Cyberpsychology and Human Factors

Dr Jo Bryce

Cyberspace Research Unit, School of Psychology, University of Central Lancashire, Preston, PR1 2HE

Abstract

The online environment has become a significant focus of the everyday behaviour and activities of individuals and organisations in contemporary society. The increasing mediation of communication has led to concerns about the potential risks and associated negative experiences which can occur to users, particularly children and young people. This is related to the emergence of the online environment as a location for criminal and abusive behaviour (e.g., harassment, sexual exploitation, fraud, hacking, malware). One of the key aspects of understanding online victimisation and engagement in criminal behaviours is the characteristics of online communication that are related to the affordances of the technologies, services and applications which constitute digital environments. The aim of this paper is to examine the influence of these characteristics on individual and group behaviour, as well as the associated opportunities for victimisation and criminal behaviour. These issues are of relevance for those involved in the design and implementation of technologies and services, as the ability to assess their potential use in this way can enhance strategies for improving the security of systems and users. It can also inform educational strategies for increasing user understanding of potential informational, privacy and personal risks, and associated steps to improve their security and privacy. Each of the main characteristics of mediated communication is examined, as well as their potential impact on individual and group behaviour, and associated opportunities for victimisation and offending. The article ends by considering the importance of recognising these issues when designing and implementing new technologies, services and applications.

1. Introduction

The online environment has become a significant focus of the everyday behaviour and activities of individuals and organisations in contemporary society. The increasing mediation of communication has led to concerns about the potential risks and associated negative experiences which can occur to users, particularly children and young people. This is related to the emergence of the online environment as a location for criminal and abusive behaviour (e.g., harassment, sexual exploitation, fraud, hacking, malware). One of the key aspects of understanding online victimisation and engagement in criminal behaviours is the characteristics of online communication that are related to the affordances of the technologies, services and applications which constitute digital environments. The aim of this paper is to examine the influence of these characteristics on individual and group behaviour, as well as the associated opportunities for victimisation and criminal behaviour. These issues are of relevance for those involved in the design and implementation of technologies and services, as the ability to assess their potential use in this way can enhance strategies for improving the security of systems and users. It can also inform educational strategies for increasing user understanding of potential informational, privacy and personal risks, and associated steps to improve their security and privacy. Each of the main characteristics of mediated communication is examined, as well as their potential impact on individual and group behaviour, and associated opportunities for victimisation and offending. The article ends by considering the importance of recognising these issues when designing and implementing new technologies, services and applications.

2. Characteristics of Online Interactions

Research has examined the characteristics of online communication, how they differ from those of face-to-face (F2F) communication, and their associated influence on individual and group behaviour[1]. This has focused on differences in visual, audio and social cues between online and offline environments, and associated behavioural influences[1]. Social interaction involves the exchange of different communication cues3. These can be verbal (e.g., tone, volume), visual (e.g., facial expressions, non-verbal gestures), or textual (e.g., information communicated in written form)[3,4]. These cues assist interpretation of the content of communication, enabling individuals to determine the motivations and intentions of interactional partners, as well as their trustworthiness and emotional mood. As a result, they are important in determining how individuals respond to each other during social interaction, and cue availability has been found to influence perceptions of social presence in both the offline and online environment[3,5,6]. Social presence is the sense of closeness and immediacy which develops as individuals interact and communicate[3,6]. It is the 'social glue' which enables the development of intimacy and trust, key aspects of the formation and maintenance of social relationships (e.g., personal, family, work)[3,6].

Different types of communication cues have been found to facilitate different levels of social presence in different contexts[7]. Those which convey immediacy between interactional partners are associated with higher

social presence[6]. For example, F2F interaction has been found to result in higher social presence than that which is mediated by technology due to the greater availability of verbal and visual cues, and their ability to convey closeness and immediacy[3,8]. In contrast, research suggests that online interaction is lower in social presence as the result of reliance on textual cues which are less effective at building a sense of immediacy and connection[3,8,9]. Both communication cues and social presence have been found to have an influence on subsequent individual and group behaviour[3,5]. Research suggests that the reduced sense of closeness and intimacy in online interactions is associated with greater expression of uninhibited comments and stronger group polarisation than in F2F interaction[3,9,10]. It can also create difficulties for individuals when interpreting the motivations and intentions of interactional partners, and lead to a psychological distancing effect in which individuals are removed from the impact of their communications and behaviour on others. This is potentially exacerbated by the perceived anonymity of online interactions and identities.

3. **Anonymity and Disinhibition**

Anonymity has been a central focus of research on individual and group behaviour in online spaces[1,2]. The perception of anonymity in digital environments is associated with the potential lack of cues available to attribute an identity to an individual, and there are variations in levels of anonymity related to the use of pseudonyms, technical tools to hide identity and control of personally identifying information[1,11]. This creates an individual or psychological state or perception of anonymity[1]. At the individual level, anonymity can lead to a reduction in inhibitions against behaviours which would be negatively evaluated offline as individuals do not perceive themselves able to be identified or held responsible for their actions[12,13,14]. This online disinhibition effect can lead to increases in aggressive and abusive behaviours [1,2]. An early research focus in this area was on 'flaming' or the deliberate use of hostile textual communication (e.g., aggressive language, negative comments) and specific linguistic formats (e.g., mixed of fonts, capitalisation, colours) to express hostility[2,14], Spears, Postmes, Lea and Wolbert[15] found that anonymity in online interactions led to more flaming incidents than F2F communication. Flaming and aggressive communications have been identified as common behaviours in a variety of online environments (e.g., YouTube, gaming sites)[16,17,18]. This is consistent with research suggesting that lack of F2F interaction and perceived anonymity in the online environment encourages young people to behave in ways that would not be acceptable offline (e.g., harassment, bullying)[19,20]. The potential escalation of flaming and hostility can lead to criminal behaviour in the online environment (e.g., incitement of religious or racial hatred) and offline violence. Online anonymity, particularly when combined with disinhibition, may also encourage users to access illegal content (e.g., indecent images of children, extreme adult pornography), download media files which infringe copyright, and visit sites which are infected with malware. It may also lead individuals to become members of online communities or networks based around deviant or extreme beliefs[21]. Anonymity also provides opportunities for individuals to be deceived and manipulated by others which can lead to harassment, sexual and financial exploitation (e.g., online grooming, online dating scams). These outcomes will be examined in greater detail

in subsequent sections of the paper.

4. Disclosure of Personal Information, Hyperintimacy, Deception

Researchers have also found evidence that perceived anonymity and disinhibition in online interactions can lead to greater disclosure of personal information, faster development of intimacy and more positive perceptions of interactional partners[21,22,23]. As the majority of online communication is textual and asynchronous, individuals have the ability to edit their messages before sending in a way that is not possible in F2F settings[24]. This provides greater control over communications and opportunities to maximise the way in which individuals present themselves and their personal attributes to others[23,24]. This is consistent with research suggesting that individuals communicating online experience more socially desirable interactions than when communicating F2F, and that this leads to the development of more positive interpersonal impressions and relationships[23,25,26,27]. As a result, the hyperpersonal nature of communication may increase disinhibition, as well as the speed and type of personal information disclosed, leading to the intensification of processes of relationship formation. This create opportunities for victimisation, antisocial and criminal behaviour[7,28,29,30]. For example, it may lead to greater identification with interactional partners and their ideological perspectives (e.g., justifications for sexually exploitative behaviour, support for extremist political or religious beliefs), which may increase risk of offending in the online and offline environments.

The development of hyperintimacy, trust and idealised perceptions of interactional partners can also be exploited by individuals to be deceptive about their identity and intentions, and to manipulate others for sexual or financial purposes[31,32,33]. For example, there is evidence that sexual offenders use both identity and intention deception as part of the process of grooming children and young people online[34]. Similar processes of deception are involved in online dating scams in which individuals are contacted and become involved in relationships with offenders who aim to persuade them to part with money[35]. Offenders may use fake profiles and pictures to create attractive personas, and are likely to examine profiles for information indicating potential vulnerability to approach and exploitation[35]. As a result, this involves a process which is similar to the online grooming process. In both forms of victimisation, offenders often spend a significant amount of time developing trust and building a relationship in order to achieve their objectives.

The characteristics of online interactions can also create challenges for detecting deception, particularly the lack of verbal and visual cues which are used to assist in lie detection offline[36]. Their absence potentially reduces opportunities to recognise manipulation and instances in which individuals are being deceived. This is particularly relevant for children and young people who may not have sufficient skills to detect deception, subsequently increasing their risk of manipulation and victimisation.

5. **Anonymity, Deindividuation and Group Behaviour**

Researchers have also examined the influence of anonymity on group dynamics in the online environment. This is particularly relevant given that similar research in F2F settings has identified group polarisation, or an increase in supporting extreme attitudes, as an important influence on group attitudes and behaviour, particularly in group settings characterised by anonymity[1,37]. Sia et al.[3] found experimental evidence of greater group polarisation during online interactions compared with F2F settings, suggesting that such processes are also present in the digital environments.

Research in this area has drawn on established social psychological theories developed to explain individual behaviour in offline group settings1. For example, Zimbardo's[38] deindividuation theory explains the effect of anonymity on behaviour through the creation of a psychological state of deindividuation in which group members do not perceive themselves and others as individuals[39]. This leads to a decrease in self-awareness and evaluation of behaviour which weakens inhibitions against non-normative behaviour (e.g., feelings of shame, guilt, fear) and increases the likelihood of such actions[39]. For example, perceived anonymity in large crowd settings (e.g., football matches) can lead to increases in anti-social behaviour.

Deindividuation theory has been the basis of theories of the effect of anonymity on group behaviour in the online environment[40,41]. Social Identity Deindividuation Theory (SIDE) is partially based on Social Identity Theory which states that individuals have multiple social identities (e.g., gender, ethnicity, religious, political), which are individually are salient or assume greater significance and meaning in specific contexts[42,43]. It also draws on aspects of Zimbardo's theory, with a greater emphasis on situation specific factors and two aspects of components of the effect and use of anonymity in online communication[1]. The cognitive component (effect) focuses on the processes by which group dynamics and individual behaviour is influenced by anonymity and individual identities in online groups[40,44]. Research suggests that anonymity strengthens social identity, the impact of social norms and their influence when an individual identifies with the group and social identity is strong, leading to increased identification with group beliefs and goals, and the expression of more extreme views[40,44,45].

SIDE Theory also specifies a strategic component or the intentional use of anonymity by members of marginalised groups to resist the opinions and goals of a powerful majority group through voicing alternative and potentially unpopular views as a means of achieving group goals[1,41,46]. An example of the strategic use of anonymity in online spaces is demonstrated by a study of the comments posted on an anonymous local newspaper online discussion board about a series of potentially racially-motivated local assaults and a murder in Tacoma, Washington[1,47]. The online space was intended to encourage positive dialogue, but many of the posts were prejudiced, retaliatory and aggressive. This contrasted with the more balanced and conciliatory opinions expressed by the community in a face to face meeting about the crimes[47]. The researchers suggested that online anonymity was strategically used to express opinions which would draw criticisms in F2F contexts due to their prejudiced and aggressive nature[1]. This demonstrates how groups with beliefs or alternative interpretations of events which are seen as unacceptable or characteristic of a minority

group in society can utilise online spaces to comment on or share opinions about events and issues which have an ideological component. The ability to become a member of online communities focused on specific ideologies and / or behaviours which are illegal (e.g., extremist political or religious views, sexual interest in children) can strengthen associated social identities and legitimise their ideological foundations. This may facilitate incitement and planning activities which can subsequently lead individuals to engage in criminal behaviour online and offline (e.g., sexual exploitation, violence, terrorist activities). It can also enable offenders to involved in hacking, creation of malware to form networks in which tools, data or other services can be traded (e.g., Holt, 2013).

6. **Online Behaviours Exposing Individuals to Risk of Victimisation**

The previous sections of the paper have examined the potential influence of the characteristics of mediated communication on both individual and group behaviour. They are also related to engagement in routine online behaviours which may subsequently expose adults and young people to risk of victimisation. Although the majority of research has focused on risky behaviours in relation to young people[48], adults also frequently engage in activities which can potentially increase their vulnerability to exploitation and other negative online experiences. For example, one of the key concerns relating to the potential victimisation of young people is the amount of personal information they post and share online[32]. This is an important aspect of the development of trust and relationships[32], and is also related to hyperintimacy as discussed in a previous section of the paper. Individuals share identity-related (e.g., location, date of birth) or activity-related information, as well as details of emotions and relationships on social media. These details can be used by offenders to identify indicators of vulnerability and to make initial contact with potential victims[49] for the purposes of grooming, dating scams and other fraudulent activities. It can also be used for the purposes of harassment and stalking by individuals, or to guess passwords or utilise social engineering techniques, as well as hacking bank and social media accounts.

Interacting with strangers, making friends and posting images online can also potentially create opportunities for offending and victimisation. Livingstone et al.[48] found that 29% of 11-16 year olds had interacted with someone online with whom they had no prior contact, 36% had accepted friend requests from someone they had never met F2F, and 45% of 9-16 year olds had posted or shared images. There are no equivalent figures relating to the frequency with which adults engage in these behaviours online, but given the popularity of social networking and meeting people online, it is likely that the numbers will be higher. This suggests that a significant number of adults engaging in these behaviours may also potentially be exposed to risk and negative online experiences. For example, posting and sharing images can lead individuals to be victimised through harassment, coercion and blackmail, particularly if they are sexually explicit. Young people making images of this kind available online could also be at risk of sexual approaches, contact and coercion by adults[34]. Research suggests that the more frequently children and young people engage in these different risky online behaviours, the increased likelihood of experiencing sexual approaches, threats and coercion

leading to sexual exploitation[50,51]. This is likely to also be the case for other forms of victimisation (e.g., harassment, deception, stalking, fraud) in both adults and young people.

These behavioural vulnerabilities are the result of the influence of mediated communication on individual and group behaviour. However, vulnerability is a multi-faceted concept which operates at different levels. The online behaviours described above, despite being associated with risk of victimisation, are also routine behaviours associated with communication, the development and maintenance of friendships and romantic relationships etc. This is particularly the case for young people, as online spaces have emerged as an important location in which they achieve developmental tasks associated with identity and intimacy, and the desire for attention and acceptance may lead them to engage in risky online behaviours associated with the potential for online sexual exploitationr[21,32]. Research has also identified psychological (e.g., low self-confidence, social anxiety, depression) and environmental vulnerabilities (e.g., chaotic family situation, parental conflict, divorce) which are associated with this form of victimisation[21,32]. The greater the number of these different factors present in a young person's life, the greater their vulnerability and risk of victimisation. Equivalent psychological and environmental characteristics are likely to be present for some adults, and combine to increase their vulnerability to the different categories of victimisation covered in this paper.

7. **Conclusions**

This paper has examined the characteristics of online communication, how they differ from F2F interaction, and the associated opportunities they create for both victimisation and offending. The online behaviours which users engage in as part of their everyday online activities and interactions potentially create a number of potential risks to their privacy and security associated with a variety of different forms of victimisation (e.g., sexual and financial exploitation, harassment, radicalisation, ID theft & fraud, malware). It also provides access to illegal content and networks involved in deviant or criminal behaviour (e.g., sexual interest in children, extremist ideologies).

The characteristics of online communication can be exploited by offenders in a number of ways to facilitate criminal behaviour. For example, perceived anonymity and lack of visual and verbal cues can be used by offenders to be deceptive about their identity and intentions. Asynchronous communication provides opportunities for the editability and control of the content of communications which enables individuals to maximise their self-presentation to interactional partners and enhance their ability to be deceptive or manipulative. This is further reinforced by the associated hyperintimacy and sharing of personal information by potential victims. Disinhibition can also lead individuals to access content which is illegal and the ability to connect with like-minded individuals can lead to the legitimisation of extreme beliefs or interests which contributes towards offending, as well as membership of online criminal networks.

As a result, the characteristics of digital environments and online communication, together with their

individual and group behavioural influences, have been claimed to create a unique and complex criminal environment[52]. From this perspective, the factors examined in this paper can be characterised as situational crime determinant(s) as the result of their ability to be exploited by offenders to facilitate a variety of types of offending. They also create behavioural vulnerabilities which may combine with other characteristics of individuals to increase their risk of different forms of victimisation. This can be further exacerbated a lack of understanding of potential risks associated with online behaviour and opportunities for victimisation.

This creates a number of challenges for understanding online victimisation, as well as its investigation and prevention. However, the digital data which is generated by online interactions and behaviours are a source of evidence which can be forensically recovered and investigated by law enforcement agencies to identify and apprehend offenders. Forensic device analysis can enable examination of digital crime scenes and provide investigators with information which can be used to identify victims and offenders, as well as specific offence details[52]. In relation to indecent image offending, for example, this can identify evidence of involvement in production and distribution, actions to evade detection (e.g., use of encryption, file deletion), and networking with other offenders[52]. This demonstrates the need for investigators to have an understanding of the behavioural dynamics of online offending, including the influence of the characteristics of mediated communication.

This highlights the importance of recognising how the online environment and communication create these potential opportunities and vulnerabilities, and to consider ways in which these may be reduced through the design and implementation of technologies and applications. These issues are of relevance for those involved in the design and implementation of technologies and services, as the ability to assess their potential use in this way can enhance the security of systems and users. It can also inform educational strategies for improving user understanding of potential informational, privacy and personal risks, and associated steps to improve security and privacy. Prevention messages should focus on the need to consider the potential for certain online behaviours to potentially expose users to different types of victimisation. This includes being careful about the amount of personal information disclosed in online profiles and interactions with others, the potential for deception and manipulation, and the need to use security software on devices and networks.

The online environment is a complex environment in which interactions between the behavioural affordances of the technological infrastructure and individuals create vulnerabilities to victimisation and opportunities for offending. Discussions about cybersecurity often focus on technological vulnerabilities in networks or software which create opportunities for hacking, infection by malware etc., but do not effectively incorporate a consideration of the influence of the characteristics of mediated communication on individual and group behaviour as creating behavioural vulnerabilities which can be exploited by others for criminal or anti-social behaviour. Technical cybersecurity risks can be addressed with appropriate technical solutions or protections, but behavioural vulnerabilities are more difficult to reduce. They rely on the ability of users to be aware of and understand potential risks and vulnerabilities, and to take effective technological and behavioural actions to protect their privacy and security in the online environment. Greater recognition of the

influence of behavioural and other vulnerabilities will enable those involved in developing new technologies and applications, as well as security solutions, to more fully anticipate and mitigate these opportunities for victimisation and offending.

References

1 K. M. Christopherson, The positive and negative implications of anonymity in Internet social interactions: 'On the Internet, nobody knows you're a dog'. Computers in Human Behavior, 23 (2007) 3038-3056.

2 N. Lapidot-Lefler, A. Barak, Effects of anonymity, invisibility, and lack of eye-contact on toxic online disinhibition. Journal of Computers in Human Behavior, 28 (2012) 434-443.

3 C. Sia, B. Y. Tan, K. Wei, Group polarization and computer-mediated communication: Effects of communication cues, social presence, and anonymity. Information Systems Research, 13 (2002) 70-90.

4 J. E. McGrath, (1984) *Groups: Interaction and Performance*, Prentice-Hall.

5 R. Johansen, D. Sibbet, S. Benson, A. Martin, R. Mittman, and P. Saffom, (1991) *Leading Business Teams: How Teams Can Use Technology and Process to Enhance Group Performance*, Addison-Wesley.

6 B. J. Short, B. Williams, B. Christie, (1976) *The Social Psychology of Telecommunication*, John Wiley.

7 L. Sproull, S. Kiesler, Reducing social context cues: Electronic mail in organizational communication. Management Science, 32 (1986) 1492-1512.

8 D. E. Straub, E. Karahanna, Knowledge worker communications and recipient availability: Toward a task closure explanation of media choice. Organization Science, 9 (1998) 160-175.

9 S. Kiesler, D. Zubrow, A. M. Moses, V. Geller, Affect in computer-mediated communication: An Experiment in synchronous terminal-to-terminal discussion. Human-Computer Interaction, 1 (1985) 77-104.

10 J. Siegel, V. Dubrovsky, S. Kiesler, T. W. McGuire, Group processes in computer-mediated communication. Organizational & Human Decision Processes, 37 (1986) 157–187.

11 S. C. Hayne, R. E. Rice, Attribution accuracy when using anonymity in group support systems. International Journal of Human–Computer Studies, 47 (1997) 429–452.

12 J. A. Bargh, K. Y. A. McKenna, The Internet and social life. Ann. Rev. of Psychology, 55 (2004) 573–90.

13 A. N. Joinson, (2007) Disinhibition and the Internet. In *Psychology and The Internet: Intrapersonal, Interpersonal and Transpersonal Implications* (2nd edn) (Gackenbach, J., ed), pp. 76–92, Elsevier Academic Press.

14 J. Suler, The Online Disinhibition Effect. Cyberpsychology & Behavior, 7 (2004) 321-326.

15 R. Spears, T. Postmes, M. Lea, A. Wolbert, When are net effects gross products? The power of influence and the influence of power in computer-mediated communication. Journal of Social Issues, 58 (2002) 91–107.

16 S. Brotsky, D. Giles, Inside the ‘‘Pro-ana’’ community: A covert online participant observation. Eating Disorders, 15 (2007) 93–109.

17 M. Chau, J. Xu, Mining communities and their relationships in blogs: A study of online hate groups. International Journal of Human-Computer Studies, 65 (2007) 57–70.

18 Y. Y. Huang, C. Chou, An analysis of multiple factors of cyberbullying among junior high school students in Taiwan. Computers in Human Behavior, 26 (2010)1581–1590.

19 M. J. Berson, The computer can’t see you blush. Kappa Delta Pi Record, 36 (2000) 158-162.

20 J. Bryce, J. Fraser, “It’s common sense that it’s wrong”: Young peoples’ perceptions and experiences of cyberbullying. Cyberpsychology, Behavior and Social Networking, 16 (2013) 783-787.

21 J. Bryce, (2014) The technological mediation of leisure in contemporary society. In *Leisure in Mind: Meanings, Motives and Learning* (Elkington, S. and Gammon, S., eds), Routledge.

22 K. Y. A. McKenna, A. S. Green, A. S. Gleason, Relationship formation on the Internet: What’s the big attraction? Journal of Social Issues, 58 (2002) 9-31.

23 J. B. Walther, Computer-mediated communication: Impersonal, interpersonal, and hyperpersonal interaction. Communication Research, 23 (1996) 3-43.

24 J. B. Walther, Selective self-presentation in computer-mediated communication: Hyperpersonal dimensions of technology, language, and cognition. Computers in Human Behavior, 23 (2007) 2538-2557.

25 J. A. Bargh, K. Y. A. McKenna, G. M. Fitzsimons, Can you see the real me? Activation and expression of the ‘‘true self’’ on the Internet. Journal of Social Issues, 58 (2002) 33–48.

26 J. B. Walther, Group and interpersonal effects in international computer-mediated collaboration. Human Communication Research, 23 (1997) 342-369.

27 J. T. Hancock, P. J. Dunham, Language use in computer-mediated communication: The role of coordination devices. Discourse Processes, 31 (2001b) 91-110.

28 J. R. Carlson, J. F. George, J. K. Burgoon, M. Adkins, C. H. White, Deception in Computer-Mediated Communication. Group Decision and Negotiation, 13 (2004) 5-28.

29 R. E. Guadagno, B. M. Okdie, F. J. Bernieri, A. L. Geers, A. R. Mclarney-Vesotski, Getting to know you: Face-to-face versus online interactions. Computers in Human Behavior, 27 (2011) 153-159.

30 T. Postmes, R. Spears, M. Lea, The formation of group norms in computer-mediated communication. Human Communication Research, 26 (2000) 341-371.

31 A. J. Baker, (2005) *Double Click: Romance and Commitment Among Online Couples*, Hampton Press.

32 J. Bryce, J. Fraser, Risk perceptions, disclosure of personal information and trust in young peoples' online interactions. Computers in Human Behaviour, 30 (2014) 299-306.

33 K. Y. A. McKenna, J. A. Bargh, Plan 9 from cyberspace: The implications of the internet for personality and social psychology. Personality and Social Psychology Review, 4 (2000) 57-75.

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

35 M. T. Whitty, T. Buchanan, The online dating romance scam: A serious crime. CyberPsychology, Behavior, and Social Networking, 15 (2012) 181-183.

36 A. Vrij, (2000) Detec*ting Lies and Deceit: The Psychology of Lying and its Implications for Professional Practice*, John Wiley and Sons.

37 D. J .Isenberg, Group polarization: A critical review and metaanalysis. Personality and Social Psychology, 50 (1986) 1141-1151.

38 P. G. Zimbardo, The human choice: Individuation, reason, and order vs. deindividuation, impulse and chaos. Nebraska Symposium on Motivation, 17 (1969) 237–307.

39 L. Festinger, A. Pepitone, T. Newcomb, Some consequences of de-individuation in a group. Journal of Abnormal and Social Psychology, 47 (1952) 289–382.

40 M. Lea, R. Spears, D. deGroot, Knowing me, knowing you: Anonymity effects on social identity processes within groups. Personality and Social Psychology Bulletin, 27 (2001) 526–537.

41 R. Spears, M. Lea, Panacea or Panopticon? The hidden power in computer-mediated communication. Communication Research, 21 (1994) 427–459.

42 N. Ellemers, R. Spears, B. Doosje, Self and social identity. Annual Review of Psychology, 53 (2002) 161-186.

43 H. Tajfel, J. C. Turner, (1986) The social identity theory of inter-group behavior. In *Psychology of Intergroup Relations* (Worchel, S. and Austin, L. W.,eds), Nelson-Hall.

44 A. N. Joinson, Self-disclosure in computer-mediated communication: The role of self-awareness and visual anonymity. European Journal of Social Psychology, 31 (2000) 177–192.

45 T. Postmes, R. Spears, K. Sakhel, D. deGroot, Social influence in computer-mediated communication: The effects of anonymity on group behaviour. Personality and Social Psychology Bulletin, 27 (2001) 1243–1254.

46 R. Spears, M. Lea, R. A. Corneliussen, T. Postmes, W. T. Haar, Computer-mediated communication as a channel for social resistance: The strategic side of SIDE. Small Group Research, 33 (2002) 555–574.

47 B. Coffey, S. Woolworth, Destroy the scum, and then neuter their families: The web forum as a vehicle for community discourse? The Social Science Journal, 41 (2004) 1–14.

48 S. Livingstone, L. Haddon, A. Görzig, K Ólafsson, (2011) *Risks and Safety on the Internet: The UK Report*, LSE, EU Kids Online.

49 J. Wolak, D. Finkelhor, K. J. Mitchell, M. L. Ybarra, Online 'predators' and their victims: Myths, realities, and implications for prevention and treatment. American Psychologist, 63 (2008) 111-128.

50 K., Mitchell, D. Finkelhor, J. Wolak, Youth internet users at risk for the most serious online sexual solicitations. American Journal of Preventive Medicine, 32 (2007b) 532–537.

51 M. L. Ybarra, K. J. Mitchell, K. J. How risky are social networking sites? A comparison of places online where youth sexual solicitation and harassment occurs. Pediatrics, 121 (2008) 350–357.

52 M. L. Long, L. A. Alison, M. A. McManus, Child pornography and likelihood of contact abuse: A comparison between contact child sexual offenders and non-contact offenders. Sexual Abuse: A Journal of Research and Treatment, 25 (2013) 370-395.