (Coopamootoo and Ashenden, 2011). There is no discussion about why people might set them otherwise, or why there are variable settings at all.

Giving out personal information is constructed as dangerous because of characteristics of the online environment that relate to exposure, the ease of propagation of data and images and the existence of hostile actors with occluded or deceitful identities. Online spaces are represented as axiomatically public places. In *Jigsaw*, an adult walks into a child's bedroom and starts putting physical photos into his bag. This represents the ease with which images online can be copied.

The anonymity provided by the internet allows malicious actors to adopt false identities, or to easily lie and dissimulate. A parents' fact sheet suggests: 'Help your child to understand that some people lie online and therefore it's better to keep online mates online. They should never meet up with any strangers without an adult they trust.'

Another feature of online communication is demonstrated in *Matt Thought He Knew*. The camera moves through the computer screen to show that although the young male protagonist believed he was talking to a girl of a similar age, he is actually talking with an adult male, selecting from a range of potential photographs to use as a profile picture (CEOP, 2009b). A related dangerous behaviour is the swapping of online friends and contacts between young people, without full knowledge of who the contacts are. Privacy in CEOP material also encompasses a barrier against exposure of the individual to images and information that is upsetting or seen as potentially harmful or inappropriate for children (presumably this is sexualized content). Young people are encouraged to set up filters to prevent such exposure.

boyd and Marwick's (2011: 1) ethnographic research into young people's online privacy attitudes and behaviours raises a number of issues with implications for privacy and online safety education. They argue that young people do care about privacy during their interaction in 'networked publics'. Because they have little ability to affect technology, law or the market, young people look to control their interactions online through social

norms. Young people often reported unhappily on an absence of privacy in their lives, for example, due to parents intruding on their space, or monitoring their social network use. This suggests the private space of the bedroom in *Jigsaw* is less private than we might think. A total of 69 per cent of nine to 17-year-old regular internet users reported minding their parents restricting or monitoring the online activities, while a majority report having taken some action to hide online activity from their parents (Livingstone and Bober, 2005: 3). This conflict may reflect a perception that children do not have a right to privacy in the same way that adults do. If this is a widespread belief then it may be partly responsible for the absence of privacy within e-safety education.

Reassurance Policing and E-Safety Education

Also relevant to this discussion is the concept of 'reassurance policing'. Increased engagement and visibility of policing are seen as a key element of reassuring the public that police are committed to responding to crime and disorder (Hinds and Grabosky, 2008: 99). The National Policing Improvement Agency (NPIA) (n.d.) states that:

> Providing 'a sense of security' is a vital part of the Police force's role when it comes to reassuring the public. Making a real difference is only possible if reassurance is recognised as an integral part of the force's day-to-day business alongside priority crimes.

Furthermore NPIA associates reassurance with rapid reaction to 'signal crimes' and the visible effects of crime. Reassurance is strongly linked to visible responses to visible issues in specific localities; a methodology which might be complicated in the online environment where visibility, geographic responsibility and criminal investigations are complicated (Thomas and Loader, 2000). Victims are not always aware they are victims, or the victimized are not visible to broader populations. Engagement in e-safety activities demonstrates a police presence. A strong message of the CEOP narratives is that reporting worrying or disconcerting online activity to the police will receive a prompt and active expert response. This level of response may function to signal active police engagement. Reassurance is likely affected by broader youth attitudes towards the police, which can be more negative than those of adults, highly variable and demographically striated (Hurst and Frank, 2000).

Police representatives appear in the videos in response to alerts from young people. They are shown as taking abusers and offenders into custody, solving the worries of the protagonist. This is often accompanied with narration by the protagonist, stating that 'There is someone who can help you' or 'There is someone you can tell.' The impression is of an effective, empowered and active actor. The focus upon the institutional actors, and power attributed to them may have the result of putting individuals and especially children into a client position, with interactions constructed as occurring between individual clients and more powerful, beneficent institutions.

One area potentially analogous with e-safety education provided by policing actors may be drugs education. This has been provided by police officers and there is an existing research base (White and Pitts, 1998). The CEOP activity differs from this model in that it rarely places police officers in the classroom. Instead teachers and youth workers

are provided with training and materials by CEOP to deliver themselves. This may reduce potential antagonism or disengagement from young people with a negative attitude to the police, but may also lose some of the benefits of speaking from a position of perceived authority and experience (Hammond et al., 2008). The role of the police in producing education is somewhat masked by the presence of intermediary actors, but this also introduces the potential for resistance, alteration of message or reworking of material and its disseminators (Martin et al., 2009).

Responsibility and Behaviour

E-safety education can be understood fairly unproblematically as 'responsibilization' (O'Malley, 1992). Bell (1993) examines governmental practices involved in childcare, locating them within broader perspectives on liberal governmentality (Dean, 2010; Miller and Rose, 2008). The governance of children is conducted at a distance through the family, formalizing both 'parental responsibility' and a stand-off role for the State. While the domestic domain is ostensibly private, a range of governmental programmes provide (technically voluntary) tasks for parents regarding their children. Parents are invited to engage in risk assessment, helped by experts, with the Government providing basic security (Bell, 2002: 6–7). E-safety information is also cascaded to parents through their children's schools. Through e-safety initiatives, both children and their parents or guardians are made responsible. Both are constructed as able to take steps to increase their own safety. Adults are however granted a more significant role, which relates to the traditional, non-digital practices of interpersonal surveillance characteristic of parenting. Berson and Berson (2003: 114) argue that:

> The active involvement of caring adults is necessary to prepare them for safe navigation. Direct observation of children online in a public space with periodic interaction and ongoing discussions of their web experiences are the foundations of internet safety procedures.

The fundamental message running through CEOP e-safety discourse is that young people have the responsibility to report anything potentially illegal they encounter online to authority figures, in particular to CEOP themselves. This is the core message of the CEOP videos, where negative impacts on a young person from online sexual predation are mitigated or entirely prevented when the young person remembers the ThinkUKnow website or the CEOP reporting button and uses it. This results in the arrival of uniformed police officers. This moment is often the dramatic tipping point of the narrative, accompanied by more uplifting music or brighter imagery as the young person continues a happy and normal life. CEOP also affirms that such reports will be taken seriously and treated in a professional manner. Reporting something suspicious to the authorities is constructed by CEOP as helping to make (or sometimes keep) the internet safe, and therefore involving a responsibility to other children.

The second form of responsibility is the responsibility placed upon children and young people to play an active part in protecting themselves from online threats and in managing their own exposure to risk. Children between five and seven are encouraged to become a self 'protector' like the cartoon superhero 'Sid' (CEOP, 2011), while older

children are encouraged to take on individual responsibility for managing risk, and avoid doing risky things online. This includes being aware and developing knowledge. In one video, a sexual abuser gives a sarcastically delivered set of 'rules', knowledge of which would protect a young person from him (CEOP, 2009a). Young people are also encouraged to conduct their own surveillance, gathering evidence in cases of potential abuse. Victims of cyber-bullying are encouraged to save abusive texts, emails or messages for use as evidence (CEOP ThinkUKnow script) and to take screenshots of sites and save conversations (CEOP Background Information to Online Safety).

In several of the CEOP videos, young people are represented as confident in their use of online technology, including chat, email and mobiles. Several videos show skilled competency and familiarity with the technology. However, this confidence is combined with a naivety regarding the intentions of people they communicate with, and a lack of strategies for responding to situations that make them feel uncomfortable. The message repeated across several of the ThinkUKnow videos is that young people may think they know what they are doing, but lack a wider perspective, knowledge or appropriate level of caution. In comparison to education material produced by the Information Commissioner's Office (http://www.ico.gov.uk/youth.aspx) and Childnet (http://www.childnet-int.org/), the level of responsibility placed upon the child is lower in CEOP discourse. A greater weight of responsibility is placed upon policing institutions in a responsive mode should things go wrong, and educational actors in a proactive, preventative mode.

Hinds and Grabosky (2008) examined the factors that influence people to accept more responsibility for protecting themselves from crime, building upon Garland's observations that crime control was increasingly made the responsibility of individuals as experience of crime was normalized and the State acknowledged that it could not prevent all crime. The response was to encourage individuals to change their everyday behaviour to reduce the risk of crime. Hinds and Grabosky (2008: 97) attempted to map the voluntary acceptance of crime control responsibility. Responsibilization in the e-safety context does face some resistance. Hinds and Grabosky identify a number of reasons why the message may not be accepted. These range from the theoretical/political (taxpayers believing the State should take responsibility for crime prevention) to the practical (too busy, too wedded to their current behaviour or unable to afford expensive crime prevention measures) to the perceptual (crime is perceived as a low risk) and the fatalistic (crime will happen regardless of individual action) (2008: 98).

Experts

Understanding the attribution of responsibility also necessitates incorporating the role of experts in the process. Miller and Rose (2008) identify the role of expertise in linking up deliberations in one place with actors in another (in this case moving from policy and education theory circles to multiple individual schools) and also in the possibility of aligning self-governing subjects with the objectives of political authorities. Teachers require CEOP training before they deliver CEOP material and this training contributes to the continuing development of education, policing and child protection professionals. CEOP texts devote significant space to setting out the responsibilities of teachers in

response to disclosure of private information or what to do if a young person reports abuse to them, as well as who to pass that information to. Delivering the training involves accepting responsibility for professional behaviour and agreeing to a code of conduct. Teachers are also required to present the CEOP material in an unmodified form, although this is not always adhered to in practice. Teachers interviewed had made modifications based upon their understanding of their students.

Norms of appropriate behaviour

As part of responsibilization e-safety texts provide evaluations of appropriate and dangerous behaviours for actors in this field. CEOP explicitly reflects on the modality of its ThinkuKnow material:

> ThinkUKnow has been designed to be emotionally engaging and impactful in terms of getting … key messages over to children. It is interactive and uses a number of powerful short films to educate children about the risks they may encounter when using the internet. Importantly it seeks to empower children to know how to report a problem, including abuse. (Safeguarding and Promoting the Welfare of Children and Young People through the ThinkUKnow Education Programme, Practice Guidance for Teachers)

Normal behaviour for children and young people in CEOP discourse involves an orientation towards 'normal' childhood activities, such as play, shopping or meeting friends. These feature heavily in the films, demonstrating the normal life disrupted by abuse. CEOP discourse also depicts a normal relationship between children and technology. Using computers and spending (some) time online is normal and even positively evaluated. However, this is sometimes constructed in a passive manner that presents young people as primarily consumers of media rather than as producers or creators. Young people are encouraged to 'be careful' online, act responsibly and be nice to others. In contrast to Childnet material, strategies for staying safe online are primarily framed in terms of behaviour to avoid, rather than proactive strategies to adopt. While the discourse encourages the management of risk by young people, it is somewhat opaque on how this can be enacted – there are no strategies for assessing risk beyond the relatively simply binary distinctions between trusted/non-trusted adults, and offline/online friends.

The CEOP discourse constructs two linked sets of dangerous behaviour that arise from mistaken assessment of the offline and online environments. The first set of behaviours arises from assuming that the online and offline worlds are the same, the second from assuming that they are different. CEOP discourse constructs the online environment as more dangerous than the offline environment. People on the internet lie, it is easy to be anonymous and images can be circulated more freely. Internet addiction – spending too much time online to the extent of neglecting offline life is also dangerous. There should therefore be a separation between online and offline worlds.

The second type of dangerous behaviour involves assuming that online activity exists in a vacuum unrelated to offline life. This is exemplified by posting images online that you would not want people in the offline world to see. The CEOP discourse constructs

online activities as having offline consequences. This is best represented in the *Jigsaw* video, where children are posed questions such as 'would you leave your front door open?' then shown they are doing effectively that online.

In many CEOP films an initial state of confidence is revealed as actually being a product of ignorance of the true nature of a situation or environment. Once this revelation has been made, and the true nature demonstrated, then new, more reliable knowledge can be created. CEOP texts use this pattern to represent young people's online behaviour, which is often confident, and often expressed with confidence by young people themselves. Behaviour is then represented as being based on ignorance – young people are unaware of online deception, anonymity and offline consequences. The children in *Jigsaw* look embarrassed and acknowledge the discrepancy between avowed norms and behaviour when it is revealed. This modality is intrinsic to a central message of ThinkUKnow. Films *Clare thought she knew* and *Matt thought he knew* highlight that young people may think they know what they are doing, but are mistaken, and should have greater awareness and make different choices. *Lee and Kim's Animal Adventure* reveals the danger behind seemingly friendly and safe virtual environments. The film *Consequences* uses anagnorisis in a related way. An initial assumption by the viewer that the narrator is a normal young adult/late teenager is subverted when we find out he is stalking people online. This unsympathetic narrator describes surveillance activities from his perspective. His confident assertions are shown to be false in another reversal, when his victim remembers appropriate behaviour and reports his activity to authorities. The repeated message is that she had not previously thought about online dangers and had incorrectly thought she was safe.

Young people themselves can be a source of negative online behaviour, through the activity of cyber-bullying. *Jigsaw* refers to the hurtful activities of 'those girls at school' who repost pictures from a social network page around school to cause embarrassment. In another video, several young people are interacting online and a girl becomes the victim of cyber-bullying. The bully's comments are reflected in the distortion of the victim's features. The other children are shown taking pleasure in this.

Hope (2010) argues that risk approaches often ignore reasons for young people to take what adults see as risks, and this is often also true of information security approaches to privacy. This included the emotional and seductive appeal of risk – an adrenaline rush, which might be increased by potentially being under surveillance. Risk taking can foster an identity as a knowledgeable, brave or skilled individual. Risk taking was also associated with skilled performance, demonstrated to an audience of peers (Hope, 2010: 240). In this sense, taking risks online and coping with them may be a form of edgework (Lyng, 1990, 2005), both in terms of escaping from risk-adverse culture through skilled performance, and also as part of a structure that expects risk-management rather than risk aversion. Rooney (2010: 347) argues that children need to be seen as dialogical partners in negotiating trust and risk, rather than objects of control, where all risk assessments are made for them by others. Livingstone and Brake draw a strong positive association between opportunities and risks online. Children experiencing one also experience the other. Attempting to close down and remove all risk from the online environment will likely reduce the opportunities that it can bring, in addition to being unsuccessful. Pushing too far in this direction may also risk closing off a potential domain of identity

creation for young people. Young people exhibit a strong desire to communicate and form relationships, and increasingly part of this activity will take place online, including experimentation and identity performance (Livingstone and Brake, 2010: 76).

Conclusions

There is a deep politics of knowledge, technology and surveillance operating in e-safety. This is in need of further analysis, but an important dimension is the degree of technological knowledge, capacity and mastery that is attributed to actors and subject positions, and also the degree of knowledge that they are seen as requiring. How knowledge is acquired, and the role of fear in encouraging knowledge acquisition can also be contested. The police are enmeshed in this as risk experts (Ericson and Haggerty, 1997), but also as educators and perception managers. Lack of knowledge is seen as the cause of negatively evaluated behaviour, with the assumption that an increase in knowledge will prevent or eliminate that behaviour. The rational actor of liberal governmentality requires knowledge with which to reflect upon his or her behaviour and alter it. Through this guidance and education, children are constructed as responsible managers of their risk and activity online, but only up to a point, due to a fundamental lack of technological knowledge and awareness of the online environment. Opportunity costs, such as educational disadvantage or missing out on social capital that might result from abstaining or avoiding digital communication technology are not discussed in the CEOP material. It therefore could be understood as a direct harm paradigm.

We can identify surveillance in the discourse in relation to criminal actors, the encouragement of reporting to authority and in parenting and care. The State and commercial surveillance are downplayed, and there is a near complete absence of privacy education. The material does not contain a critique of personal information processing that is legal but potentially exploitative, nor does it examine excessive desire for personal information for corporate and marketing purposes (Pridmore and Zwick, 2011). Rather, personal information is misused when it is used for criminal ends such as child abuse or cyber-bullying. None of the material provides strategies or advice on how to change the structure of the environment, beyond supporting the policing activity of authorities. Risk is either normalized or it can only be systematically reduced by authorities governing through crime. There is little room for individuals and sub-state groups to alter their technological environment in a manner more suiting to them.

If, as boyd and Marwick (2011) suggest, privacy is a boundary negotiation problem, the discussion of social boundaries is likely distorted by the invocation of the paedophile, constructed as axiomatically hostile to social norms. If however, the focus of young people is cyber-bullying and surveillance of their online presence by parents or teachers, then norms become very important. boyd and Marwick find that young people often lack the social skills to express effectively or negotiate their privacy preferences and their privacy norms. Privacy and e-safety education might therefore benefit from including attention to the development of these social skills. They are likely to be beneficial in other areas of young people's development. Being equipped to manage online interactions, and having the confidence to do so may be highly effective. Holmes (2009: 1189) recommends that young people should be given 'simple and understated guidance

on negotiating risks' while fully engaging in the benefits of ICT communication. Interventions should be focused on 'the inappropriate nature of certain relationships (adult-youth sexuality) rather than all online relationships' (2009: 1189). Several e-safety texts suggested that young people should not befriend people online that they did not know offline. A no-contact rule such as this risks rejection as implausible, reducing the benefits of diverse socialization, and marginalization of the vulnerable. Furthermore the literature on edgework suggests that this will never encompass youth attitudes to risk. Research by Mitchell et al. (2004) into 10–17-year-olds in the USA suggested that only a relatively small proportion of young people reporting unwanted sexual solicitation online found this upsetting. Younger children had a harder time dealing with solicitations, but children vary in their ability to manage their online interactions. Educational focus should be upon competent negotiation of risk as well as recognizing that inappropriate contact between adults and children also occurs offline with known (and 'trusted') adults. General internet literacy, as well as the ability to evaluate online content critically should provide many teachable moments outside the security paradigm. Berson (2003: 16) also suggests that successful educational programmes will incorporate the voices of youth in their creation, will be strength-based, rather than deficit-based and empower children to discriminate better between ambiguous events. This is the approach taken in Childnet International education material. As well as gaining a communication advantage, it is more likely to speak directly to youth concerns about their use of online spaces (cyber-bullying, managing relations and expressing privacy concerns) rather than institutional priorities of sex offenders and the policing response to them.

The current reliance upon policing and information security experts colours the norms and values embedding in e-safety education. Young people in boyd and Marwick's (2011) study often expressed a 'gains-based' attitude to sharing and interacting online, in which they looked to see what they could gain from this activity. This can be contrasted with the predominantly loss-based approach prevalent in the field of Information Security. The opposition of values might be problematic in acceptance of message, as well as in meeting the needs of the young people. Both commercial Information Security and policing have a cultural tendency to undervalue norms other than security, as well as focus upon the technologically possible in determining threats, which has led to some difficulties in communication with other parts of organizations with different goals and functions.

Assigning responsibility in child safety can have social consequences. Vigilante parent groups have constructed the State as not revealing information on the location of sexual offenders to those who need it. Surveillance of sexual criminals is conducted not just by state authorities, but also by the popular media through name-and-shame campaigns and by local actors. Bell argues that parents as vigilantes emerge in response to the contemporary requirements for parents to act as risk-assessors and to be ever vigilant. They are given a responsibility for security, but denied the full information they feel they require, and demonized by liberal voices when they take action (Bell, 2002: 4). In making parents responsible, the material assumes a level of technology capacity and willingness which may not be present in all circumstances. Other issues with attributing responsibility include making young people into surveillance agents as part of a diffuse network. The way that young people's reporting integrates into CEOP intelligence practices is currently unavailable to the public. Promoting a high security, low engagement perspective, in which any possible risk is avoided, while concerns are

elevated up to policing authorities rather than being evaluated and explored at the individual level may cause a number of issues. Young people of 18 years or more do not fall within CEOP's authority. If they have no experience of managing their own online interactions until this point, then this may leave them unprepared.

CEOP e-safety education material is well intentioned and a response to a potential harm, as well as to an apparent social demand for this material. Somewhat inevitably it serves a role of legitimating the function and stance of the organization. In this case an absence of privacy, young people as victims not agents and a focus on harms rather than benefits. It is not that CEOP should not be involved in this area but that it is important to understand these structural tendencies. This allows internal adjustments or for teachers and parents to draw upon other sources to balance or complement this approach.

Note

1. Additional analysis of this material was produced as part of this research and is available from the author.

References

Banks M (2005) *Visual Methods for Social Research*. London, Los Angeles, CA and New Delhi: SAGE.

Beech AR, Elliot IA, Birgden A and Findlater D (2008) The internet and child sexual offending: A criminological review. *Aggression and Violent Behaviour* 13: 216–228.

Bell V (1993) Governing childhood. *Economy and Society* 22(3): 390–405.

Bell V (2002) The vigilant(e) parent and the paedophile: The News of the World campaign 2000 and the contemporary governmentality of child sexual abuse. Available at: http://eprints.gold.ac.uk/80/ (accessed 16 May 2011).

Berson IR (2003) Grooming cybervictims: The psychosocial effects of online exploitation for youth. *Journal of School Violence* 2(1): 5–18.

Berson MJ and Berson IR (2003) Lessons learned about schools and their responsibility to foster safety online. *Journal of School Violence* 2(1): 105–117.

boyd d and Marwick A (2011) Social steganography: Privacy in networked publics. Paper presented at the International Communication Association, Boston, MA, 28 May. Available at: http://www.danah.org/papers/2011/Steganography-ICAVersion.pdf.

Bryce J (2010) Online sexual exploitation of children and young people. In: Jewkes Y and Yar M (eds) *Handbook of Internet Crime*. Cullompton and Portland, OR: Willan Publishing.

Byron T (2008) *Safer Children in a Digital World: The Report of the Byron Review*. London: Department for Children, Schools and Families and Department for Culture, Media and Sport.

CEOP (2009a) Consequences: Assembly for 11 16 year olds. Available at: http://www.youtube.com/watch?v=hK5OeGeudBM&feature=youtube_gdata_player (accessed 7 June 2011).

CEOP (2009b) Matt thought he knew. Available at: http://www.youtube.com/watch?v=nDBDUX7KPT0&feature=youtube_gdata_player (accessed 7 June 2011).

CEOP (2011) Safer internet day: Lee & Kim's adventure – animal magic. Available at: http://www.youtube.com/watch?v=qOHHpTbBh9A&feature=youtube_gdata_player (accessed 7 June 2011).

CEOP (n.d.) YouTube – jigsaw: Assembly for 8 10 year olds. Available at: http://www.youtube.com/watch?v=_o8auwnJtqE (accessed 7 June 2011).

Coopamootoo PL and Ashenden D (2011) Designing usable online privacy mechanisms: What can we learn from real world behaviour? In: Fisher-Hübner S, Duquenoy P, Hansen M, Leenes R and Zhang G (eds) *Privacy and Identity Management for Life*. Berlin and Heidelberg:

Springer, pp. 311–324. Available at: http://www.springerlink.com/content/m33x4q520227n345/ (accessed 8 June 2011).
Davidson JC and Martellozzo E (2008) Protecting vulnerable young people in cyberspace from sexual abuse: Raising awareness and responding globally. *Police Practice and Research: An International Journal* 9(4): 277–289.
Dean M (2010) *Governmentality: Power and Rule in Modern Society*. London and Los Angeles, CA: SAGE.
Edgar-Nevill D (2008) Internet grooming and paedophile crimes. In Bryant R (ed.) *Investigating Digital Crime*. Chichester: Wiley.
Ericson R and Haggerty K (1997) *Policing the Risk Society*. Toronto and Buffalo: University of Toronto Press.
Fairclough N (2003) *Analysing Discourse: Textual Analysis for Social Research*. London and New York: Routledge.
Glynos J and Howarth D (2007) *Logics of Critical Explanation in Social and Political Theory*. London and New York: Routledge.
Hall S (2006) Encoding/decoding. In: Hamilton P (ed.) *Visual Research Methods*. London, Los Angeles, CA and New Delhi: SAGE.
Hammond A, Sloboda Z, Tonkin P, et al. (2008) Do adolescents perceive police officers as credible instructors of substance abuse prevention programs? *Health Education Research* 23(4): 682–696.
Hinds L and Grabosky P (2008) Responsibilisation revisited: From concept to attribution in crime control. *Security Journal* 23(2): 95–113.
Holloway S and Valentine G (2003) *Cyberkids: Children in the Information Age*. London and New York: Routledge.
Holmes J (2009) Myths – and missed opportunities: Young people's not so risky use of online communication. *Information, Communication & Society* 12(8): 1174–1196.
Hope A (2005) Panopticism, play and the resistance of surveillance: Case studies of the observation of student Internet use in UK schools. *British Journal of Sociology of Education* 26(3): 359–373.
Hope A (2010) Seductions of risk, social control and resistance to school surveillance. In: Monahan T and Torres RD (eds) *Schools under Surveillance: Cultures of Control in Public Education*. New Brunswick and London: Rutgers University Press.
Hurst Y and Frank J (2000) How kids view cops: The nature of juvenile attitudes toward the police. *Journal of Criminal Justice* 28: 189–202.
Johnston L and Sheering C (2003) *Governing Security*. London: Routledge.
Laclau E and Mouffe C (2001) *Hegemony and Socialist Strategy: Towards a Radical Democratic Politics*. London and New York: Verso.
Livingstone S and Bober M (2005) *UK Children Go Online: Final Report of Key Project Findings*. London: LSE.
Livingstone S and Brake DR (2010) On the rapid rise of social networking sites: New findings and policy implications. *Children & Society* 24(1): 75–83.
Loader I (2000) Plural policing and democratic governance. *Social and Legal Studies* 9(3): 323–345.
Lyng S (1990) *Edgework: A Social Psychological Analysis of Voluntary Risk Taking*. New York and London: Routledge.
Lyng S (2005) *Edgework: The Sociology of Risk Taking*. New York and London: Routledge.
Martin AK, Van Brakel RE and Bernhard DJ (2009) Understanding resistance to digital surveillance: Towards a multi-disciplinary, multi-actor framework. *Surveillance & Society* 6(3): 213–232.
Miller P and Rose N (2008) *Governing the Present: Administering Economic, Social and Personal Life*. Cambridge: Polity.

Miller WJ (2005) Adolescents on the edge: The sensual side of delinquency. In: Lyng S (ed.) *Edgework: The Sociology of Risk-Taking*. New York and London: Routledge.
Mitchell KJ, Finkelhor D and Wolak J (2004) Victimization of youths on the internet. *Journal of Aggression, Maltreatment & Trauma* 8(1): 1–39.
Monahan T and Torres RD (eds) (2010) *Schools under Surveillance: Cultures of Control in Public Education*. New Brunswick, NJ: Rutgers University Press.
National Policing Improvement Agency (NIPA) (no date) Reassurance policing. Available at: http://www.npia.police.uk/en/docs/Reassurance_policing_.pdf (accessed 8 March 2011).
Nissenbaum H (2010) *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford, CA: Stanford Law Books.
O'Malley P (1992) Risk, power and crime prevention. *Economy and Society* 21(3): 252–275.
Pridmore J and Zwick D (2011) Marketing and the rise of commercial consumer surveillance. *Surveillance & Society* 8(3): 269–277.
Rooney T (2010) Trusting children: How do surveillance technologies alter a child's experience of trust, risk and responsibility? *Surveillance & Society* 7(3/4): 344–355.
Sharples M, Graber R, Harrison C and Logan K (2009) E-safety and Web 2.0 for children aged 11–16. *Journal of Computer Assisted Learning* 25(1): 70–84.
Simon J (1998) Managing the monstrous: Sex offenders and the new penology. *Psychology, Public Policy and Law* 4(1–2): 452–467.
Simon J (2007) *Governing through Crime: How the War on Crime Transformed American Democracy and Created a Culture of Fear*. Oxford and New York: Oxford University Press.
Solove D (2008) *Understanding Privacy*. Cambridge, MA: Harvard University Press.
Steeves V and Jones O (2010) Editorial: Surveillance, children and childhood. *Surveillance & Society* 7(3/4): 187–191.
Taylor E (2010) I spy with my little eye: The use of CCTV in schools and the impact on privacy. *The Sociological Review* 58(3): 381–405.
Thomas D and Loader B (2000) *Cyber Crime: Law Enforcement, Security and Surveillance in the Information Age*. London: Routledge.
Wall DS (2010a) Policing cyberspace: Situating the public police in networks of security within cyberspace (revised May 2010). *Police Practice and Research: An International Journal* 8(2): 183–205.
Wall DS (2010b) Criminalising cyberspace: The rise of the Internet as a 'crime problem'. In: Jewkes Y and Yar M (eds) *Handbook of Internet Crime*. Cullompton and Portland, OR: Willan Publishing.
White D and Pitts M (1998) Educating young people about drugs: A systematic review. *Addiction* 93(10): 1475–1487.
Withers K and Sheldon R (2008) *The Hidden Life of Youth Online*. London: Institute for Public Policy Research.
Wolak J, Finkelhor D, Mitchell KJ and Ybarra ML (2008) Online 'predators' and their victims: Myths, realities and implications for prevention and treatment. *American Psychologist* 63: 111–128.
Yar M (2010) *Cybercrime and Society*. London, Los Angeles, CA, New Delhi and Singapore: SAGE.

Biography

David Barnard-Wills is Research Fellow in Informatics and Systems Engineering, Cranfield University. He obtained his PhD in Politics from the University of Nottingham. Research interests include the politics of technology, security, privacy and surveillance.