IGI PUBLISHING ITJ 5349

701 E. Chocolate Avenue, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.igi-global.com

This paper appears in the publication, International Journal of Technology and Human Interaction, Volume 5, Issue 4
edited by **Bernd Carsten Stahl © 2009, IGI Global**

Counter-Surveillance Strategies Adopted By Child Pornographers

Marie Eneman, University of Gothenburg, Sweden

ABSTRACT

On the one side, it could be argued that ICT provide a perceived anonymity for people downloading and distributing child abusive material, also labelled child pornography. While, on the other side the technology offers powerful surveillance mechanisms to monitor these activities and thus constitutes a powerful tool for law enforcement. This article aims to explore how offenders manage the risk of surveillance when downloading, distributing and exchanging child abusive material. Critical research with a focus on panopticon is used as a theoretical framework. The data is drawn from interviews with offenders, convicted of child pornography. The findings show that the offenders have developed technological and social strategies to reduce the risk of surveillance and addresses the need of a new theoretical concept better adjusted to surveillance practices that allow the many to watch the many. The ultimate motivation for researching this topic is to contribute to the development of effective child protection strategies.

Keyword: *Child Abusive Material, Critical IS Research, ICT, Offender, Panopticon, Strategies, Surveillance*

INTRODUCTION

The widespread dissemination and use of information and communication technologies (ICT) (Knights & Murray, 1994) in combination with technological advances have facilitated for individuals with a sexual interest in children to produce, download, distribute and exchange child abusive material (Taylor & Quayle, 2003; Sheldon & Howitt, 2007; Gillspie, 2008). Another characteristic of the technology is that it easily can be used to create networks where people with a sexual interest in children can meet other like-minded individuals (Thomas & Loader, 2000). Research shows that these kind of networks are considered important by people with a sexual interest in children, since they offer the possibility to share and exchange child abusive material regardless of national boundaries (Taylor & Quayle, 2003; Eneman, 2008). Murray (2006) highlights the dualistic nature of ICT and uses the metaphor of a double-edged sword. One could argue that, on the one side, the technology provides 'perceived anonymity' (Sheldon & Howitt, 2007) or 'apparent cover of anonymity' (Gillespie, 2008), accessibility and affordability. Another feature of the technology is that it reduces the social exposure for people downloading and distributing child abusive material (Taylor & Quayle, 2003; Adam, 2005; Eneman, 2008). Whilst, on the other side the technology offers

DOI: 10.4018/jthi.2009062501

powerful surveillance mechanisms that can be used to monitor these activities and thus constitute a powerful tool for law enforcement in crime detection (Gillespie, 2008; Lyon, 2006; Thomas & Loader, 2000). Contemporary surveillance systems have become less obvious and overt, and more systematic and subtle in our everyday life (Lyon, 2001; Haggerty, 2006). Consequently, even that people are aware of the risk of being monitored when downloading and/or distributing child abusive material, they do not know exactly when they are subject of surveillance or how comprehensive others' knowledge of them actually is (Lyon, 1994).

The research topic of this article is child abusive material (Quayle et al, 2006; 2008), also labelled child pornography. Gillespie (2008) argues that child pornography is 'an extremely controversial label' and that professionals tend not to use it since it reduces the gravity of what the material portrays and invites comparisons with adult pornography. The term child pornography is not unproblematic and there is not one single definition of it. Interpol has formulated the following useful definition of child pornography: "Child pornography is created as a consequence of the sexual exploitation or abuse of a child. It can be defined as any means of depicting or promoting the sexual exploitation of a child, including written or audio material, which focuses on the child's sexual behaviour or genitals" (Sheldon & Howitt, 2007). This definition highlights that child pornography can exist in different forms such as visual depictions, audio depictions and textual depictions (Gillespie, 2008). Quayle et al (2008) have, in the recent thematic paper on *Child Pornography and Sexual Exploitation of Children Online*, recognised that there has been a significant change in the discourse used to describe the material portraying sexual abuse and/or exploitation of children. They have identified that the terms 'abusive images' and 'abusive material' now are widely used by professionals. It should be emphasized that not all sexual depictions of children are visual, therefore the latter term 'abusive material' is more appropriate to use since it also capture non-visual material such as audio and text (Sheldon & Howitt, 2007). Most jurisdictions use the term 'child pornography' (Gillespie, 2008). This article will primarily use the term 'child abusive material' but the term 'child pornography' will also be used due to that it is the legal definition used in Sweden. I do however agree with Gillespie (2008) and Quayle et al (2006; 2008) that the term child pornography is an inadequate term. The research topic of child abusive material is studied in relation to ICT usage. When using the term ICT it should be noted that ICT is not one homogenous technology (Gillespie, 2008; Eneman, 2006). ICT consists of several different technologies, which have different characteristics, and there are also variations in how different technologies are interpreted and used (Monteiro & Hanseth, 1995; Walsham, 2004).

According to current Swedish legal position: production, distribution and possession of child pornography are criminalised. The Swedish legislation has however been proven to be inadequate in parts (Eneman, 2005), and has not been adjusted to tackle the contemporary technological challenges (Gillespie, 2005; 2008). The limitations refer to the lack of legal regulation of viewing child pornography online and the current classification of child pornography as a 'crime against public order' and not as a sexual crime. England and Wales solved the issue of viewing child pornography online by inserting the verb 'to make' into the legislation to more effectively adjust it to modern advanced technology (Gillespie, 2005; 2008). Besides being a criminal offence in many Western countries, child pornography is also a phenomenon that is strongly unacceptable in society (Taylor and Quayle, 2003). To sum up, the implication is that people who download, distribute and exchange child abusive material, also labelled 'child pornographers' (Sheldon & Howitt, 2007), have strong incitement to protect their identity to reduce the risk of being detected and thereby be prosecuted for the committed crime.

My ultimate motivation (Walsham, 2005; Stahl, 2008) for researching this topic is to contribute with knowledge to the development

of effective child protection strategies (Taylor & Quayle, 2003; Gillespie, 2008). Adequate knowledge can paradoxically only be obtained by studying the offenders' behaviour. This article aims therefore to explore the offenders' relationship toward the risk of surveillance by focusing on the following question: How offenders manage the risk of surveillance when downloading, distributing and exchanging child abusive material?

This article contributes to the theoretical field of critical information systems research (CISR) by exploring how the idea of panopticon (Foucault, 1979) can be applied to better understand the offenders' behaviour to manage surveillance issues related to child abusive material. Brief reflections upon the application of emancipation in relation to the studied topic will also be made (Alvesson & Deetz, 2000; Stahl, 2008). Furthermore the article aims to contribute to the debate of this topical issue and thereby support policy developments on a national and international level. It is of critical importance to study the offenders' use of ICT as part of their offending behaviour (Sheldon & Howitt, 2007). The development of effective legal and technological regulation models for preventing child abuse crime via ICT are dependent on our understanding of the offenders ICT usage (Eneman & Gillespie, 2009). The article is organised as follows: in the next section the theoretical framework of critical information systems research is presented with a focus on the theoretical concept of panopticon, followed by a description of the research strategy. Then the findings are presented, followed by a discussion and finally the article closes with a conclusion.

THEORETICAL FRAMEWORK

Critical IS Research

An emerging research field within the IS discipline, relevant for this study, is critical IS research (CISR) (Howcroft & Trauth 2005). CISR can be seen as a reaction to the mainstream IS research which tends to assume that technological innovation is 'inherently desirable' and beneficial to all (McGrath, 2005). The offenders' usage of ICT for child abusive material is an illustrative example of how well established usage of ICT becomes the foundation for harmful content. CISR is based on 'critical theory' (Horkheimer and Adorno, 1972; Klein and Huynh 2004; Croon- Fors, 2006). 'Critical theory' is not a unified theory 'but rather a set of loosely linked principles' (Klecun, 2005), with a commonality 'to change the status quo and promote emancipation' (Alvesson & Deetz, 2000; Stahl, 2008). Critical IS researchers use a wide spectrum of critical social theories (for example Bourdieu, Foucault, Habermas) to critically question established assumptions about the technology, its use and its implications (Cecez-Kecmanovic, 2005, Willcocks, 2006). Engaging in CISR entails the study of the research object with the aid of concepts relevant to critical theory, for example domination, power, control, emancipation etc (Cecez-Kecmanovic, 2005). In addition to using relevant concepts, the research object should be placed in a wider historical, political, social and economic context (Alvesson & Deetz, 2000). A wider discussion of the historical, social and political context of child pornography can be found in Taylor and Quayle (2003) and Sheldon and Howitt (2007). By critically questioning 'social realities' and provide alternative insights how these 'realities' are historically, politically and socially constructed and strongly shaped by asymmetries of power in society, we are able to move beyond established definitions and assumptions and can achieve emancipation from traditional existing structures (Cecez-Kecmanovic, 2005; Alvesson & Deetz, 2000).

The central aim in critical IS research is its deep interest of emancipation (Stahl, 2008; Alvesson & Deetz, 2000). Stahl (2008) highlights some of the fundamental problems involved with the critical intention to emancipate, for example when the research subjects do not prefer to be emancipated. The emancipatory perspective in this article refers to emancipation on a societal level to effectively protect children

through legal and technological regulations (Gillespie, 2008). The rationale to study the offenders' surveillance practices is to obtain insights about their behaviour that can be used in the development of effective societal child protection strategies.

Surveillance and Panopticon

Surveillance is not a new phenomenon, humans have always kept an eye on each other with purpose to control their surrounding (Lyon 1994). The diffusion of ICT in society has however changed the conditions for surveillance radically (Lyon, 2006). One of the most important differences is that today with the use of ICT, the surveillance systems have become less obvious, more systematic and subtle in our everyday life (Haggerty, 2006). Accordingly, people seldom know exactly when they are subjects of surveillance or how comprehensive others' knowledge of them actually is (Lyon 1994). Both Murray (2006) and Lyon (2006) accentuate the dualistic nature of surveillance technologies. Lyon (2006) claims that surveillance technologies have 'two faces' and can be used to control unwanted behaviour, such as illegal activities, but at the same time the technology can be used to facilitate such illegal activities (Lyon, 2001). One of the most unparalleled metaphors of the power of surveillance in the contemporary world is panopticon (Foucault, 1979; Lyon, 2006). The panopticon was originally an architecture design developed by Bentham as a special surveillance tower for a prison (Foucault, 1979). This architecture consists of a central visible surveillance tower and a courtyard surrounded by an outer ring of cells (Willcocks, 2004). The issue of visibility is of vital importance in the panopticon design, since it constantly reminds the prisoners of the possibility of being observed (Foucault, 1979). The design is based upon the principle that the few guards in the tower could watch the many prisoners in the cells, while the observed could not communicate with each other, nor see the observers, but are constantly aware of the risk of being monitored by the guards (Willcocks, 2004). With this design, surveillance became automated and depersonalized as the identity of the observer remains hidden (Lyon, 2001).

Foucault (1979) reinvented the concept of panopticon as a metaphor for 'modern disciplinary societies'. Panopticon can be seen as 'the illusion of constant surveillance', since the prisoners are constantly aware of the risk of being monitored regardless if they de facto are monitored or not (Foucault, 1979; Whitaker, 1999). The feeling of constant surveillance creates a 'permanent panopticon', where the prisoners act as if they are constantly monitored (Jonsson, 2006). The panopticon design constitutes a power mechanism that aims to control and discipline the prisoners' behaviours (Willcocks, 2004). As the prisoners fear that they might be watched, and fear punishment for transgressions, they internalize rules (Foucault 1979). According to Foucault (1979) power should be seen as something that is exercised rather than possessed in the panoptic environment. The power is exercised and maintained by the individuals in the panoptic environment. In Foucault's point of view, power relations should not be seen as merely negative but productive as well (Foucault, 1979). The panopticon design constituted an automatisation of the surveillance systems. While the design of panopticon allows the few to watch the many, the concept of synopticon (Mathieson, 1997) refers to surveillance practices where the many watch the few (for example through television). Mathieson (1997) argues however that these two systems should not be seen as each others contrasts, since they can interact intimately and strengthening each other (Lyon, 2003). Mathieson (1997) emphasizes the parallels between synopticon and panopticon. They have developed through the same period, from 1800 to 2000, and both have been 'technologically upgraded and intensified in the later twentieth century' (Lyon, 2003). Another common characteristic is that they can both be used as means of power (Lyon, 2003).

Surveillance, Panopticon and ICT

Through the use of ICT the surveillance capabilities have been expanded and further automated (Lyon, 2006). ICT enables many processes and tasks to be performed at the same time and can be used to large-scale collection and storage of data (Jonsson, 2006). The technology also allows for data to rapidly flow within and between different systems. Jonsson (2006) describes how ubiquitous environments can be seen as panoptic environments since they enable a form of surveillance, which persists across time and space where people have to assume that they can be monitored the whole time. The issue of visibility, a central visible surveillance tower, is one of the major differences between the original panopticon and surveillance systems based on ICT (Lyon, 2006). ICT-based surveillance systems are often concealed in the environment and are thus invisible for the users. Jonsson (2006) claims that a consequence of this, when the surveillance mechanisms are embedded in the environment, is that the users are aware that surveillance potentially can take place at any time, performed by unknown actors and for unknown purpose. Ball (2006) describes how powerful panopticon structures can elicit active resistance, where strategies to avoid surveillance are developed. Research shows that users in ICT-based environments can circumvent surveillance capabilities in the environment (Timmons, 2003), by finding out when they are being monitored and organise collective resistance (Bain & Taylor, 2000). This highlights that it is a mistake to believe that surveillance systems result in complete disciplinary power (Lyon, 2006).

Critique of Panopticon

Even though the panopticon is a strong metaphor to conceptualize and understand surveillance practices it has been criticised for its limitations to adequately understand contemporary technological societies (Lyon, 2006; Haggerty, 2006). The critique is based upon the argument that we must 'move beyond' panopticon, since the concept does not reflect all aspects of computerized surveillance. Poster (1995) introduced the concept 'super panopticon' to illustrate how databases enhance the surveillance capabilities. The 'postmodern panopticon' is another concept presented by Albrechtslund (2005) to highlight the new dimension introduced by ubiquitous computing. Despite its critique, the panopticon concept refuses to go away and the reasons for this are manifold but clearly one of them is that panopticon is such a rich multifaceted concept (Lyon, 2006). It can be used for interpretation in a number of ways and in different contexts. Lyon (2006) argues that it is impossible to evade some interaction with the panopticon, either historically or in today's analyses of surveillance. Following the same vein, Boyne (2000) claims that it is best to 'accept the panoptic presence, even if only as the ghost lurking within the post-panoptic world'.

Panopticon in Different Contexts

Willcocks (2006) argues that despite that Foucault himself wrote little directly about ICT, the work of Foucault is useful for the IS discipline in contemporary social studies of ICT. The concept of panopticon has been used in the analysis of different contexts such as prisons (Foucault, 1979), workplaces (Zuboff, 1988; Doolin, 1998; Jonsson, 2006; Ball, 2006) and in other public spaces (Koskela, 2006). Adam (2005) has applied a similar surveillance and control perspective in her studies of cyberstalking and Internet pornography. Adam's focus is upon the offenders' possibility to carry out surveillance on potential victims in this technological environment. In the light of the risk of being monitored when carrying out a criminal offence such as child pornography, this article applies the concept of panopticon. The motivation to use this concept is to obtain insights of how the individual offender manage the risk of surveillance when downloading, distributing and exchanging child abusive material by using ICT (Foucault, 1979; Lyon, 2006; Willcocks, 2006; Jonsson, 2006; Brooke, 2002).

RESEARCH METHODOLOGY

Researching the 'world of child pornography' (Taylor & Quayle, 2003) involves both certain practical and ethical considerations. This includes for example how to gain access to people who have experience from this world as they can be characterised as a 'hard to reach group' for people outside this world (Taylor & Quayle, 2003; Wilson & Jones, 2008). Due to that the production, distribution and possession of child pornography is a criminal offence in most Western countries, it is unlikely that people involved in this world would be willing to discuss their activities prior convictions. It would also be an extremely difficult and complex issue, practically, ethically and legally, for a researcher to try and gain access to non-convicted persons who have experience of producing and/or downloading and/or distributing and/or exchanging child abusive material. The approach used within this study has been to interview offenders convicted of child pornography (Taylor & Quayle, 2003; Noaks & Wincup, 2004; Wilson & Jones, 2008). It could be argued that offenders who have been involved in activities related to the world of child pornography are key experts and thus can provide information about their activities and behaviour within this world (Wilson & Jones, 2008). The motivation to interview convicted offenders was to obtain information that increase the understanding about how the individual offender manage the risk of surveillance when downloading, distributing and/or exchanging child abusive material.

Data Collection

The data was collected through semi-structured interviews with fifteen male offenders (Taylor & Quayle, 2003; Noaks & Wincup, 2004) aged 19 to 55 years old. They have all been convicted of production and/or, distribution and/or possession of child pornography, where ICT has been used. Of these fifteen offenders, eleven were also convicted for other sexual offences, mainly sexual abuse against children. These other offences have however not been in focus in this article. The offenders came from a variety of demographic backgrounds and their engagement with treatment programmes also varied. The researcher gained access to the offenders through prison psychologists at the prison and probation services. Noaks & Wincup (2004) emphasize that it is important that researcher address the responsibilities they have to their respondents. This includes ensuring that the relationship between the researcher, who collects the data, and the respondent, who provides the data, is clear and professional. This was achieved by providing all the respondents, prior the interviews, with an information letter about the study and the principle with informed consent. (Brantsaeter, 2001; Taylor & Quayle, 2003; Noaks & Wincup, 2004). The letter contained information about (1) the purpose with the study and the interviews, (2) how the data would be used and stored, (3) the issue of confidentiality, (4) that the participation was voluntary and that the respondents could withdraw at any time and if so none of the data would have been used and finally (5) information how to get in contact with the researcher at a later stage if the respondent would like to comment and/or ask anything in relation to the study.

All the interviews took place in the prison, either in the visiting room or in the prison psychologist's office. The interviews, each lasting between 1.5 and 2 hours hours, were in eleven cases tape recorded and later transcribed. In four cases, where the respondents did not want the interview to be tape recorded, field notes were taken and carefully written out immediately after the interview (Silverman, 2005; Noaks & Wincup, 2004). The same researcher has both interviewed the respondents and transcribed the data (Taylor & Quayle, 2003). The purpose with the interviews was to obtain a deeper understanding of the individual offender's management of the risk of surveillance when downloading, distributing and exchanging child abusive material. During the interviews the respondents were asked questions regarding their individual experience, understanding and management of the risk of surveillance in the specific context. Open-ended questions were used rather

than closed questions, and efforts were made to 'elicit stories' from the respondents (Taylor & Quayle, 2003; Noaks & Wincup, 2004). To avoid eliciting 'one-word answers' (Hollway & Jefferson, 2000), the open-ended questions were designed like 'tell me about your experiences of avoiding surveillance when downloading child pornography'. Follow-up questions were used to further develop the respondents' stories (Taylor & Quayle, 2003). Since this study is part of a wider ongoing research project, exploring the offenders' use of ICT for child abusive material, the interviews covered more issues than the surveillance related ones.

Data Analysis

The process of analysis should not be seen as a distinct stage, but as an ongoing process that permeates every stage in the research study (Noaks & Wincup, 2004). The process of transcription offered the opportunity for initial reflection on the data. Once the data was transcribed, it was first read and re-read and initially notes were taken to comment the material. In the next stage the material was structured and coded in relation to the research question and the data sorted into emerging categories (Taylor & Quayle, 2003; Noaks & Wincup, 2004). This was influenced by theoretical concepts, such as surveillance, power, control and resistance etc, and a search of patterns within the data (Coffey & Atkinson, 1996). During the last stage subjective meanings were searched and differences and similarities were identified among the categories identified in the previous stage (Taylor & Quayle, 2003; Silverman, 2005). In this study, the researcher has used certain theoretical concepts, which have worked as themes, both in the design of the data gathering and when analysing the data.

Critical Reflections

When reflecting on this approach critically, it means that the researcher went into the area with certain preconceived ideas and a thematic focus when analysing the collected data. One of the potential pitfalls with using a 'theoretically informed empirical research' (Noaks & Wincup, 2004) as an approach is that the researcher only focus upon themes known in advance and misses other relevant themes in the data. The researcher has however tried to combine a 'theoretical informed empirical research' approach with 'openness and flexibility, (Coffey & Atkinson, 1996) in the search of themes in the data. An alternative approach could have been the use of a combination of analytic strategies. Such a 'triangulation' approach could have provided varying perspectives and as such alternative insights of the research subject (Coffey & Atkinson, 1996).

The limitations of the material should be noted. All the respondents in this study have been arrested and convicted of child pornography and in many cases, as mentioned above, also for other sexual offences. It should be acknowledged that arrested and convicted offenders only represent a fraction of all child pornographers and that child pornography and other sexual crimes have a very low reporting rate (Quayle et al., 2006; Terry & Tallon, 2004).

Ethical Reflections

This study follows the ethical rules and guidelines for research, formulated by the Swedish Research Council[1]. As described above, all the respondents were prior their involvement in the study provided with information about the purpose of the study and how the material will be used and stored. Furthermore the respondents have given their consent to participate in the study. Another important consideration for this study has been to ensure confidentiality for the respondents. All identifying information has been removed or changed to ensure this. As described above this article is part of a wider ongoing project, which is approved by the Ethical Committee at the University of Gothenburg. The interviews have provided a rich source of information about the individual offenders' behaviour when managing the risk of surveillance, which would have been difficult to obtain ethically in any other way.

FINDINGS

Before presenting the result regarding how the offenders manage the risk of being under surveillance, this first section presents findings that illustrate the offenders' awareness of the risk of being monitored. During the interviews a recurring theme was the tension between how to be able to conduct the desired activities at the same time as avoiding being revealed. The findings show that surveillance and anonymity are considered as important and serious issues among all the respondents. In the interviews the offenders expressed concern about the risk of being under surveillance when downloading child abusive material. It is considered important among the offenders to protect their identity and to reduce the risk of being detected. One respondent expressed his concern of surveillance as follows:

Yes, one always thinks about it. Every time you put on the computer. You notice how it blinks like hell and one starts to wonder who the hell it is, sometimes one wonders if it is the cop. Of course one thinks of it, every time one is out there (Interview C)

This illustrates a constant awareness over the risk of being monitored. It also highlights the uncertainty of not knowing who the other persons are in the environment. The other respondents confirmed this constant worrying. They are well aware that production, distribution and possession of child pornography is a criminal offence according to Swedish legislation and therefore they know that they can be monitored at any time. The following quotation illustrates how the awareness of the risk of surveillance is expressed:

Of course I have felt chased. Sometimes I have felt jittery, when it has been a lot of raids. Then it is only a matter of time, one can be totally jittery. But then one thinks that it won't happen to me, but that's what everybody says. (Interview J)

The anxiousness of being monitored appears in different ways. Common issues that are expressed by the quotations above are feelings of being chased, feeling jittery and being under stress. The later quotation adds another dimension, which illustrates an interesting conflict. The respondent describes the feeling of being chased and that it is only a matter of time before getting caught and at the same time he thinks that it won't happen to him. However, the awareness of the risk of surveillance does not seem to refrain the offenders from their involvement in the illegal activities. One the one hand they express serious concern of the risk of being monitored and getting caught, but on the other hand they seem to persuade themselves that it will not happen to them.

As this section has shown the offenders are aware of the risk of being observed. This result is however not very surprising, i.e. that people who are involved in criminal activities are aware and anxious of the risk of being monitored. The awareness does not seem to act as a deterrent for not downloading, distributing and exchanging child abusive material, instead different strategies have been developed and adopted by the offenders.

Developed Strategies

Two principal strategies relating to how the respondents manage the risk of surveillance emerged during the analysis: technological and social strategies. The strategies are often used in a combination, which further indicates the importance of studying the social behaviour and social context, which affect the development and adoption of technological strategies (MacKenzie & Wajcman, 2002).

Technological Strategies

Technology Choice

All the respondents state that it is important to use secure technology and consequently it is also important to avoid insecure technologies. The respondents express that they are careful in their

choice of technology. The technology choice is based on their belief that it is a more secure technology to use, i.e. that it is more difficult for law enforcement to monitor their activities. When talking about the use and security level among different types of ICT one respondent expressed his experience of choosing secure technology like this:

One quickly learns which technology one should use to not be visible. (Interview F)

This illustrates that the offenders view certain technologies as insecure and others as more secure, and that this is something they learn quickly. The technologies that are considered more secure, make the user more invisible and act as a shield for surveillance systems. When talking about insecure and secure technologies the respondents were unanimous in their attitude against World Wide Web. One respondent expressed his concern as follows:

Web pages are not to think of, they are too insecure. (Interview B)

This quotation shows that the respondents exclude certain technologies since they are considered to be insecure. This quotation indicates that this particular technology, World Wide Web, is not even an alternative due to the insecurity. The concern of using insecure technology is confirmed in the following quotation, but this quotation also shows the offender's awareness of the consequences of using insecure technologies.

And yet one knows that if one use for example WinMX [freeware peer-to-peer file sharing program], and if one meets the wrong person on the other side one is screwed up. If loading up to a board without encryption, one is also totally screwed up. If I start downloading from a news server, I am logged everywhere. Sometimes one does not think about it. (Interview E)

What is shown here is the offender's awareness of the risk of using insecure technology, and consequently that the risk of getting caught is increased by using insecure technology. The quotation also illuminates the fear of not knowing whom the other person really is that the respondent is exchanging material with. Awareness and concern are expressed over being logged, i.e. that data is collected about the respondent's activities when using insecure technology. It is however interesting to note that despite the awareness of the risks, the respondent says that he sometimes does not think about the risks but just do it.

Advice and Recommendations regarding Technology Use

Users, who initially don't possess adequate knowledge about which technology that is preferable to use to enhance the security, can obtain advice and recommendations from other users.

During one of the first occasion when I was out looking for something to download, I talked with a person who had greater experience of this than me. He gave me tip-off which technology I should use and which to avoid. (Interview N)

This supports the idea that people who are part of the 'world of child pornography' (Taylor and Quayle, 2003) advice each other regarding technological issues, based on the rationale to enhance the protection of their identity. The inclination to help each other can be explained by the fact that advising other in their environment can also be seen as a protection of themselves. This is due to the fact that production, distribution and possession of child pornography is a criminal offence in many countries, and if one is caught several others also risk to get caught if there are any traceable connections.

Obligatory Rules regarding Technology Use

Besides the advice and recommendations there are a further dimension, with obligatory rules which the user is obliged to follow. Within this network it was obligatory to follow the guidelines in the manual regarding the technology use. It is interesting to note that the members actually are forced to use certain types of technology, otherwise they risk to be excluded from the network. The purpose with these obligatory rules is to ensure a high level of security for all the members within the network.

Everything is built from the ground, all these boards had programmers. One chap who writes the scripts and who is responsible for it. There was another chap who was responsible for a manual with guidelines which everybody were forced to use, about secure technology. (Interview K)

Another interesting aspect shown here is how the network is organised, with certain persons responsible for different aspects. Within this particular network there were for example programmers responsible for the scripts. Another person was responsible for the manual. Respondents who have been member in other networks confirmed that it is common with this kind of social organisation.

Social Strategies

Use of Personal Information

If we move beyond the technological strategies the findings show that the offenders also have developed and adopted different social strategies. As mentioned before, the technological and social strategies are often used in a combination and it is important to understand both the technological and the social aspects of the offenders' behaviour since the two aspects are strongly connected and affect each other. The awareness of the surveillance risk and the incitement to protect the identity affects the offenders' behaviour when interacting with other. One approach that is commonly practiced among the respondents is to be careful with revealing personal information about oneself when interacting with others. This is due to the fact that they almost never can be sure who the other person really is. One respondent expressed it like this:

I have never revealed my real identity and I know that nobody else does it either, it's the way it is you don't think about it. (Interview G)

This statement shows that the offenders are careful with revealing personal information that can reveal their identity. It also shows that this approach is considered to be generally accepted among the users.

Use of Alias

One effect of being careful with personal information is that the offenders use several different alias instead, to enhance the protection of their identity. The risk of getting caught is considered to be reduced when using several alias instead of always using the same. The use of different alias is illustrated in following quotation:

I have different names. A sometimes, B sometimes, C sometimes, it varies. One just picks a name. Unfortunately I can't remember all the names right now, they are too many. No, I can't say that I have used any specific name more than the other. (Interview O)

This respondent claims that he does not use any particular alias more than the other. This is however not a common approach among the other respondents, instead they state that they have one or two alias that they use more frequently. This behaviour can be explained by the fact that it is considered important to build up a reputation connected to the used alias to gain status among like-minded in the environment (Taylor & Quayle, 2003; Eneman, 2005).

Rules for Interaction

Rules for interaction constitute a further dimension of social strategies that are used within closed networks. The purpose with the rules is to enhance the collective security for the users within the network. Following quotation exemplifies what sort of interaction that the rules attempts to regulate:

It's just the way it is, there has to be certain rules for how it should work, what is allowed and what is not. It is the main administrators that create the rules. For example, there are rules that forbid buying and selling. Payment is never allowed. If one is to sell or buy material, there has to be some personal information and then it is a risk of being revealed in some way. We are in fact not allowed to exchange names and telephone numbers and stuff like that, but people do that anyway after a while. (Interview L)

Rules are considered necessary for the network to work safety. Once again we see example of the social organisation of these networks. Main administrators are responsible for creating the rules. Technological rules were presented earlier, which purpose is to regulate the technology used among the users to enhance the security. In this example the rules attempts to regulate what interactions that should be allowed in the network. Buying and selling are forbidden, since such transactions often require a certain amount of personal information and consequently enhance the risk of being revealed. It is also possible to discern a conflict here since the respondent express that the users do not always follow the rules.

Use of Languages

The following quotation is an illustrative example where the offenders carry out counter-surveillance towards their environment, with the purpose to reduce the risk of being monitored. All the offenders in this study are aware of the possibility to carry out surveillance as a form of counter-strategy. They also state that they have monitored other users' behaviour in the ICT-based environment. The following quotation shows how the use of language is monitored:

At least he is English-speaking, it's obvious in the way he writes. Most write in English, but you notice that some make spelling mistakes. Germans don't master English, it's obvious. They write really bad, Frenchmen as well. They mix terribly. One can tell directly that English is not their native language. (Interview I)

The respondent is attentive and observes another user's language usage during their interaction. What is observed is how well the user master the English-language, by spelling correctly. Based on this observation the respondent draws certain conclusions regarding the nationality of the user. This constitute an interesting example of how the offenders are able to discern further information about the other users during their interaction, besides the information actually written.

Use of Patterns

Besides the possibility to observe the language usage, other behaviour have also been observed among the offenders:

I am quite sure that it was the same person. We were several that suspected that. Well, the way these two persons loaded up stuff. Sometimes it was the same places and everything. It is too similar for two different persons to do exactly like that. (Interview I)

This is an illustrative example of how the technology is used to observe another user's behaviour when uploading material. The offenders are attentive and suspicious of certain behaviours in their environment. Furthermore, what is shown is that several users have observed this particular user's behaviour and that they have also discussed this user's behaviour with each other.

DISCUSSION

In this section, the findings will mainly be discussed in relation to the theoretical concept of panopticon. The section will also conclude with some brief reflections regarding the application of the concept of emancipation on this topic.

Feeling of Constant Surveillance

One of the main principles with the panopticon design is to mediate a feeling of 'constant surveillance', where the individuals may not really being observed, they just think or imagine that they are (Foucault 1979, Lyon, 2006). The offenders' statements are well in line with this principle. The results show that they are constantly aware of the risk of being monitored, which confirms the feeling of 'constant surveillance'. Panopticon aims to control and discipline undesirable behaviour by making the prisoners act as if they were observed (Foucault, 1979). The offenders' awareness of the constant risk of being monitored indicates that the 'power mechanism' of panopticon works in ICT-based environments (Willcocks, 2004). However, the 'power mechanism' doesn't seem to act as a deterrent for the offenders. The results show that they have developed and adopted resistance in form of different strategies to be able to continue with their activities. This illuminates that it is a mistake to believe that panoptic environments result in complete disciplinary power (Lyon, 2006; Jonsson, 2006).

Resistance of Surveillance

Powerful panopticon structures can elicit resistance (Foucault, 1979). Ball (2006) describes how the knowledge about the risk of being exposed of surveillance can evoke active resistance among those who believe that they might be monitored. As the findings show the offenders have developed and adopted different strategies to circumvent the risk of being observed, to be able to continue with their activities. Two principal strategies have been identified: technological and social strategies, and they are commonly used in a combination. The developed strategies constitute an illustrative example of the offenders' active resistance of the surveillance capabilities in the environment. Some of the strategies are developed on an individual basis while other can be seen as the organisation of a collective resistance (Bain & Taylor, 2000). The offenders' purpose, with these developed strategies, is to reduce the risk of being visible when carrying out their activities. For the offenders it is important to be as invisible as possible when carrying out their activities, since many actions surrounding the phenomenon is a criminal offence (Taylor & Quayle, 2003).

The development and use of strategies such as 'technology choice' and 'use of alias' are based on the belief that the use of secure technologies, such as encryption etc, make them invisible for surveillance systems in the environment. Some of the identified strategies may seem obvious such as the importance of using 'secure technology', carefulness with 'personal information' and 'use of alias' etc. It is however important to develop knowledge, based on empirical material, about the offenders technology use for child abusive material. The development of technological and legal regulation models (Gillespie, 2008) must be based on adequate knowledge, empirically underpinned, regarding the offenders' behaviour otherwise these regulation models risk being ineffective. The result from this article shows that the offenders are aware that certain technologies are more insecure to use and that they risk being visible for surveillance systems if using them. Therefore, they avoid using technologies such as World Wide Web. This result also highlights why technological regulation such as different Internet Service Provider's (ISPs) filtering techniques, which block the access via World Wide Web to certain websites containing child abusive material, don't work effectively (Eneman, 2006).

The Issue of Visibility

Certain differences have been identified between the original panopticon design and contemporary surveillance structures based on ICT. The issue of visibility is one of the main differences (Willcocks, 2004). In the original panopticon the surveillance tower is visible, whereas in ICT-based environments the surveillance capabilities is invisible 'embedded' in the environment (Jonsson, 2006). The result shows that the offenders feel a constant risk of surveillance, despite that the surveillance systems often are invisible in the environment. This result indicates that the issue of visibility of surveillance systems should no be considered as a decisive aspect regarding surveillance systems in ICT-based environments. Another aspect that differs is that the prisoners in the original panopticon design could not communicate with each other, nor see the observers. As this research shows, the offenders have communicated with each other regarding surveillance issues. An example of this is when they discuss another user's language use. The two examples with the observation of another person's language use and the observation of another person's behaviour when uploading material show how the offenders have adopted counter-surveillance as a strategy to monitor other persons and their behaviour in the environment.

Usefulness of Panopticon

For the purpose of this article, the concept of panopticon was useful in the organisation and coding of the empirical material since it helped the researcher to identify and reflect upon elements such as power, control, discipline and resistance, which are central to adequately understand surveillance practices. It is however important to reflect of the risk, when using theoretical concepts, that the researcher focuses too much upon these concepts and therefore risks to miss other relevant themes in the material. Besides being useful in the analysis, the concept was also useful in the discussion since it helped the researcher to focus upon the important elements, mentioned above, which are central components for the understanding of surveillance practices.

Limitations of Panopticon

One of the main principles of the panopticon design is that it allow for 'the few guards to watch the many prisoners' (Foucault, 1979). One of the characteristics with contemporary technological environments is that it enables for the many to watch the many. According to this, it is important to question whether panopticon is the most useful concept to fully understand the contemporary surveillance practices or if we should listen to the voices raised which claims that it is time to 'move beyond panopticon' (Lyon 2006, Haggerty 2006). However, despite its critique and limitations the concept of panopticon can be used as a powerful concept to understand some of the complex issues of surveillance in contemporary society (Lyon, 2006; Koskela, 2006; Boyne, 2000). Despite that panopticon has been useful to understand some of the complex issues of the offenders surveillance practice, this article claims that we need a new concept. We now have the concept of 'synopticon' for studying surveillance practices where 'the many watch the few' (Mathieson, 1997) and the concept of 'panopticon' where 'the few watch the many' (Foucault, 1979). What is needed, is a third concept that acts as a complement to these two and that can be used to better understand contemporary complex surveillance practises where the many watches the many.

Emancipation

Finally, this topic constitutes an illustrative example of the complexity involved with the critical intention of emancipation (Alvesson & Deetz, 2000) within the field of critical IS research. Stahl (2008) argues that there are certain 'fundamental problems' involved when carrying out critical empirical IS research and accentuates that there are certain ethical concerns involved in the application of the emancipatory perspective. He highlights the complexity that arises when for

example the researcher's ambition is to emancipate the research subjects whereas the research subjects don't wishes to be emancipated. The emancipatory perspective in this article refers to emancipation on a societal level (Alvesson & Deetz, 2000) to effectively protect children through legal and technological regulations (Gillespie, 2008). The researchers motivation to study the offenders practice has been to obtain knowledge about their technological and social behaviour in relation to the research question, since this kind of knowledge based on empirical findings is critical in the development of effective child protection strategies (Taylor & Quayle, 2003). The issue of emancipation in relation to the different stakeholders in the context of child abusive material is a complex issue that will be explored in more detail in future studies.

CONCLUSION

The aim of this article was to explore how offenders manage the risk of surveillance when downloading, distributing and exchanging child abusive material. The topic is strongly related to issues such as use, misuse and regulation of ICT and hence highly relevant and interesting for critical information system researchers. Child pornography is an emotional topic where moral opinions tend to dominate the debate rather than empirical based research. In summary, the article shows that the risk of surveillance does not act as a deterrent for the offenders, instead they behave as active actors and have developed resistance to reduce the risk of being monitored. Two principal strategies, technological and social, were identified which the offenders have developed to reduce the risk of being monitored when downloading, distributing and exchanging child abusive material. This emphasizes that it is a mistake to believe that panoptic environments automatically result in disciplinary power.

The theoretical contribution of the article is to show how critical ideas such as Foucault's concept of panopticon can be used to highlight issues related to misuse of ICT. The concept of panopticon has been useful to better understand the offenders' surveillance practice, since it enabled the researcher to identify, reflect and understand how central elements such as power, control, discipline and resistance affect the offenders' behaviour and shape their surveillance practice. However, this article argues that a new concept with a critical edge is needed to better understand contemporary complex surveillance practices that allow for the many to watch the many. To be useful for its purpose, the concept should be designed to act as a complement to panopticon and synopticon.

Furthermore, the article highlights the complexity involved in the critical intention to emancipate. The ultimate goal for critical researchers is to contribute to the transformative praxis and therefore it is important to be explicit with who is going to be emancipated and why. The emancipatory perspective in this article refers to emancipation on a societal level to effectively protect children through legal and technological regulations. In this article the researcher has studied the offenders practice to be able to obtain insights about their behaviour that can be used in the development of effective preventative child protection strategies. Further critical studies are called for to investigate the complexity that can arise when applying the concept of emancipation within the area of child abusive material.

Critical reflection of the conducted research is considered as an important part of critical research. Following that vein, it should be acknowledged that the article has not covered all possible angles such as the economic, historical, political and social context, which are considered central for a critical investigation of a social phenomenon. A more detailed ethical analysis of the topic may also have helped highlighting certain issues. A critical reflection of the selection of respondents, i.e. indicates that the result from this study is perhaps more representative of convicted offenders rather than of non-convicted offenders downloading, distributing and exchanging child abusive material. Which raises the question if non-convicted

offenders have developed and use different and more advanced strategies to avoid being detected.

Despite certain limitations of this article, it will hopefully make an important contribution to the theoretical field of critical information systems research by showing the relevance of critical research when applied to misuse of ICT and to the debate surrounding child abusive material by providing insights of offenders behaviour when downloading, distributing and exchanging child abusive material.

REFERENCES

Adam, A. (2005). *Gender, Ethics and Information Technology*. Palgrave Macmillan.

Albrechtslund, A. (2005, July 17-19). The Potmodern PanopticonSurveilance and privacy in the age of Ubiquitous Computing. *Conference Proceedings of CEPE 2005*.

Alvesson, M., & Deetz, S. (2000). *Doing Critical Management Research*. Sage.

Avgerou, C., & McGrath, K. (2005). Rationalities and emotions in IS innovation. In D. Howcroft & E. Trauth (Eds.), *Handbook of Critical Information Systems Research*. Edward Elgar.

Bain, P., & Taylor, P. (2000). Entrapped by the Electronic Panopticon? Worker Resistance in the Call Centre. *New Technology, Work and Employment, 15*(1). doi:10.1111/1468-005X.00061

Ball, K. (2006). Organization, Surveillance and the Body: Towards a Politics of Resistance. In D. Lyon (Ed.), *Theorizing Surveillance: The Panopticon and Beyond*. Willan Publishing.

Boyne, R. (2000). Post-Panopticism. *Economy and Society, 29*(2), 285–307. doi:10.1080/030851400360505

Brantsaeter, M. (2001). *Möter med menn dömt för seksuelle overgrep mot barn*. Doctoral Thesis, Report 3:2001, Institutt for Sosiologi og Samfunnsgeografi, Universitetet i Oslo.

Brooke, C. (2002). What Does it Mean to be 'Critical' in IS Research? *Journal of Information Technology, 17*(2).

Cecez-Kecmanovic, D. (2005). Basic assumptions of the critical research perspectives in information systems. In D. Howcroft & E. Trauth (Eds.), *Handbook of Critical Information Systems Research*. Edward Elgar.

Coffey, A., & Atkinson, P. (1996). *Making Sense of Qualitative Data: Complementary Research Strategies*. Sage Publications.

Croon-Fors, A. (2006). *Being-With Information Technology: Critical Explorations Beyond Use and Design*. Doctoral Thesis, Department of Informatics, Umeå University, Umeå, Sweden.

Doolin, B. (1998). Information Technology As A Disciplinary Technology: Being Critical in Interpretive Research in Information Systems. *Journal of Information Technology, 13*(4). doi:10.1057/jit.1998.8

Eneman, M. (2005). The New Face of Child Pornography. In M. Klang & A. Murray (Eds.), *Human Rights in the Digital Age*. Cavendish Publishing.

Eneman, M. (2006, September 21-23). Child Pornography & ICT: Reflections on the Need for an IS Research Agenda. [*Conference*, Nova Gorica, Slovenia.]. *Proceedings of IFIP-T, C9*, HCC7.

Eneman, M. (2008, June 8). Panoptic Environments: Offenders Balance of Privacy and Surveillance in the Context of Digital Child Pornography. *Proceedings of the 3rd International Workshop on Critical Research in Information Systems*, Galway, Ireland.

Eneman, M., & Gillespie, A. (Forthcoming 2009). Tackling the Grooming of Children Through ICT: A Comparative Approach. *Forthcoming in a journal 2009*.

Foucault, M. (1979). *Discipline and Punish: The Birth of the Prison*. Vintage.

Gillespie, A. A. (2005). Indecent Images of Children: The Ever-Changing Law. [Published online in Wiley InterScience] [www.interscience.wiley.com]. *Child Abuse Review, 14*, doi:10.1002/car.919

Gillespie, A. A. (2008). *Child Exploitation and Communication Technologies*. Russell House Publishing.

Haggerty, K. D. (2006). Tear Down the Walls: On Demolishing the Panopticon. In D. Lyon (Ed.), *Theorizing Surveillance: The Panopticon and Beyond*. Willan Publishing.

Howcroft, D., & Trauth, E. M. (2005). *Handbook of Critical Information Systems Research: Theory and Application*. Edward Elgar.

Jonsson, K. (2006). The Embedded Panopticon: Visibility Issues of Remote Diagnostics Surveillance. *Scandinavian Journal of Informatin Systems, 18*(2).

Klecun, E. (2005). Competing rationalities: a critical study of telehealth in the UK. In Howcroft & Trauth (Eds.), *Handbook of Critical Information Systems Research*. Cheltenham: Edward Elgar.

Klein, H., & Huyhn, M. (2004). The Critical Social theory of Jurgen Habermas and its Implications for IS Research. Mingers & Willcocks (Eds.), *Social Theory and Philosophy for Information Systems*. John Wiley & Sons, Ltd.

Kling, R., Rosenbaum, H., & Sawyer, S. (2005). *Understanding and Communicating Social Informatics: A Framework for Studying and Teaching the Human Contexts of Information and Communication Technologies*. Information Today, Inc.

Knights, D., & Murray, F. (1994). *Managers Divided: Organizational Politics and Information Technology Management*. Chichester: Wiley.

Koskela, H. (2006). 'The Other Side of Surveillance': Webcams, Power and Agency. In D. Lyon (Ed.), *Theorizing Surveillance: The Panopticon and Beyond*. Willan Publishing.

Lyon, D. (1994). *The Electronic Eye: The Rise of Surveillance Society*. University of Minnesota Press. Lyon, D. (2001). *Surveillance Society: Monitoring Everyday Life*. Open University Press. Lyon, D. (2003). *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination*. Routledge. Lyon, D. (2006). *Theorizing Surveillance: The Panopticon and Beyond*. Willan Publishing.

MacKenzie, D., & Wajcman, J. (2002). *The Social Shaping of Technology*. Open University Press.

Mathieson, T. (1997). The Viewer Society: Foucault's Panopticon Revisited. *Theoretical Criminology, 1*(215), 34.

McGrath, K. (2005). Doing critical research in information systems: a case of theory and practice not informing each other. *Information Systems Journal, 15*, 85–101. doi:10.1111/j.1365-2575.2005.00187.x

Mcluhan, M. (2003). *Understanding Media: The Extensions of Man: Critical Edition*. Gingko Press.

Monteiro, E., & Hanseth, O. (1995). Social shaping of information infrastructure: on being specific about the technology. In W. Orlikowski, G. Walsham, M.R. Jones, & J.I. DeGross (Eds.), *Information technology and changes in organisational work*. Chapman & Hall.

Murray, A. (2006). *The Regulation of Cyberspace: Control in the Online Environment*. Routledge Cavendish.

Noaks, L., & Wincup, E. (2004). *Criminological Research: Understanding Qualitative Methods*. Sage Publications.

Poster, M. (1995). *The Second Media Age*. Cambridge: Polity.

Quayle, E., Erooga, M., Wright, L., Taylor, M., & Harbinson, D. (2006). *Only Pictures? Therapeutic Work with Internet Sex Offenders*. Russell House Publishing.

Quayle, E., Lööf, L., & Palmer, T. (2008). Child Pornography and Sexual Exploitation of Children Online. *Thematic Paper to the World Congress III against Sexual Exploitation of Children and Adolescents*.

Richardson, H. (2005). Consuming passions in the 'global knowledge economy'. In Howcroft & Trauth (Eds), *Handbook of Critical Information Systems Research*. Cheltenham: Edward Elgar.

Sheldon, K., & Howitt, D. (2007). *Sex Offenders and the Internet*. John Wiley & Sons, Ltd.

Silverman, D. (2005). *Doing Qualitative Research*. Sage Publications.

Stahl, B. (2008). *Information Systems: Critical Perspectives*. Routledge.

Taylor, M., & Quayle, E. (2003). *Child Pornography: An Internet Crime*. Routledge.

Thomas, D., & Loader, B. D. (2000). *Cybercrime: Law Enforcement, Security and Surveillance in the Information Age*. Routledge.

Timmons, S. (2003). A Failed Panopticon: Surveillance of Nursing Practice via new Technology. *New Technology, Work and Employment, 18*(2). doi:10.1111/1468-005X.00116

Walsham, G. (2004). *Making a World of Difference: IT in a Global Context*. John Wiley & Sons Ltd.

Walsham, G. (2005). Learning about being critical. *Information Systems Journal, 15*, 111–117. doi:10.1111/j.1365-2575.2004.00189.x

Whitaker, R. (1999). *The End of Privacy.* New York: The New Press.

Willcocks, L. (2004). *Foucault, Power/Knowledge and Information Systems: Reconstructing the Present In Social Theory and Philosophy for Information Systems.* John Wiley & Sons, Ltd.

Willcocks, L. (2006). Michel Foucault in the Social Study of ICTs: Critique and Reappraisal. *Social Science Computer Review, 24*(3). doi:10.1177/0894439306287973

Wilson, D., & Jones, T. (2008). 'In My Own World': A Case Study of a Paedophiles Thinking and Doing and His Use of the Internet. *Howard Journal, 47*(2).

Zuboff, S. (1988). *In the Age of the Smart Machine: The Future of Work and Power.* Basic Books.

ENDNOTE

1 http://www.codex.vr.se/codex_eng/codex/index.html

Marie Eneman is a PhD student and lecturer at the Department of Applied IT at the University of Gothenburg, where she also is part of the research group IT & Innovation. Eneman is carrying out research within the area of child pornography and information technology, with a focus of the technology involved. She also studies the phenomenon of grooming. The empirical material consists of Swedish court records and police records of all child pornography crimes during the period of 1993-2007 and of semi-structured interviews with offenders convicted of child pornography. Eneman applies a critical approach in her research and is active within the international critical informations systems research field. The issues of child pornography, grooming and ICT is the focus of her doctoral thesis.