Child Online Safety and Parental Intervention: A Study of Sri Lankan Internet Users

Hemamali Tennakoon
Sri Lanka CERT|CC
hemamali@cert.gov.lk

George Saridakis
Kingston Business School
G.Saridakis@kingston.ac.uk

Anne-Marie Mohammed
The University of the West Indies
Anne-Marie.Mohammed@sta.uwi

Abstract

Purpose

Today's world of digital and mobile media does not require actual physical contact, between the suitable target and the motivated offender, as with traditional crime. In fact, as Mesch (2009) contends that the internet is not merely an information channel but it creates a new space of activities for children, where they are exposed to motivated offenders and the actors of fourth party. Therefore, for the sake of children's safety, the practice of parental mediation control is increasingly becoming more pertinent everyday. Thus, the major purpose of this paper is to examine how parental mediation control in Sri Lanka is influenced by their internet self-efficacy, their experience as an online victim and their trust in online users.

Design/methodology/approach

This paper uses a unique dataset of computer and internet users from Sir Lanka to examine parental intervention in their children's online activities. Specifically, the dataset contains 347

responses from computer and internet users. To analyze our data we use a binary dependent (probit) model.

Findings

The results show that such factors alter the baseline probability of parental intervention. However, some differences are found between younger and older parents, with the latter group responding more to trust in online users and victimization experience while the former is mainly driven from computer self-efficacy. In particular, the older group is less likely to trust online internet users in terms of never adding unknown persons in the social media. Finally, being self-employed and an older parent has a positive effect on the likelihood of adopting parental controls, possibly because of the non-pecuniary attributes of self-employment.

Originality/value

This study adds to the emerging parental mediation control literature by looking at the likelihood of younger and older parents who were victims of cybercrimes, who have greater internet self-efficacy and lower online third party trust to adopt parental mediation control behaviours. Also another contribution to the literature is the role of occupation type on parental monitoring behaviours.

1. Introduction

The young generation of today is keenly embracing the digital technologies and is rapidly evolving into a new breed of cyber citizens. The rise of the smartphone and the popularization of social networking sites with its applications have contributed significantly to how and when young people engage online. According to recent statistics[1], in 2014-2015, the majority of the children (within the 12-17 age groups) in the UK, US and Australia own smartphones and have used these mobile devices to access the internet. In a 2015 report, the communications watchdog Ofcom reported that young people between the ages of 16-24 spend more than 27 hours on the internet per week[2]. Compared to the previous decade, this is more than double the time spent by young adults online each week. Some have attributed such changes in internet consumption habits to the increase in the use of tablet computers and smartphones (Anderson, 2015). The internet offers many benefits to children and young adults, and these may include opportunities to explore knowledge, share ideas, express themselves, and build relationships. However, similar to the physical world, there are dangers in the online environment. The increased online interactions and the heavy use of online media expose vulnerable individuals and young children to dangers, such as cybercrime. Bryce (2010) pointed out that the greatest threat to children and young people online was sexual exploitation, however, they can also be faced with other online risks such as cyber bullying and exposure to violent online contents.

The anonymity, lack of physical boundaries associated with online environments and "percetual challenges" such as lack of life experience, maturity etc. provide ample opportunities for cyber criminals to target adolescents easily (Pereira et al., 2016). Furthermore, unlike the traditional criminal activities, there is no need for actual physical contact between the suitable

[1] https://www.esafety.gov.au/about-the-office/research-library/aussie-teens-and-kids-online.
[2] http://media.ofcom.org.uk/news/2015/time-spent-online-doubles-in-a-decade/.

target and the motivated offender as Mesch (2009) contended that the internet was not merely an information channel but it created a new space of activities for children. Put differently, it is a new space of social activity consisting of: web pages that present new information, forums that are both moderated and unmoderated, clips and pictures that can be sought and posted, entertainment of online games and the possibilities of interactions with both known and unknown individuals (Livingstone, 2007; Mesch, 2007). Consequently, they can be open to victimization such as online bullying which requires knowledge about the potential victim (Mesch, 2009).

A significant outcome of online victimization is the negative psychological impact there could be on the victim. It has been shown that youth internet victimization could "elevate rates of trauma symptomatology, delinquency, and life adversity" (Mitchell et al., 2011:128). As a result of this, there can be increases in the distress levels of the youths (Mitchell et al., 2016). Hence, the online safety of children has become a significant concern for not just parents but for law enforcement services, policy makers, child protection services and service providers (Bryce, 2010). Parents have a significant role to play in protecting their children online. Ybarra and Mitchell (2004: 1315) pointed out that "parental involvement and monitoring of their children's internet use to ensure safe and appropriate online navigation" was essential. Mesch (2009) found that not all parental mediation techniques could provide adequate protection for children but more parental participation could reduce internet risks from targeting and preying upon the youths.

In other words, the mediation of internet practices among their children is dependent or related to the parenting strategy (Wang et al., 2005; Eastin et al., 2006; Valcke et al., 2010; Lau et al., 2016). Parenting styles can be categorized into four groups: the authoritative, authoritarian,

indulgent and neglectful parenting strategies (Chan and Koo, 2011; Horzum and Bektas, 2014; Ihmeideh and Shawareb, 2014; Kashahu et al., 2014; Chou et al., 2016). Ihmeideh and Shawareb (2014: 411) found in a study involving Jordanian parents that "authoritative internet parenting style was the most commonly used…followed by permissive and authoritarian parenting styles, with the neglectful parenting style being used the least".

Eastin et al. (2006) found that the evaluative strategies of viewing and discussing with their children the contents of the internet were generally practised by parents with the authoritative style. Additionally, they found that the authoritarian and neglectful styled parents tended to resort to restrictive approaches. Furthermore, they found that parenting strategies were a function of age. In particular, parents within the 35-45 years age group were more likely to be practitioners of the authoritative style, those under 34 years the authoritarian style and those over 45 years the neglectful style. However, there are mixed findings with regards to these results within the limited empirical literature. For instance, the findings of Eastin et al. (2006) were verified by Valcke et al. (2010), but Wang et al. (2005) found that it was the older parents who would tend to adopt a strategy based on more control and less guidance.

In this context we seek to ascertain empirically how parental control and risk awareness are influenced by the parents' internet self-efficacy; if they were previous online victims (as an adult/parent) and finally, their trust in online users. To a lesser extent, we also examine the role of occupation type of the parent on the parental behavior in monitoring their child's online activity. Hence, the aim of this paper is twofold: the first aim is to identify how the above factors influence parental control and risk awareness while the second aim is to highlight policy suggestions that would encourage effective use of parental control in promoting online safety for children.

The rest of the paper is structured as follows. Section 2 discusses prior work and extracts the research hypotheses of this paper. Section 3 describes the data and the statistical framework adopted in this paper. Section 4 presents the results. Section 5 discusses some key recommendations and policy implications that arise from our results. Section 6 discusses the limitations of this study and provides future directions of research. The final section concludes the paper.

2. Background and hypothesis development

Henson et al. (2011) found that most studies on "online interpersonal victimization" focused on young individuals and on harassment, sexual solicitation online and cyberstalking victimizations. They also found that some of the online initiated victimization could have transcended into the offline environments. For example, the literature finds that there is an overlap between cyberstalked victims and those who are stalked in the physical world (see also Didden et al., 2009; Dilmac, 2009). Furthermore, Wurtele and Kenny (2010) found that age and gender were the key parameters in determining online victimization. They also found evidence of a positive relationship between the ages of the victims, specifically, as the children's ages increased, so did the likelihood of victimization increase while, additionally, girls were found to be more vulnerable to internet-initiated sex crimes. The report of EU Kids Online survey by Livingstone et al. (2011) identified the online risk types that were prevalent for European children such as: pornography, bullying, sexting, and meeting online contacts offline. Additionally, the report highlighted both parental awareness and parental mediation (or lack of) as important indicators of the online safety of the children, for instance, and most importantly, Hinduja and Patchin (2007) found that as a consequence of cyberbullying victimization there were school problems

and delinquency which had negative implications for adolescent development. Furthermore, Van Geel et al. (2014) showed that cyberbullying, just as much as traditional bullying, was also strongly related to suicidal ideation. Thus, the risks associated with online usages are serious and as such parenting mediation is of paramount importance in today's world of the digital and mobile media, "defined as mobile phones, laptops with internet connection, and other devices that deliver entertainment such as television programming, films, games, and music that have indelibly …changed the landscape of family media use" (Clark, 2011:324). Hence, there has been a drastic change in the role of the media in the home.

Parental control and mediation enable parents to monitor the online activities of their children and the people whom they associate with both online and offline (Dishion and McMahon, 1998: 33). According to Sasson and Mesch (2014) "control refers to parent initiated efforts to control their youngsters' behaviours through rules and restrictions". Existing research shows that parental mediation has a positive effect in terms of reducing the children's risky online activities. For instance, Livingstone et al. (2011), who studied children and their parents from twenty-five European countries with regards to risks and safety online, found that talking to children was the most popular method used in Europe to mediate their children's internet use actively. This is in line with the "Parental Mediation Theory" which posits that "parents utilize different interpersonal communication strategies in their attempts to mediate and mitigate the negative effects of the media in their children's lives" (Clark, 2011: 325).

The parental mediation theory grew out of the concern surrounding the negative impacts of the media on the lives of their children. These interpersonal communication strategies which can be both social and technical can be broadly classified into two approaches: active or restrictive (Chang et al., 2016). For instance, Livingstone et al. (2011) found that parents block,

filter and track websites visited by children as a way to mediate their children's internet use actively, while simultaneously, talking and communicating with them about the dangers of the internet. Thus, active mediation is about communication and discussions or even being in close vicinity, therefore, it is a process that is bidirectional, which enables their children to become more critical of the contents of the internet (Fleming et al., 2006; Clark, 2011; Padilla-Walker and Coyne, 2011). Additionally, it has been found to be effective in reducing internet addictions and exposures to the risks associated with online usages without compromising the opportunities that are available online. Even more, it reduces the negative impacts on children when they actually encounter such risks (van Den Eijnden et al., 2010; Duerager and Livingstone, 2012). Interestingly, Mesch (2009) found that cyberbullying was reduced only when parents laid down the rules as to which website they were allowed to visit. He called this evaluative parental mediation, however, in the context of our broad two classifications, this type of mediation falls within the active parental mediation strategy. Navarro et al. (2013) also found such a form of restrictive parental mediation to be effective, while both studies found that the setting up of monitors had a positive effect on the reduction of cyberbullying.

As the names imply, restrictive mediation seeks to regulate the online activities of the children through the enforcement of rules that control the time spent online, the contents viewed, files that can be downloaded and the social network sites that are visited through blocking, filtering and tracking the websites (Clark, 2011). This strategy tends to be one of last resort in the cases where apparent internet addiction is negatively affecting the children's performances academically and their interpersonal relationships (Lee, 2012). It has the effect of reducing both the amount of time spent on the internet (Chang, and Cheng, 2009; Valcke et al., 2010; Lee and Chae, 2012) and the negative impacts from the consequences of encounters with online risks

(Duerager and Livingstone, 2012). Nevertheless, its effectiveness decreases as the child gets older (Nathanson, 2002; Livingstone and Bober, 2006). Mesch (2009) utilized a sample consisting of both parents and teenagers to find that restrictive mediation actually decreased the odds of being cyber victimized.

Gender is a factor that should be taken into account when considering the use of parental mediation strategies as the literature acknowledges that there are significant differences between the online activities of boys and girls (Lau andYuen, 2013). For instance, with regards to risky online activities Lau and Yuen (2013); Notten and Nikken (2014) found that personal information was more likely to be disclosed online by boys. Furthermore, these researchers also found that there was a greater tendency for boys to engage in online activities that were risky. Madden et al. (2013) found that boys who used Facebook had a greater tendency to have public profiles. Hence, their response to parental mediation strategies may have been different, for example, in cases of cyberbullying, Wright (2017) found that girls responded to restrictive parental mediation more positively than boys, with the opposite being true for active or instructive mediation. However, Heirman et al. (2015: 274) found that in classroom settings, gender and ethnic composition did not have a significant influence on cyberbullying and argued that schools "should not primarily take these aspects into account in developing their policy against cyberbullying".

Online risks examined in past research include cyber bullying (Kamali, 2015; Del Rey et al., 2016), cyber stalking (Beech and Bishop, 2015; Winkelman et al., 2015; Goel et al., 2016), exposure to pornographic and violent content (Romito and Beltramini, 2015; Chang et al., 2016), online fraud (Cross, 2015; Whitty, 2015), hate speech (Näsi et al., 2015) etc. However, the types and the nature of these risks are constantly evolving andwhether the awareness of the user

develops to match the developing variations in the online threats is unclear. In the context of e-commerce exchanges, it has been found that "risk awareness reduces the level of trust between the retailer and the consumer" (Olivero and Lunt, 2004: 243). It has been pointed out that providing awareness and avoidance skills is one of the best prevention and treatment methods that can be used against online sexual predators and victimization of young children (Wolak et al., 2011). Interesting research questions, therefore, are what factors determine parental awareness and what monitoring measures can minimize the potential risk of a child's online activity? This paper argues that parents' online victimization experiences may increase awareness and cause monitoring of a child's online activity.

Staude-Müller et al. (2012) found that prior experiences of online victimization correlated with greater distress. Even more, and in the context of this study, both qualitative and quantitative studies have revealed that there is quite a range of negative psychological symptoms that may manifest on the victim as a consequence of online victimization such as cyber bullying, especially when it is more intense and of a longer duration (Hinduja and Patchin, 2007; Raskauskas and Stoltz, 2007; Cassidy et al., 2009; Spears et al., 2009; Ortega et al., 2009; Raskauskas, 2010; Wang et al., 2011; Ryan and Curwen, 2013). These include depression (Raskauskas, 2010; Wang et al., 2011), social anxiety (Dempsey et al, 2009), somatic symptoms (Gradinger et al., 2009), both low self-confidence and self-esteem and suicidal ideation (Ortega et al., 2009; Price et al., 2010). Furthermore, there can also be behavioural issues such as falling attendance and grades in schools and declines in the family relationships (Beran and Li, 2005; Price et al., 2010) Thus, online victimization can have serious consequences on the victim and it would be quite rational to expect that such parents who were victims would not want that to happen to their children. Hence, they would be more than likely to be practitioners of parental

mediation strategies as they would have felt the pain and so would not want such an experience to happen to their children. Meter and Bauman (2016) found that parental mediation was more prevalent among youths who engaged in cyberbullying. They alluded this finding to the view that when parents became aware of such activities they would try to prevent their repetition and to educate their children about the safe use of online technologies. Similar findings were recorded by Sasson and Mesch (2017) who showed that such parents would, in particular, resort to supervisions both social and technical. Thus, we expect that parents who are aware of the negative effects of cyberbullying because they themselves were victims, would take the necessary steps to prevent the same from happening to their children. We can perhaps draw upon the theory of reasoned actions to form the framework of this hypothesis.

Finally, Hoschold (1989) put forward the view that emotions were deeply embedded in the social fabric of the individual and the literature states that the negative emotions as a consequence of being an online victim, especially a cyberbully victim, are traumatic and long lasting. Thus, assuming they are rational or good parents, they will not allow their children to experience such and this intent will be deeply embedded in their social fabric. On the other hand, the theory of reasoned action (Ajzen, 1985; Fishbein and Yzer, 2003) as applied to the parent may imply that that parents' behavioural intent of not allowing the same fate to fall upon the child, would be more likely to engage in parental mediation strategies. In other words the theory premises that the behaviour of the parents would be governed by their pre-existing attitudes, namely the trauma of being among the victimized: "… their decision making when it comes to media overwhelmingly involves their emotions, and specifically their feelings about parenting and about their children" (Clark, 2011:330).

Given all this, we therefore, propose the following hypothesis:

H1: Parents who have been victims of internet crime will be more likely to monitor their children's online activities.

According to Eastin and LaRose (2000:1), internet self-efficacy is "the belief in one's capabilities to organize and execute courses of internet actions required to produce given attainments." Internet self-efficacy must not be confused with computer self-efficacy (Eastin and LaRose, 2000; van Deursen et al., 2015) as it requires the mastery of additional skills (Warschauwer, 2003; Litt, 2013; van Dijk and van Deursen, 2014). These additional skills are known as digital skills (Livingstone et al., 2017). The concept of digital skills is not fully defined; it is sometimes referred to as technical efficacy (Anderson and Agarwal, 2010).[3] However, it incorporates not only technical skills as required in computer self-efficacy but also critical, creative and social skills which enable the participant to employ communication and content creation technologies for social purposes (Helsper and Eynon, 2013; van Deursen and van Dijk, 2014; van Deursen Van et al., 2015). Thus, acquisition of the combination of these skills engenders internet self-efficacy. The world today as previously stated in this paper, is an environment that is media-rich and technologically innovative. Hence, not only society but parents in particular are required to ensure that their children are in sync with the times and at the same time protected from the numerous online risks (Livingstone et al., 2017). One of the major risks and potential sources of harm associated with the advent of social networks is the voluntary disclosure of personal information (Lowry et al., 2011; Conger et al., 2013; Jiang et al., 2013; Benson et al., 2015). Such information disclosures can be used by both third party individuals and even organizations to the detriment of not only the children, but also their families: "The possibility of real on time monitoring and eavesdropping, aggravates the problem, by exposing

[3] However, in this research, the survey questionnaire included items pertaining to both internet and computer self-efficacy. Therefore, both will be considered under self-efficacy.

individuals to potential harassment and flaming, or even more extreme forms of aggravation such as stalking and sexual abuse" (Jiang et al., 2013:579).

These online risks are a consequence of the various online actors. For instance, the expanded personal information privacy (PIP) model of Benson et al. (2015) illustrates that there are four sets of parties or actors within the social networks and the fourth party includes the malicious actors or the individual criminals. It is premised that internet self-efficacy will enable both the understanding and awareness of the various actors or parties that can be sources of risks on the social networks. Nevertheless, online crime does not occur randomly, but instead has a pattern that is regular, namely, according to the routine activity theory, there are three components (Marcum et al., 2010). This theory, as developed by Cohen and Felson (1979), states that for a crime to occur there must firstly be motivated offenders, secondly, suitable targets and thirdly, the lack of guardians that are capable of preventing this crime. Specifically, the motivated offender belongs to the fourth party as mentioned before, and is the individual who has the willingness to commit a crime, once the other two components are lacking (Cohen and Felson, 1979; Mustaine and Tewksbury 2002). On the one hand a suitable target is the child without the necessary precautionary measures which ensures protection. On the other hand, and in the context of this study, a capable guardian is the parent with the ability to prevent the occurrences of such online crimes (Tseloni et al., 2004). Simply put, this theory implies "…that if a motivated offender is presented with a suitable target that is not properly guarded against victimization, a crime is likely to occur" (Marcum et al., 2010:385). The literature has validated the applicability of various models of the routine activity theory to online criminal activities and risks (Marcum et al., 2010; Popp and Peguero, 2011; Reyns et al., 2011; Navarro and Jasinski, 2013; Ouytsel et al., 2016) and it has even been extended into the cyber lifestyle-routine

activities theory as both parties i.e. the victims and the offenders, need not be within the same space and time (Reyns et al., 2011).

Therefore, it stands to reason that parents who are capable guardians as they possess sufficient digital skills which then manifest as internet self-efficacy will be in a better position to prevent their children from being victims of online crimes (Duerager,and Livingstone, 2012). Research suggests that high parenting self-efficacy is associated with greater levels of parenting competence which together increase the likelihood of positive child outcomes (Jones and Prinz, 2005; Crncec et al., 2010; Wong et al., 2015). For example, Blaya and Alava (2012) reported that 47% and 46% of the 9 to16 year olds in France who responded to an online survey reported that their teachers showed them how to use the internet safely and which websites were good or bad. Thus, we can premise that parents with internet self-efficacy will be as knowledgeable as the teachers in the Blaya and Alava (2012) report. In other words, they will have the awareness of not only the potential risks as a result of the actors within the social network that can result in online exploitations but also the technical capacities to block, filter and track online activities in order to protect their children when online. Interestingly, Horzum and Bektas (2014) labelled parents who were late or not up to date towards developing their digital skills as digital immigrants, while van den Eijnden et al. (2010) found that parents without digital skills were much less likely to manage the online activities of their children effectively. Mesch (2009) stated that there was a human element in guardianship, but capable guardianship by the parent implied a degree of digital skills which in turn manifested as internet self-efficacy.

Therefore, we forward our second hypothesis that:

H2: Parents with higher internet self-efficacy will be more likely to control their child's online activity.

Grabner-Kräuter and Bitter (2015: 51) described trust as a situational, cross-situational, and cross-personal construct "encompassing individual characteristics of the trustor". Further, they argued that over time, as people developed, their disposition to trust or their trustworthiness towards other people, technological systems and social networking sites changed. McKnight et al. (1998) found that dispositional trust towards others was higher in unfamiliar situations. Hence, Grabner-Kräuter and Bitter (2015) argued that this strongly influenced less experienced social network participants in terms of their trust towards other participants in the online social network. Researchers have explored whether there is an association between what is being posted online and who has access to this information. Henson et al. (2011) posited that risk of victimization did not depend on the type of information posted online but instead on the trustworthiness of the individuals who had access to this information. This has been confirmed in a previous study by Wolak et al. (2008) who found that it was the adding and the interacting with unknown people on social networks that increased online victimization and not the sharing of personal information nor the use of social networking sites.

There is a direct relationship between the parenting styles and trust (Meyers and Gilbert, 2012; Meehan and Hickey, 2015), and in the context of parenting mediations we draw upon the conceptualizations of sociological trust: "…of technically competent performance and … of fiduciary obligation and responsibility" (Barber, 1983:165). Here, trust is a process that evolves over time as it is dynamic, context-dependent and conditional (Gubbins and MacCurtain, 2008; Castelfranchi and Falcone, 2010). Furthermore, it is always an element of calculated risk

associated with trust and once the risks are too great the individuals and, in the context of this study, the parents will abstain from trusting. From a psychological perspective which focuses on interpersonal relationships, trust is seen as: "expectancy held by an individual or a group that the word, promise, verbal or written statement of another individual or group can be relied on" (Rotter, 1971:443), while social capital and network theory sees trust as; "… a belief or expectation about the other (trusted) party, or as a willingness to rely on another party, coupled with a sense of vulnerability or risk if the trust is violated" (Grabner-Kra¨uter, 2009:506). Based on these perspectives and especially the social capital and network theory, unknown persons or third parties can be seen as social capital which has a preventative and mitigating factor against children's online threats and harm. Thus, in the presence of such, the parental anxiety levels will be reduced and by extension the degree of parental controls. We argue that if a parent has higher levels of trust in online users, he or she can add an unknown person to social media and is quite likely to feel less worry about potential threats to his or her child during online use.

Hence we hypothesize that:

H3: Lower trust in online users (e.g. add only known people to social media or open an email from a known person only) increases parental control and risk awareness in a child's online activity.

3. Data and statistical model

A questionnaire was used to collect data from the target population. The original questionnaire was developed to assess the cybersecurity awareness of Sri Lankans who attended a national ICT exhibition held in the capital city, Colombo. The first part of the questionnaire contained several demographic questions including gender, age, education, and occupation. In the second part of

the questionnaire, the respondents were asked to provide information regarding their Internet usage. This included questions on number of years of Internet use, purpose for using the Internet, and whether they have been victims of online bullying, stalking, identity theft etc. Then, the respondents' knowledge about safe internet and computer usage was measured using several questions. The questions focused on their knowledge about firewalls, opening email attachments, email scams, anti-virus software, password management, privacy controls on social media, reporting cyber-crime and knowledge about activating parental controls. The questions were newly developed to suit the expected audience at the ICT exhibition.

The initial questionnaire was developed in English and then translated into Sinhala (native language). Printed copies were obtained from both versions. The sample of this study was drawn from a population of internet users in Sri Lanka. To collect the data a convenience sampling approach was used which targeted individuals who visited the exhibition held for the general public over a 3-day period in Colombo, Sri Lanka. Those who took part in the survey were individuals who visited a stall set up by a government agency to educate the public on cybersecurity issues. Individuals who showed interest in completing the survey were provided with either the English or Sinhala (native language) version of the questionnaire. 160 responded using the English version of the questionnaire while 221 used the translated Sinhala version. In total, the dataset amounted to 347 responses from computer and internet users in Sri Lanka. From the 347 respondents, 54% were parents.[4] Since the current study is focusing on parental control and online victimization, the following analysis is based on 186 Sri Lankan parents who use computer and internet (and have answered the subsequent question: Have you ever taken

[4] The survey does not provide information about the origin of the parents. However, even though it is not reported here, we find that speaking either English or Sinhala does not explain the differences in parental control.

measures to ensure that your child is safe online?).[5] 41.40% of the parents reported that they had taken measures while 58.60% reported no measures or trusted their child to be safe online.

In this paper we are interested in the factors that influence whether a parent monitors his or her child's online activities. Since the response variable is binary (taking the value of 0 if no measures have been taken and 1 if parental measures have been taken to monitor the child's online activity), we use a probit model. Unfortunately the survey does not allow us to distinguish between different parenting styles as has been suggested in previous work (Chan and Koo, 2011; Horzum and Bektas, 2014; Ihmeideh and Shawareb, 2014; Kashahu et al., 2014; Chou et al., 2016). Hence, we denote p_i^* as the unobserved (latent) variable *and* X_i as a row vector of individual characteristics such as: the individual's online victimization experience (i.e. whether or not the parent has been a victim of any type of online victimization), computer self-efficacy (captured by knowledge of basic computer protection skills for example ability to identify email scams, installation of firewall and antivirus in the computer and knowing where to report incidence of cybercrime), user's online trust (i.e. whether unknown persons are added in social media or emails from unknown persons are opened) and various individual controls (gender, age, education, occupation, years of online usage and content value for hackers). Table 1 presents summary statistics of the variables used in this study.

Our latent variable model can be simply written as:

$$p_i^* = \beta' X_i + \varepsilon_i \quad (1)$$

$$p_i = 1 \text{ if } p_i^* > 0 \quad (2)$$

$$p_i = 0 \text{ if } p_i^* \leq 0 \quad (3)$$

[5] Those who are not parents (161 individuals) were not asked whether they had ever supervised children during their online activity and if so how they had ensured their online safety. Future research should seek to compare family and non-family groups and examine whether levels of children online supervision and adult intervention differ between them. Also, it will be interesting to extend the analysis to broken families and single-parent families.

To compute estimates of the coefficients (βs) and their associated standard errors, maximum likelihood techniques are used. Since the estimated coefficients are related to the latent variable p_i^*, they cannot be interpreted in the same way as the normal regression coefficients. For this reason we report marginal effects at the sample mean values of the regressors. Since we have only binary independent variables, the marginal effects measure discrete changes.

Table 1. Summary statistics (%)

Dummy variables	All	a) Parental monitor is used	b) Parental monitor is not used
Parental monitor is used (Dep. variable)	41.398		
Victim of online crime	82.796	84.416	81.651
Able to identify scam email	50.000	**64.935**	**39.450**
Antivirus is enabled	85.484	*90.909*	*81.651*
Firewall is enabled	74.194	79.221	70.642
Aware of online crime reporting	46.237	**58.442**	**37.615**
Open emails only from known persons	48.387	**62.338**	**38.532**
Never add unknown person in social media	47.849	46.753	48.624
Male	83.333	85.714	81.651
Under 26	52.151	**66.234**	**42.202**
26-35	19.355	**10.390**	**25.688**
36-45	13.978	11.688	15.596
46-55	9.677	6.494	11.927
Above 55	4.839	5.195	4.587
School or some school qualification	41.398	37.662	44.037
University qualification	39.785	40.260	39.450
Professional qualification	18.817	22.078	16.514
Student	39.785	44.156	36.697
Public sector employed	19.355	*12.987*	*23.853*
Private sector employed	26.344	25.974	26.606
Self-employed	9.140	12.987	6.422
Unemployed	5.376	3.896	6.422
No content value to hackers	40.323	42.857	38.532
Less than six years online experience	32.796	29.870	34.862
Observations	186	77	109

Figures in bold (italics) indicate statistically significantly different percentages between group (a) and group (b) at the 5% (10%) level.

4. Empirical results

In this section we present the results of modelling parental control of a child's online activity. The results are given in Table 2. The explanatory variables of interest are parental victimization experience, self-efficacy and trust in online users. Model 1 presents the results of the full sample. The results of the full sample found some support for computer self-efficacy and parental control of the child's online activity. In particular, we found that parents who were able to identify spam emails were more likely to undertake protective measures for online use for their children. The probability increased by 18.7 percentage points. Similarly, the probability of parental control increased by 20.2 percentage points when parents were aware of institutions to report cybercrimes. We also found strong evidence that parents with less trust of online users, such as opening email only from known users, were also more likely to monitor the child's internet experience. Hence, we found some support for hypotheses 2 and 3. However, we failed to find any association between parents' online victimization experience and parental control. The results also suggest significant effects of age, with older parents being less likely to control their child's online activity than younger parents.

To explore the age result further, we re-estimated the model individually for younger (i.e. less than the age of 26) and older (i.e. above the age of 26) parents and these results were interesting. Looking firstly at the younger parents' results we found that the results followed a similar pattern to that of the full model. We tested whether there was a change in the magnitude of the coefficient of "Able to identify scam email" (Prob.>x^2= 0.189), "Aware of online crime reporting" (Prob.>x^2=0.242) and "Open emails only from known persons" (Prob.> x^2=0.199), but we found no statistical differences in the reported coefficients of Model 1 and Model 2. However, when we turn to the older parents' sub-sample (Model 3), the results are more

interesting. Prior victimization experience was found to have a significant effect on parental control, with those who were previously victimized being more likely to monitor their child's online activity (ME=0.212). Perhaps, older parents, having lived longer, may have experienced both a longer duration and intensity of cybercrimes, which most likely would have resulted in both negative psychological symptoms (Cassidy et al., 2009; Spears et al., 2009; Ortega et al., 2009; Raskauskas, 2010; Wang et al., 2011; Ryan and Curwen, 2013) and behavioural issues (Beran and Li, 2005; Price et al., 2010). We also found that being aware of online crime reporting institutions[6] and having less trust on online users both increased the probability of undertaking measures for safer online experience of children.

Trust becomes an even more important aspect of this group since it is found that trust spreads across email and social media usage. Hence, for this sub-sample estimates, all of our three hypotheses are supported. The results for this age group lend support for the findings of Wang et al. (2005) but not those of Eastin et al. (2006) and Valcke et al. (2010). In particular, Wang et al. (2005) found that it was the older parents who tended to adopt a strategy of greater control and less guidance; a greater tendency towards an authoritarian style. According to Ponte and Simões (2009), it was the older parents rather than the younger ones who were more likely to be digitally excluded. Low usage leads to lack of understanding of the internet and such parents are likely to have more concerns over their children visiting certain websites, buying online, befriending strangers etc. Hence, older parents may impose stricter parental control over their children's online behaviour which explains our findings. Put differently, older parents are more likely to be late or not up to date towards developing their digital skills and as such be digital immigrants (Horzum and Bektas, 2014). Therefore, they are less likely to have the guardian

[6] We tested the equality of the two coefficients from Model 2 and Model 3 and found that the equality hypothesis could not be rejected (Prob. x^2 =0.272).

capabilities that result from internet self-efficacy, so it may be beyond their means to carry out an active parental mediation strategy. Such a strategy entails having the digital skills to block, filter and track the websites that they visit, engaging in discussions with their children and co-use, hence, the resort to a very restrictive strategy that consists of simply laying down the rules with strict adherence. However, this result is in sync with the findings of Kashahu et al. (2014) who found that such parents over the age of 45 tended to practise an authoritarian style, but furthermore, their results showed that this was the least educated group. Therefore, this is another reason why their digital skills, that enable capable guardianships, are not adequate.

The results also give some tentative support that younger parents may possess greater self-efficacy as they are more able to identify scam email, less likely to be victims of internet crime and as such will have lesser trust or resort less to social capital networks.

The notion that it is the women rather than the men who assume the responsibilities of controlling and guiding the technological usages of the children is supported by the results which show that the males are less likely to monitor children's online activity compared to female parents. In particular, this tendency is the greatest for the males over the age of 26 years. Similarly, results of the female parents taking greater responsibilities in terms of guidance and control of the children's online activities as evidenced in our results in terms of the negative and significant male marginal effect were found by Wang (2005); Dholakia (2006); Lim and Soon (2010); Valcke et al. (2010) and Lau and Yuen (2016). On the whole, the literature reveals that the authoritative parenting style is generally practised by mothers while fathers tend to opt for the authoritarian style (Aunola et al., 2000).

Strangely, the educational level of the parents, whether male or female, was not a significant predictor of parental control and even more, the coefficients were negatively signed,

suggesting an inverse relationship, however, the correct sign as in accordance with the literature was found in the model with the older parents. The literature regards the educational levels of the parents as one of the three dominant predictors influencing the usages of the internet by children (Lau and Yuen, 2016). For example Sun et al. (2005) found that there was a positive association between the educational levels of the parents and home internet usage by their adolescent children. While, the empirical literature found a positive relationship between the educational level of the parents and control and guidance of their children's online activities (Wang et al., 2005; European Commission, 2008; Valcke et al., 2010; Álvarez et al., 2013). Interestingly, and in the context of our results which did not find the educational level of the parents to be significant, Özgür, (2016) found that mothers who were both younger and more educated exercised greater online guidance and controls.

Finally, we find that being self-employed increases the likelihood of monitoring a child's activity on the internet compared to private sector-employed. This can be explained to some extent by the "working mother" hypothesis or "mother absent" hypothesis. It is argued that when mothers work outside the home, they are less able to provide supervision and socialize with their children, thereby affecting their development and behavior (Hill and Duncan, 1987). McLanahan (1985) presented a similar argument for absent fathers. Hence, one could argue that self-employed parents are more available to their children, can monitor their behavior better and provide guidance where necessary as opposed to parents who are employed. Further, self-employed parents are more likely to use online technology and thus are more aware of potential threats that internet usage experience may have.

Table 2. Probit estimates (marginal effects)

Model:	Model 1		Model 2		Model 3	
	Full Sample		Parents under the age of 26		Parents above the age of 26	
	ME	Robust Std. Err.	ME	Robust Std. Err.	ME	Robust Std. Err.
Victim of online crime	0.054	0.106	-0.039	0.162	0.212*	0.085
Able to identify scam email	0.187**	0.084	0.241*	0.124	0.090	0.111
Antivirus is enabled	-0.005	0.141	-0.075	0.193	0.075	0.135
Firewall is enabled	0.074	0.094	0.078	0.132	-0.054	0.128
Aware of online crime reporting	0.202**	0.087	0.230*	0.125	0.191*	0.115
Open emails only from known persons	0.205**	0.079	0.235*	0.117	0.170*	0.096
Never add unknown person in social media	0.053	0.084	-0.075	0.128	0.271**	0.094
Male	0.058	0.108	0.163	0.143	-0.328*	0.197
Under 26						
26-35	-0.414**	0.072	-	-	-	-
36-45	-0.275**	0.111	-	-	-	-
46-55	-0.294**	0.103	-	-	-	-
Above 55	-0.134	0.149	-	-	-	-
Education (School or some school qualification)						
University qualification	-0.084	0.093	-0.152	0.123	0.064	0.160
Professional qualification	-0.007	0.131	-0.248	0.204	0.086	0.165
Occupation (Private sector employed)						
Student	-0.148	0.127	-0.260	0.213	-0.103	0.155
Public sector employed	-0.131	0.114	-0.210	0.270	-0.134	0.101
Self-employed	0.160	0.172	-0.066	0.394	0.298*	0.190
Unemployed	-0.247	0.121	-0.355	0.224	-0.095	0.157
No content value to hackers	0.039	0.085	-0.025	0.123	-0.115	0.101
Less than six years online experience	-0.125	0.096	-0.167	0.127	0.025	0.164
Wald chi2(20)	44.44**		27.57**		30.26**	

Wald chi2(16)			
Log pseudo likelihood	-101.311	-54.922	-39.907
Pred. probability	0.388	0.526	0.217
Observations	186	97	89

**Statistically significant at 5% level. *Statistically significant at 10% level.

5. Recommendations

Based on the findings of our study, there are several strategies that can be recommended to parents who seek to enhance the online safety of their children. Authoritarian control with less guidance is seen prominently in the older parents in this current study. Instead of employing this type of control, it might be better to apply as recommend by Nikken and Jansz (2014), similar strategies that are used for television and video games such as "co-use", "active mediation", and "restrictive mediation". However, Livingstone and Helsper (2008) argued that active co-use and software-based monitoring/filtering did not effectively reduce online risks for children. Instead, Livingstone and Helsper (2008) recommended the development of safety guidelines aimed at parents and teenagers, while Nikken and Jansz (2014) proposed strategies such as the "supervision" and development of "technical safety guidance". To provide the latter, parents could use the "active mediation" strategies as proposed by Lwin et al. (2008).

Parental control and monitoring may not be possible in all aspects of internet usage by children. For example, Chou et al. (2016: 211) argued that parents "may not be able to successfully supervise or control children's online game playing", but neglecting such needs of children could lead to adverse consequences such as gaming addictions. In addition to that, such behaviour could also expose young children to other online threats (e.g. online predators, violent content). Horzum and Bektas (2014) found that the right parenting style could determine how the children would use the internet. For instance, children subjected to authoritative internet parental style increasingly used the internet for research and educational purposes. Children of parents who used a laissez-faire style mainly used it for entertainment purposes. Therefore, one could suggest a parenting style that supports the children's internet use but with some parental control.

Finally, the following policy recommendations can be introduced to enhance online safety of children that are in line with the research findings. In a report titled "EU Kids Online", Livingstone and Haddon (2009) provide several policy recommendations that are applicable to the current research context. For example, the researchers recommend the introduction of e-inclusion policies to incorporate under-represented groups such as those from less well-off households and parents who are not online. This is a highly relevant recommendation in a Sri Lankan context where the internet penetration rate is on the increase. Children are increasingly using mobile devices to access the internet while not all Sri Lankan parents are internet users, especially those living in non-urban areas. Another recommendation would be to promote online safety education at the school level where children can be empowered to understand and mitigate online risks. This is in line with Atkinson et al. (2009) who suggest promoting e-safety via peer education.

6. Study limitations and future directions for research

Given the small sample size used in this study, our results should be interpreted with caution and a larger-scale work is required to explore the relationships further. Having this in mind, the implications of this study are mainly two fold. Firstly, it establishes the fact that prior online victimization experiences affect individuals adversely not just in the short term, but also affect their future decisions. For instance, individuals who have been victimized by cybercrime tend to control not only their individual futuristic behaviours but in addition, that of their children. Current research findings are limited in three aspects: (1) findings are characterized by younger and older parents, (2) "cybercrime victimization" is considered as a broader concept, and (3) demographic variations in children were not considered (e.g. gender, age). Hence, further

research could focus on 2-parents/single-parents (since parenting style can vary based on family structure) (Chan and Koo, 2011), parents who are millennials and their parenting style in controlling children's internet usage, nature of the prior cybercrime victimisation of the parent and how it would influence parental control, and variations in parental controls based on children's ages (e.g. young-adults, teenagers etc.).

Krcmar and Cingel (2016) found significant differences between parents from the United States (US) and the Netherlands in parents' mediation of their adolescents' social media use. Compared to developed countries such as the US and Netherlands, Sri Lanka has a lower internet usage. In 2016, only 27.4 % of the total population used the internet[7] while the "overall computer literacy reported in the first half of 2015 for Sri Lanka was 26.8%"[8]. According to the Department of Census and Statistics of Sri Lanka, the country is "still not a fully-fledged computer user. Therefore, it is not possible to adopt definitions on computer literacy used by developed countries"[9]. Therefore, generalizing or comparing the findings of the current research with other countries should be done with caution. The limited sample size and the inability to compare the results with other cultures and nationalities provide room for further research.

Self-efficacy in the current study is limited to computer related self-efficacy. However, there are other forms of self-efficacy. For instance, parents who are working in the IT industry or engaged in IT/computer related occupations will have a higher computer efficacy based on their formal computer training. As an example, a parent who is professionally engaged in work that is related to cyber-crime may have superior knowledge of cyber-crimes and victimisation. Due to their professional exposure to cyber-crime (and not necessarily due to personal experience as a

[7] http://www.internetworldstats.com/asia/lk.htm
[8] http://www.statistics.gov.lk/samplesurvey/ComputerLiteracy-2015Q1-Q2-final%20.pdf
[9] http://www.statistics.gov.lk/CLS/

victim) and their knowledge of it, such parents may exercise more control over their children's online behaviour. This too, is another interesting area that can be explored in a future research.

Also, future work should seek to examine how parents who do not use computers/internet monitor and control their children's online activities and if such measures are more effective than those used by parents who use computers/internet as part of their daily lives.

7. Conclusions

The practice of parental mediation control is becoming increasingly more pertinent as internet activity is associated with risks that can impact children negatively (Clark, 2011). This paper adds to the emerging parental mediation control literature by looking at the likelihood of parental mediating controls in parents who were victims of cybercrimes, who have greater internet self-efficacy and who have lower online third party trust. We also examined whether or not occupational type is associated with higher or lower parental monitoring behavior.

Essentially, our results suggest that older parents who were cybercrime victims are more likely not to want the same to happen to their children. As a consequence, when compared to others, they are more likely to resort to parental mediation techniques as compared to those who were not cyber victims. Thus, our first hypothesis is somewhat supported: Parents who have been victims of internet crime will be more likely to monitor their child's online activity. Stronger support for our first hypothesis may have been evidenced, if the factors that account for duration and intensity of the exposure to cybercrimes were considered in this study. However, due to data limitations this was not possible in the current study.

With regard to our second hypothesis: Parents with higher internet self-efficacy will be more likely to control their children's online activities; only few of the independent variables for

this hypothesis are statistically significant in the models. However, the findings give support for our second hypothesis.

On the other hand, our study demonstrates the strongest support for our third hypothesis: Lower trusts in online users (e.g. add only known people to social media or open an email from known persons only) increase parental control and risk awareness in a child's online activity. Here, both models reveal that all the parents with lower trusts in online users will only open emails from known persons. With regard to the second trust variable: never adding unknown persons in the social media, this was only significant for the older parents in the second model.

Surprisingly, and in contrast to the literature, our education controls were not significant in both models and was negatively signed in the full model. However, our results suggest that females to a greater extent than males are more likely to resort to offering guidance and control of their children's online activities. Finally, our results suggest that the non-pecuniary attributes of self-employment allow greater control and guidance of the online activities of the children by the older parents.

Hence, we can say that the results of our study lend certain support to our three hypotheses. It might have been interesting to see how our results would have differed if the different parenting mediating styles were taken into account, especially for the younger and the older parents.

References

Atkinson, S., Furnell, S. and Phippen, A. (2009). Securing the next generation: enhancing e-safety awareness among young people. *Computer Fraud and Security*, 7, 13-19.

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 50, 179–211.

Álvarez,M., Torres, A., Rodríguez, E. and Padilla,S. (2013). Internet use and parental mediation: A cross-cultural study use by primary and secondary school children. *Computers and Education*, 67, 69–78.

Anderson, C.L., Agarwal, R. (2010). Practicing safe computing: a multimethod empirical examination of home computer user security behavioral intentions. *Management Information Systems Quarterly*, 34, 613–643.

Anderson, E. (2015). Teenagers spend 27 hours a week online: how internet use has ballooned in the last decad'. *The Telegraph. Online* [accessed: 10 August 2016] http://www.telegraph.co.uk/finance/newsbysector/mediatechnologyandtelecoms/digital-media/11597743/Teenagers-spend-27-hours-a-week-online-how-internet-use-has-ballooned-in-the-last-decade.html.

Barber, B. (1983). The logic and limits of trust. New Brunswick NJ: Rutgers University Press.

Beech, M. and Bishop, J. (2015). Cyber-stalking or Just Plain Talking?: Investigating the Linguistic Properties of Rape-Threat Messages as Compusive Behavious. In J. Bishop (Ed.), Psychological and Social Implications Surrounding Internet and Gaming Addiction, (111-137). Hershey, PA.

Benson, V., Saridakis, G. and Tennakoon, H. (2015). Information disclosure of social media users: does control over personal information, user awareness and security notices matter? *Information Technology and People*, 28(3), 426-441.

Beran. T, and Li, Q. (2005). Cyber-harassment: a study of a new method for an old behaviour. *Journal of Educational Computing Research*, 32 (3), 265–277.

Blaya, C. and Alava, S. (2012). Risks and safety for children on the internet: the FR report. Full findings from the EU Kids Online survey of 9-16 year olds and their parents in France. LSE London: EU Kids Online.

Bryce, J. (2010). Online sexual exploitation of children and young people. In Handbook of Internet Crime, Jewkes, Y. and Yar, M., 320–342. Culhompton: Willan Publishing.

Cassidy, W., Jackson, M. and Brown, K. N. (2009). Sticks and stones can break my bones, but how can pixels hurt me? Students' experiences with cyber-bullying. *School Psychology International*, 30, 383-402.

Chang, F.C., Chiu, C.H., Miao, N.F., Chen, P.H., Lee, C.M. and Chiang, J.T. (2016). Predictors of unwanted exposure to online pornography and online sexual solicitation of youth. *Journal of Health Psychology*, *21*(6), 1107-1118.

Chan, T. W. and Koo, A. (2011). Parenting style and youth outcomes in the UK. *European Sociological Review*, 27(3), 385-399.

Chou, H.L., Chou, C. and Chen, C.H. (2016). The moderating effects of parenting styles on the relation between the internet attitudes and internet behaviors of high-school students in Taiwan. *Computers and Education*, 94, 204-214.

Castelfranchi, C. and Falcone, R. (2010). *Trust Theory: A Socio-Cognitive and Computational Model.* John Wiley and Sons, Ltd.

Chan, T.W. and Koo, A. (2011). Parenting style and youth outcomes in the UK. *European Sociological Review,* 27(3), 385-399.

Chang, H. and Chen, S. (2009). Consumer perception of interface quality, security, and loyalty in electronic commerce. *Information and Management*, 46(7), 411–417.

Chou, H.L., Chou, C. and Chen, C.H., (2016). The moderating effects of parenting styles on the relation between the internet attitudes and internet behaviors of high-school students in Taiwan. *Computers and Education*, 94, 204-214.

Clark, L.S. (2011). Parental mediation theory for the digital age. *Communication Theory*, 21(4), 323-343.

Cohen, L. and Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, 44, 588–608.

Conger, S., Pratt, J.H. and Loch, K.D. (2013). Personal information privacy and emerging technologies. *Information Systems Journal*, 23(5), 401–417.

Covington, M.J. and Carskedden, R. (2013). Threat implications of the Internet of things. 5th International Conference on Cyber Conflict, NATO CCD COE Publications, Tallinn, Estonia.

Crncec, R, Barnett, B. and Matthey, S. (2010). Review of scales of parenting confidence. *Journal of Nursing Measurement*, 18(3), 210-40.

Cross, C. (2015). No laughing matter blaming the victim of online fraud. *International Review of Victimology*, 21(2), 187-204.

Dholakia, R. R. (2006). Gender and IT in the household: evolving patterns of internet use in the United States. *The Information Society*, 22(4), 231-240.

Del Rey, R., Lazuras, L., Casas, J.A., Barkoukis, V., Ortega-Ruiz, R. and Tsorbatzoudis, H. (2016). Does empathy predict (cyber) bullying perpetration, and how do age, gender and nationality affect this relationship? *Learning and Individual Differences*, 45, 275-281.

Dempsey, A., Sulkowski, M. and Nichols, R. (2009). Differences between peer victimization in cyber and physical settings and associated psychological adjustment in early adolescence. *Psychology in the Schools*, 46, 962–972.

Didden, R., Scholte, R.H., Korzilius, H., De Moor, J.M., Vermeulen, A., O'Reilly, M., Lang, R. and Lancioni, G.E. (2009). Cyberbullying among students with intellectual and developmental disability in special education settings. *Developmental Neurorehabilitation*, 12(3), 146-151.

Dilmac, B. (2009). Psychological Needs as a Predictor of Cyber Bullying: A Preliminary Report on College Students. *Educational Sciences: Theory and Practice*, 9(3), 1307-1325.

Dishion, T. J. and McMahon, R. J. (1998). Parental monitoring and the prevention of problem behaviour: A conceptual and empirical reformulation. *National Institute on Drug Abuse Monograph*, 177, 229–259.

Dredge, R., Gleeson, J. F. and Xochi de la Piedad, G. (2014). Risk Factors Associated with Impact Severity of Cyberbullying Victimization: A Qualitative Study of Adolescent Online, Social Networking. *Cyberpsychology, Behaviour, and Social Networking*, 17(5),287-291.

Duerager, A. and Livingstone, S. (2012). How can parents support children's Internet safety? London: EU Kids Online.

Eastin, M. S., Greenberg, B., and Hofshire, L. (2006). Parenting the Internet. *Journal of Communication*, 56, 486–504.

Eastin, M.S. and LaRose, R. (2000). Internet Self-Efficacy and the Psychology of the Digital Divide. *Journal of Computer-Mediated Communication* (http://www.asusc.org/jcmc/vol6/issue1/eastin.html).

Evans, D. (2011). The Internet of Things How the Next Evolution of the Internet Is Changing Everything. CISCO white paper.
https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf.

European Commission. (2008). Towards a safer use of the Internet for children in the EU – A parent's perspective. In flash Eurobarometer 248: Brussels: European Commission. http://ec.europa.eu/public_opinion/flash/fl_248_en.pdf.

Grabner-Kräuter, S. and Bitter, S. (2015). Trust in online social networks: A multifaceted perspective. *Forum for Social Economics*, 441, 48-68.

Gradinger, P., Strohmeier, D. and Spiel, C. (2009). Traditional bullying and cyberbullying: Identification of risk groups for adjustment problems. *Zeitschrift Für Psychologie/ Journal of Psychology*, 217, 205-213.

Helsper, E.J. and Eynon, R. (2013). Distinct skill pathways to digital engagement. *European Journal of Communication*, 28(6), 696-713.

Henson, B., Reyns, B.W. and Fisher, B.S. (2011), Security in the 21st century: examining the link between online social network activity, privacy, and interpersonal victimization, *Criminal Justice Review*,36 (3), 253-268.

Hill, M.S. and Duncan, G.J. (1987). Parental family income and the socioeconomic attainment of children. *Social Science Research*, 16(1), 39-73.

Hinduja, S. and Patchin, J. W. (2007). Offline consequences of online victimization: School violence and delinquency. *Journal of School Violence*, 6(3), 89-112.

Hochschild, A. R. (1989). The second shift. Berkeley, CA: University of California Press.

Horzum, M. B. and Bektas, M. (2014). Examining the Internet use aim and internet parental style of primary school students in terms of various variables. *Croatian Journal of Education*, 16(3), 745-778.

Fishbein, M., and Yzer, M. C. (2003). Using theory to design effective health behavior interventions. *Communication Theory*, 13(2), 164–183.

Fleming, M. J., Greentree, S., Cocotti-Muller, D., Elias, K. A. and Morrison, S. (2006). Safety in cyberspace adolescents' safety and exposure online. *Youth and Society*, 38(2), 135-154.

George, J.F. (2002). Influences on the intent to make Internet purchases. *Internet Research*, 12, 165–180.

Goel, A., Rivera, W.A., Kincaid, P., Montgomery, M., Karwowski, W. and Finkelstein, N.M. (2016). Ethics in Virtual World Environments Research. *Emerging Tools and Applications of Virtual Reality in Education*, 258-276.

Grabner-Kräuter, S. and Bitter, S. (2015). Trust in online social networks: A multifaceted perspective. In *Forum for Social Economics*, 44 (1)1, 48-68, Routledge.

Gradinger, P., Strohmeier D. and Spiel C. (2010). Traditional bullying and cyberbullying: identification of risk groups for adjustment problems. *Journal of Psychology*, 217, 205–213.

Gubbins, C. and MacCurtain, S. (2008). Understanding the Dynamics of Collective Learning: The Role of Trust and Social Capital, *Advances in Developing Human Resources* , 10(4), 578–599.

Heirman, W., Angelopoulos, S., Wegge, D., Vandebosch, H., Eggermont, S. and Walrave, M., (2015). Cyberbullying-Entrenched or Cyberbully-Free Classrooms? A Class Network and Class Composition Approach. *Journal of Computer-Mediated Communication*, 20(3), pp.260-277.

Henson, B., Reyns, B.W. and Fisher, B.S. (2011). Security in the 21st Century Examining the Link Between Online Social Network Activity, Privacy, and Interpersonal Victimization. *Criminal Justice Review*, *36*(3), 253-268.

Hinduja, S. and Patchin, J.W. (2007). Offline consequences of online victimization: School violence and delinquency. *Journal of School Violence*, 6(3), 89-112.

Hinduja, S. and Patchin, J. W. (2010). Bullying, cyberbullying, and suicide. *Archives of Suicide Research*, 14(3), 206-221.

Horzum, M.B. and Bektas, M. (2014). Examining the internet use aim and internet parental style of primary school students in terms of various variables. *Croatian Journal of Education*, 16 (3), 745-778.

Ihmeideh, F. M., and Shawareb, A. A. (2014). The association between internet parenting styles and children's use of the internet at home. *Journal of Research in Childhood Education*, 28(4), 411-425.

Jaing, Z.J., Heng, C. S. and Choi B.C. (2013). Research note-privacy concerns and privacy protective behavior in synchronous online social interactions, *Information Systems Research*, 24 (3), 579–595.

Jones, T.L. and Prinz, R.J. (2005). Potential roles of parental self-efficacy in parent and child adjustment: A review. *Clinical Psychology Review*, 25, 341-63.

Kashahu L, Dibra, G., Osmanaga F. and Bushati J. (2014). The relationship between parental demographics, parenting styles and academic achievement. *European Scientific Journal*, 10(13), 237–51.

Kamali, A. (2015). Assessing Cyber-bullying in Higher Education. *Information Systems Education Journal*, 13(6), 43.

Kirwan, G. (2011). Presence and the victims of crime in online virtual worlds. *Proceedings of Presence*, 11-13.

Kashahu, L., Dibra, G., Osmanaga, F. and Bushati, J. (2014). The relationship between parental demographics, parenting styles and student academic achievement. *European Scientific Journal*, 10 (13). 237-251.

Lau, W. W. F., and Yuen, A. H. K. (2013). Adolescents' risky online behavior: The influence on gender, religion, and parenting style. *Computers in Human Behavior*, 29, 2690–2696.

Lau, W. F. and Yuen, A. H. (2016). The relative importance of paternal and maternal parenting as predictors of adolescents' home internet use and usage. *Computers and Education*, 102, 224-233.

Lemish, D., Ribak, R. and Aloni, R. (2009). Israeli kids go online: From moral panic to responsible parenthood. *Megamot*, 46(1-2), 137-163.

Lee, S, C. (2012) Impact of internet literacy, internet addiction symptoms, and internet activities on academic performance. *Social Science Computer Review*, 30, 403-418.

Lee, S. and Chae, Y. (2012). Balancing participation and risks in children's Internet use: The role of Internet literacy and Parental Mediation. *Cyber Psychology and Behavior*, 15(5), 257-262.

Lim, S. and Soon, C. (2010). The influence of social and cultural factors on mothers' domestication of household ICTs - Experiences of Chinese and Korean women. *Telematics and Informatics*, 27(3), 205-216.

Litt, E. (2013). Measuring users' Internet skills: A review of past assessments and a look toward the future. New Media and Society, 15(4), 612-630.

Livingstone, S. and Bober, M. (2006). Regulating the internet at home: contrasting the perspectives of children and parents. In D. Buckingham, and R. Willett (Eds.), *Digital generations: Children, young people, and new media*. Mahwah, N.J: Lawrence Erlbaum Associates.

Livingstone, S. and Helsper, E.J. (2008). Parental mediation of children's internet use. Journal of broadcasting and electronic media, 52(4), 581-599.

Livingstone, S., Haddon, L., Görzig, A. and Ólafsson, K. (2010). Risks and safety on the internet: the perspective of European children: key findings from the EU Kids Online survey of 9-16 year olds and their parents in 25 countries. Online [http://eprints.lse.ac.uk/53058/1/__lse.ac.uk_storage_LIBRARY_Secondary_libfile_shared_repository_Content_EU%20Kids%20Online_EU_Kids_Online_Report_Risks_and_safety_for_children_on_the_internet_2010.pdf]

Livingstone, S., Haddon, L., Gorzig, A. and Olafsson, K. (2011). *Risks and safety on the internet: The perspective of European Children*. Full Findings. London: LSE, EU Kids Online.

Livingstone. S., Ólafsson. K., Helsper. E. J, Lupiáñez-Villanueva. F., Veltri. G. A. and Folkvord. F. (2017). Maximizing opportunities and minimizing risks for children online: the role of digital skills in emerging strategies of parental mediation. *Journal of Communication*, 67(1),82-105.

Lowry, P. B., Cao, J. and Everard, A. (2011). Privacy concerns versus desire for interpersonal awareness in driving the use of self-disclosure technologies: the case of instant messaging in two cultures, *Journal of Management Information Systems*, 27 (4), 163–200.

Lwin, M.O., Stanaland, A.J. and Miyazaki, A. D. (2008). Protecting children's privacy online: How parental mediation strategies affect website safeguard effectiveness. *Journal of Retailing*, *84*(2), 205-217.

Madden, M., Lenhart, A., Cortesi, S., Gasser, U., Duggan, M. and Smith, A. (2013). Teens, social media, and privacy. Retrieved from http://www.pewinternet.org/files/2013/05/PIP_TeensSocial MediaandPrivacy_PDF.pdf.

Marcum, C.D., Ricketts, M.L. and Higgins, G.E. (2010). Assessing sex experiences of online victimization: An examination of adolescent online behaviors utilizing Routine Activity Theory. *Criminal Justice Review*, 35(4), 412-437.

McKnight, D. H., Cummings, L. L. and Chervany, N. L. (1998). Initial trust formation in new organizational relationships. *The Academy of Management Review*, 23(3), 473-490.

McLanahan, S. (1985). Family structure and the reproduction of poverty. *American Journal of Sociology*, 90, 873-901.

Meehan, S. and Hickey, J. (2015). A Review of Literature Relevant to the Experiences of Irish Parents in the Mediation of their Children's use of Internet Connected Devices. *Journal of Psychology and Clinical Psychiatry, 3*(3), 1-8.

Mesch, G.. (2007). Social diversification: a perspective for the study of social networks of adolescents offline and online. pp 105-121. In Grenzenlose Cyberwelt? Nadia Kutscher and Hans Uwe Otto (Eds.). Veralg Fur Sozialwiseenschaften, Heidelberg, Germany.

Mesch, G.S. (2009). Parental mediation, online activities, and cyberbullying. *Cyber Psychology and Behavior*, 12(4), 387-393.

Mitchell, K.J., Finkelhor, D., Wolak, J., Ybarra, M.L. and Turner, H. (2011). Youth internet victimization in a broader victimization context. *Journal of Adolescent Health*, 48(2), 128-134.

Mitchell, K.J., Ybarra, M.L., Jones, L.M. and Espelage, D. (2016). What Features Make Online Harassment Incidents Upsetting to Youth? *Journal of School Violence*, 15(3), 279-301.

Meter, P.J. and Bauman, S. (2016). Moral disengagement from cyberbullying effects traditional bullying, victimization, and parental monitoring via cyberbullying involvement. *The Journal of Early Adolescence*, 1-24.

Meyers. S, and Hickey. J. (2015). A Review of Literature Relevant to the Experiences of Irish Parents in the Mediation of their Children's use of Internet Connected Devices. *Journal of Psychology and Clinical Psychiatry*, 3(3): 00135. DOI: 10.15406/jpcpy.2015.03.00135.

Mustaine, E.E. and Tewksbury, R. (2002) Sexual assault of college women: A feminist interpretation of a routine activities analysis, *Criminal Justice Review*, 27, 89-123.

Näsi, M., Räsänen, P., Hawdon, J., Holkeri, E. and Oksanen, A. (2015). Exposure to online hate material and social trust among Finnish youth. *Information Technology and People*, 28(3), 607-622.

Nathanson, A. I. (2002). The Unintended Effects of Parental Mediation of Television on Adolescents. *Media Psychology*, 4(3), 207-230.

Navarro, R., Serna, C., Martínez, V. and Ruiz-Oliva, R. (2013). The role of Internet use and parental mediation on cyberbullying victimization among Spanish children from rural public schools. *European Journal of Psychology of Education*, 28(3),725–745.

Nikken, P. and Jansz, J. (2014). Developing scales to measure parental mediation of young children's internet use. *Learning, Media and Technology*, 39 (2), 250-266.

Notten, N. and Nikken, P. (2016). Boys and girls taking risks online: A gendered perspective on social context and adolescents' risky online behavior. *New Media and Society*, *18*(6), 966-988.

Olivero, N. and Lunt, P. (2004). Privacy versus willingness to disclose in e-commerce exchanges: The effect of risk awareness on the relative role of trust and control. *Journal of Economic Psychology*, *25*(2), 243-262.

Ortega, R., Elipe, P., Mora-Merchán, J. A., Calmaestra, J., and Vega, E. (2009). The emotional impact on victims of traditional bullying and cyberbullying: A study of Spanish adolescents. Zeitschrift Für Psychologie/Journal of Psychology, 217(4), 197-204.

Ouytsel, J., Ponnet, K. and Walrave, M. (2016). Cyber dating abuse victimization among secondary school students from a lifestyle-routine activities theory perspective. Journal of Interpersonal Violence, 12, 1-10.

Özgür, H. (2016). The relationship between Internet parenting styles and Internet usage of children and adolescents. Computers in Human Behavior, 60, 411-424.

Padilla-Walker, L. M. and Coyne, S. M. (2011). Turn that thing off! parent and adolescent predictors of proactive media monitoring. Journal of Adolescence, 34(4), 705-715.

Pereira, F., Spitzberg, B.H. and Matos, M. (2016). Cyber-harassment victimization in Portugal: Prevalence, fear and help-seeking among adolescents. Computers in Human Behavior, 62(C) 136-146.

Popp, A. M. and Peguero, A. A. (2011). Routine activities and victimization at school: The significance of gender. *Journal of Interpersonal Violence*, 30(12), 2413-2436.

Pricen M. and Dalgleish, J. (2010). Cyberbullying: experiences, impacts and coping strategies as described by Australian young people. *Youth Studies Australia*, 29, 51–64.

Ponte, C. and Simões, J.A. (2009). Asking parents about children's internet use: comparing findings about parental mediation in Portugal and other European countries. In *EU Kids Online-Final Conference*. London.

Raskauskas, J. (2010). Text-bullying: Associations with traditional bullying and depression among New Zealand adolescents. *Journal of School Violence*, 9(1), 74-97.

Raskauskas, J. and Stoltz, A. D. (2007). Involvement in traditional and electronic bullying among adolescents. *Developmental Psychology*, 43(3), 564-575.

Romito, P. and Beltramini, L. (2015). Factors associated with exposure to violent or degrading pornography among high school students. *The Journal of School Nursing*, 31(4), 280-290.

Ryan, K. N. and Curwen, T. (2013). Cyber-Victimized Students: Incidence, Impact, and Intervention. Retrieved September 9, 2016, from http://sgo.sagepub.com/content/spsgo/3/4/2158244013516772.full.pdf.

Reyns, B. W., Henson, B. and Fisher, B. S. (2011). Being pursued online: Applying cyberlifestyle–routine activities theory to cyberstalking victimization. *Criminal Justice and Behavior*, 38(11), 1149-1169.

Rotter, J.B. (1971). Generalized expectancies of interpersonal trust. *American Psychologist*, 26(5), 443–452.

Sasson, H. and Mesch, G. (2014). Parental mediation, peer norms and risky online behavior among adolescents. *Computers in Human Behavior*, 33, 32-38.

Sasson, H. and Mesch, G.S. (2017). The Role of Parental Mediation and Peer Norms on the Likelihood of Cyberbullying. *The Journal of Genetic Psychology***,** 178 (1),15-27.

Spears, B., Slee, P., Owens, L., and Johnson, B. (2009). Behind the scenes and screens: Insights into the human dimension of covert and cyberbullying. *Zeitschrift Für Psychologie/ Journal of Psychology*, 217(4), 189-196.

Staude-Müller, F., Hansen, B. and Voss, M. (2012). How stressful is online victimization? Effects of victim's personality and properties of the incident. *European Journal of Developmental Psychology*, *9*(2), 260-274.

Sun, P., Unger, J. B., Palmer, P. H., Gallaher, P., Chou, C.-P. and Baezconde-Garbanati, L. (2005). Internet accessibility and usage among urban adolescents in southern California: Implications for web-based health research. *Cyber Psychology and Behavior*, 8(5), 441-453.

Tseloni. A; Wittebrood. K; Farrell. G and Pease. K, (2004). Burglary Victimization in England and Wales, the United States and the Netherlands, *The British Journal of Criminology*, 44(1), 66-91.

Valcke, M., Bonte, S., De Wever, B. and Rots, I. (2010). Internet parenting styles and the impact on Internet use of primary school children. *Computers and Education*, 55(2), 454-464.

van Deursen AJ, van Dijk,J. (2014). Towards a multifaceted model of internet access for understanding digital divides: an empirical investigation. *The Information Society*, 31(5), 379–391.

van Deursen,A.J.,. van Dijk, J.and P. M. ten Klooster. (2015). Increasing inequalities in what we do online. A longitudinal cross sectional analysis of Internet activities among the Dutch population (2010 to 2013) over gender, age, education, and income. *Informatics and Telematics*, 32 (2), 259–72.

van Den Eijnden, R. J., Spijkerman, R., Vermulst, A. A., van Rooij, T. J. and Engels, R. C. (2010). Compulsive Internet use among adolescents: bidirectional parent-child relationships. *Journal of Abnormal Child Psychology*, 38(1), 77-89.

van Dijk, J.. and van Deursen, A.J.. (2014). Digital skills, unlocking the information society. Palgrave Macmillan.

van Geel, M., Vedder, P. and Tanilon, J. (2014). Relationship between peer victimization, cyberbullying, and suicide in children and adolescents: a meta-analysis. *JAMA pediatrics*, 168(5), 435-442.

Wang, R., Bianchi, S. M. and Raley, S. B. (2005). Teenagers' Internet use and family rules: A research note. *Journal of Marriage and Family*, 67(5), 1249-1258.

Wang, J., Nansel, T. and Iannotti, R. (2011). Cyber bullying and traditional bullying: differential association with depression. *Journal of Adolescent Health*, 48, 415–417.

Warschauer, M. (2003). Demystifying the digital divide. *Scientific American*, 289(2), 42-47.

Wong, Y.C., Ho, K.M. and Chen, H. (2015). Internet supervision and parenting in the digital age: The case of Shanghai. *Open Family Studies Journal*, *7*(2), 112-123.

Whitty, M.T. (2015). Anatomy of the online dating romance scam. *Security Journal*, *28*(4), 443-455.

Winkelman, S.B., Early, J.O., Walker, A.D., Chu, L. and Yick-Flanagan, A. (2015). Exploring Cyber Harassment among Women Who Use Social Media. *Universal Journal of Public Health*, *3*(5), 194-201.

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

Wong, Y.C., Ho, K.M. and Chen, H. (2015). Internet supervision and parenting in the digital age: The case of Shanghai. *Open Family Studies Journal*, *7*(2), 112-123.

Wright, M.F. (2017). Parental mediation, cyberbullying, and cyber trolling: The role of gender. *Computers in Human Behavior*, 71, 189-195.

Wurtele, S.K. and Kenny, M.C. (2010). Preventing online sexual victimization of youth. *The Journal of Behavior Analysis of Offender and Victim Treatment and Prevention*, *2*(1), 63-74.

Ybarra, M.L. and Mitchell, K.J. (2004). Online aggressor/targets, aggressors, and targets: A comparison of associated youth characteristics. *Journal of Child Psychology and Psychiatry*, *45*(7), 1308-1316.