International Research Journal of Computer Science (IRJCS)
Issue 4, Volume 2 (April 2015)
ISSN: 2393-9842
www.irjcs.com

A Preliminary Survey on Child Online Protection Initiatives: A Focus on Namibia.

Attlee M. Gamundani*
Polytechnic of Namibia
School of Computing & Informatics
Computer Science Dept.

Fungai Bhunu-Shava
Polytechnic of Namibia
School of Computing & Informatics
Computer Science Dept.

Mercy Bere
Polytechnic of Namibia
School of Computing & Informatics
Computer Science Dept.

Herman Kandjimi
Polytechnic of Namibia
School of Computing & Informatics
Computer Science Dept.

Abstract— Child Online Protection is no more a new concept with the digital age permeating the different cultural and moral fibers that used to keep communities at bay. This paper contextualise the concern to the Namibia horizon only, not really concluding that, it is where such protection is needed, this is more than a world phenomenon, as ITU and many other concerned entities have been promoting awareness emphasizing the need to be on the lookout for activities children engage in when online. This paper presents a preliminary review on the level of awareness; the relevant stakeholders have, in terms of Child Online Protection. A consultative workshop was employed at the very early stage of this ongoing research, as such; this paper will predominantly focus on the findings of the workshop's outputs and communicate the progressive envisaged steps towards this area of research.

Keywords— COP; Awareness; Children; Workshop; Namibia.

I. INTRODUCTION

Child Online Protection is a hard and tricky concern that requires multi-national efforts if it's to be successfully tackled in the near future [1], [2]. This is mainly due to the exponential growth in smart devices and the internet or rather "the Internet of Things" [3], [4]. This paper relies heavily on literature reviews to try and explain the concept of Child Online Protection and contextualise the scenario to the Namibian horizon.

Internet penetration has increased in Namibia. This is mainly because of smart phone ubiquity and secondly because of wide availability of cheap broadband. This also implies that much more Namibian children are now using the internet and thus, it was imperative to research on how safe Namibian children are when they use the internet. The researchers decided on conducting a workshop in which relevant stakeholders concerned with Child Online Protection were invited to discuss and propose initiatives on how Namibian children are and can be protected online.

This paper is structured into five key sections which in summary are as follows: - Section I is the introduction, which gives an overarching overview of the paper focus, by giving a general view of the concept under study. Section II tries to answer the question, what is Child Online Protection? heavily relying on literature review, to derive a working definition in the context of this paper, for who qualifies to be a child. The same section also attempts to clarify, why the need to focus on Child Online Protection? The section that hint the reader on some of the initiatives that are being done elsewhere, either in the region or in the international communities, regarding awareness on Child Online Protection is section III. The workshop setting is explained in section IV. This section will inform the reader on how we designed the workshop and why we designed it that way. Section V, gives the conclusion by summarising the workshop findings and inform the reader on the work in progress in as far as this research in concerned.

II. CHILD ONLINE PROTECTION

A. Defining Child Online Protection

Child Online Protection is an initiative by responsible authorities and various stakeholders, to ensure children are safe as they interact with technology [5]. As a definition of a child rightly places them as innocent victims [6], they need a well-structured protection environment for their safe interaction with online enabled and capable gadgets.The picture of a child painted by the (Namibian Constitution, Article 15), depicts the majority of active users of technology mainly under the age of 16years, who are experimenters of technology and someone who cannot make deliberate responsible decisions on their own [5]. Henceforth, COP can refer to the extended responsibility initiatives to protect and equip children from becoming preys or yield to danger unknowingly.

All efforts to try and understand the behaviour of a child online formulates the overall understanding of what COP is all about. It is beyond understanding of who is a child and what protection they want when online or offline. There is a common misunderstanding in the terms Child Online and Online Child, although used interchangeably these terms are not the same. An Online Child mainly refers to a child whose access to online facilities is by default [7], which typically is associated with third world countries, where online facilities are offered to them ubiquitously, be it at home, school, social gathering places and sometimes the homes are remotely controlled via parents' mobile phones or equivalent technologies. On the other hand, a Child Online is a child who decides or by chance get an opportunity to be online.This paper focuses on the safety of a Child Online and not on the Online Child. The former is more vulnerable in the light of exposure as they can experiment their way through to traps that positions them, in a more critical state than the latter. Thou both two children are vulnerable and both needs protection, the attraction to focus on the Child Online is motivated by the lack of proper stakeholder involvement in the environment this child is growing.

COP [8] involves identifying risks and vulnerabilities to children in cyberspace, creating awareness and developing practical tools to eliminate the risks and then finally sharing the gained knowledge and experiences. COP is preventing children from being subjected to harmful circumstances when online or as a result of being online, while preserving the full benefits that the internet has to offer and for this to be fully achieved all stakeholders need to completely understand the threats and risks involved.

B. Some of the reasons for Child Online Protection

There is no silver bullet solution to protect children online [9]. This explains why this topic is of serious concern to the research community. For solutions being proposed may not perfectly merge with the prevailing regulatory frameworks of different countries. The need to align solutions to existing regulations enables practical orientation of solutions. This is a global issue which requires a global response from all segments of society, including children and young people themselves [8]. The ever changing nature of the technological landscape positions this research area as critically sensitive as espoused by secretary general of ITU [10] "Child Online Protection… in the era of massively available broadband internet – is a critical issue that urgently requires a global contribution, coordinated response" [10]. This signals the need to constantly upgrade and update existing solutions to match current dynamic trends.

Addressing the challenges of cyber security is without hiccups, as COP finds itself intertwined in yet another critical dimension. However, the focus of this paper is not on cyber security to a greater extend but to outline how the COP fits in the bigger picture, [18] gives different illustrations of concerns that need undivided attention, to contain some of the envisaged challenges it may pause. Taking care of cyber security issues doesn't imply the chid is now bullet proof safe. Practically looking at this notion, cyber security may be concerned with the bigger picture, yet COP utilises the finer issues, sometimes not taken care of. Rarely does security think of a 5 year old breaking into a bank's firewall. With their experimental interactions with various computer applications, they unconsciously pave an easy path for intruders. A simple online game a teenager get hooked onto, will be a window for some security concerns that can both be harmful to children themselves and extend far beyond their circles of contact. The interlink between COP and cyber security as depicted by [18], speaks volumes on the need to look at COP concerns from a holistic approach and not only classify it as a measure or move to protect the Child Online, but to go beyond that. Having a child in the domain of security brings in a complicated entity in the security equation, hence the need to seriously focus on this aspect from a threefold dimension, victim, medium and perpetrator viewpoints. The variables can be varied but the focus remains stretched and not narrowed. The mixture of challenges, standards implementation, enforcement, compliance-effectiveness, is too vast to turn a blind eye on. The need to focus on Standards & prevention tools and who they protect is also mandatory [11]. We may deliberately ask the question who the standards and prevention tools are designed for? Children? Educators? Government? Industry? The implementation side of the standards if in place is also critical. Who know and understands how to effectively use standards and tools – parents/guardians [11] ? Which stakeholders are pooling together or apart [11]? The worsening development is the dynamic nature of the variables that contribute to the problem in question, which, if not closely monitored, can become unmanageable. Being in the era of broadband access and digital citizenship, the frequency and swiftness decision makers are supposed to employ, has to be tripled if not quadrupled always [11].There may be clearly spelt out procedures to follow in certain national environments or at a global scale, however, COP is and must be a collaborative and multi-stakeholder initiative [11], [12] in approach. National cybersecurity strategy that includes COP must be worked on, in the full spectrum of the prevailing national conditions. Local and international legal frameworks as well as support may be aligned only if the objectives of Child Online Protection in a defined area are understood [12]. Awareness and know-how extensive stakeholder education [11], [12], 13] are key ingredients in brewing a solid COP framework.

III. INITIATIVES ON CHILD ONLINE PROTECTION ELSEWHERE

The most talked about initiatives on COP are by the International Telecommunication Union (ITU) especially, one that was launched in November 2008 within the then Global Cybersecurity Agenda (GCA) framework, but not to say that it's the first initiative.

The ITU's initiative was established as an international concerted network to promote the awareness and online protection of children and young people all over the world, by means of providing guidelines on safety behaviours while online. To accomplish all its objectives the initiative works with UN agencies and partners all over the globe. The ITU's initiative is based on multi-stakeholders and believes every organisation or institution – be it online or mobile, educator or legislator, technical expert or industry body - has a role to play in making the internet a safer place for every child.

The ITU's initiative revolves around five key areas in developing strategies [8] and takes a holistic approach in the promotion of Child Online safety as stated below:

- Legal measures
- Technical and Procedural Measures
- Organisational Structures
- Capacity Building
- International Cooperation

The start of the ITU's COP initiatives has attracted a lot of countries (including African countries) to join and contribute to the promotion and protection of children online. Another prominent initiative is the Children's Online Privacy Protection Act (COPPA) of 1998 by the Federal Trade commission (FTC) in the United States.

The COPPA was mainly aimed at protecting the privacy of children less than 13 years by means of parental consent before the validation of any data collection. The Chairman of the FTC at that time Robert Pitofsky said "This proposed rule aims to achieve that goal by putting parents in control of personal information that is collected from their children on the Web. The proposed rule also provides flexibility to accommodate varied business practices and the fast pace of technological change."

This Act was heavily challenged by the fact that commercial website or online services couldn't be deemed as directed solely to children and hence hard to conclude if such sites violated the rule. To try and tackle this challenge the FTC has been reviewing and improving this rule for almost every two month from the enactment of the COPPA act and as a result about three known programs were produced namely:

a) kidSafe harbour program(initiated 2013, but approved in 2014)
b) iVeriFly as a verification method for parents(February 2014)
c) iKeepSafe COPPA (August 2014)

The latest program iKeepSafe (Federal Trade Commission) also known as the Internet Keep Safe Coalition, was initiated as a safe harbour oversight program under the Children's Online Privacy Protection Act (COPPA) and the agency's COPPA Rule, and it covers a much broader area in terms of children safety online [16]. In the United Kingdom (UK), the UK Council for Child Internet Safety (UKCCIS) was initiated in September 2008, to try and promote the children safety on the Internet following recommendations from [17]'s review 'Safer Children in a Digital World'. The UKCCIS now consist of more than 200 stakeholders from across government, industry, law, academia and charity sectors that work in partnership to help keep children safe online.

In her paper [17] touched on the major issues that lead to children's safety being compromised while online and listing video games as the most causes of these unsafe behaviors. This is due to the fact that, while playing games they get options of joining review blogs and chat rooms related to such games in the end compromising their safety without even knowing it. The important roles that parents play in their children's lives as outlined by [17], and in the process of keeping them safe whether it's online or in real life, is profoundly critical and needs proper nurturing.The Child Exploitation and Online Protection Centre (CEOP) was formed under the command of the UK's National Crime Agency (NCA) in April 2006 and was tasked to promote awareness for children's online safety and bring forth cases involving children exploitation online both nationally and internationally. This CEOP uses a holistic approach to identify the main threats to children and coordinates activities against these threats and bring offenders to account.Africa is no exception to these initiatives; The African Children Cyber Safety Initiative (ACCSI) was created in 2009 during the Children and Young People Online Protection Forum organized by the African Information Security Association (AISA) with a mandate to advance the cause of safe online culture for children and young people in Africa. The ACCSI like many other world-wide initiatives aims to reduce the online threats for the African children and promote awareness thereof. The ACCSI strongly believes in creating focal points for all issues related to children online safety and in turn use this to strengthen its stakeholder's network, hence produce corroborative efforts among all the stakeholders. Regionally, a Child Online Protection workshop in Kenya (8-9 June 2011) unearthed quite a number of issues that are relevant to most African and the international environments in a way or the other. Much of the workshop findings as summarised under the policy, legal and framework for Child Online Protection by [20] reveals some of the trends that inform why Child Online Protection is quite a tropical issue.

It also hints on some of the risks the child is exposed to as a result of unaddressed issues. Some of the policy aspirations are summed up in these four key words: affordable, realiable, accessible and appropriate ICTs. Logically, the very same workshop outlined some of the key roles the governments should play, chief among them being to protect the child in the "real" world and also in the "virtual" world [11], [20]. It is on the premise of some of these initiatives in the region, which motivated this research direction. To align the efforts being done elsewhere in light of the same issue of protecting children online, there is need to understand the situation on the ground.

IV. **WORKSHOP SETTING**

The research was qualitative in nature using a workshop as a data collection strategy. Goals of the research were outlined and presented to the participants in an invitation letter. The Workshop approach was employed on the basis of its versatility on enabling different key stakeholders to converge and share their area specific knowledge in light of the various initiatives that, they might be having or ought to implement in the long run. The stakeholders had an opportunity to interact, share ideas and charter the way forward. A workshop was determined as a good pilot study on Child Online Protection as it would give a general picture of Child Online Protection by consolidating information from the invited different stakeholders. The participants were selected according to their impact on the project.

A. *Workshop Objectives*

The workshop aimed at answering the questions listed below:

- What are some of the risks faced by Namibian Children online?
- How can Namibia as a nation prevent children from being exploited when accessing the internet?
- How can the combined efforts from the Government, private sectors, communities and all other stakeholders alleviate this challenge?

Firstly it is important to understand the risks that Namibian children face so as to then initiate proper Child Online Protection mechanisms. To get the proper solution it is vital to first thoroughly understand the problem, thus it was important to find out the risks and challenges Namibian children face online. This information can only be gained by involving the stakeholders in the problem definition as well as the development of the solution. After the risks and issues facing children online were identified then next, the need to find ways and the means to solve the problem was imperative. There was a need to discern if it was acceptable in the Namibian context to take existing solutions from elsewhere and implement them as is or to take existing solutions, change some aspects of the solutions and implement in Namibia or to develop/design novel Child Online Protection mechanisms for Namibia. Finally when the type of solutions to be implemented in Namibia has been decided the last question to be answered is who should be responsible for implementing the solutions and who should be the custodian of the implemented solutions? Should it be the government, private sector, communities, children or a collaborative effort? In addition who should finance such initiatives?

B. *Target Audience*

In order to get the correct answers it was important to invite the children themselves as well as anyone who works closely with children and for children's rights and interests as well as the law makers and internet regulators. With this in mind several primary, high school children and teachers from 10 Windhoek based schools, human rights lawyers, Ministry of Gender Equality and Child welfare, Ministry of safety and Security, UNICEF, Office of the president, Office of the Prime Minister, Ministry of Information Communication Technology (MICT) employees and members of Communications Regulatory Authority of Namibia (CRAN), Lifeline and Child Line Namibia, legal assistance Centre, Council of Churches Namibia (CCN), Green Enterprise solutions and many other stakeholders were invited.

C. *Workshop proceedings*

About 26 people were part of the workshop including members of the research team. The 3 hour long workshop began with registration of participants and a welcome. A brief introduction of the workshop objectives was given. Soon after introductions the participants were asked to fill in a questionnaire just to find out if they know or if they have been exposed to Child Online Protection. It was necessary to understand the level of awareness they were bringing into the session. A presentation on African Child Online Protection (ACOPEA) then followed to provide the audience with a general overview of what is being done elsewhere.

The participants were then grouped into 4 sets with 6-8 participants for a structured discussion. Each group had a moderator who was leading the discussion and was asking each group the following questions:

1. List key players that should be involved in the Child Online Protection projects.
2. What are the legal issues surrounding Child Online Protection?
3. Are there any suitable laws that can be introduced?
4. Is there a need to create a platform/centre/website for reporting child online abuses? In what form should it be created? Who should collaborate to run it?
5. What else can be done on Child Online Protection in Namibia?
6. Is there any good framework that can be adopted to address COP in Namibia?
7. Should we conduct a survey on Child Online Protection?

Answers from the participants were noted down on flip charts. Outcomes from the questions and the short questionnaire are outlined in the next section. Presentations on ITU COP and experience from elsewhere then followed, after which an open discussion of the outcome of the group discussion was conducted. The open discussion yielded a way forward for the project as the participants deemed appropriate.

D. *Workshop Outcomes*

The workshop questionnaire had 13 questions which gathered information on the participant demographics first and gradually inquire about COP. The collected data was grouped according to themes that were being exhibited. Below is a summary of the results.

1. The elderly had few incidences and had experienced the attacks later in life. This could be attributed to the low exposure to technology in the past.
2. More females participated, maybe because children issues are closer to their hearts in our role based society
3. Most people do not report incidences, some highlighted the lack of knowhow as to where they should report, yet some felt it was not serious and others just ignored. Based on this it is necessary to enlighten people on their rights, online and the importance of reporting the incidents. For those who reported some did not follow up to see if the case was resolved, this is not a good indicator.
4. The late teens and the working class seem to be the most targeted. Could be because they use technology on the Internet the most, they are among the active working class hence they are targeted for the information asset they are custodians to.
5. Social network, Facebook is the most popular app among the participants and the most targeted followed by emails, you tube, whatsapp, e.t.c. based on this it can be inferred that socialising is most common and should be the first focal point in addressing internet security. In a related study by UNISA BMR, cyber grooming was alarmingly high with 24,4% of the surveyed population ending in an actual sexual act.
6. Multiple devices are used to access the internet services, phones and pcs are top on the list of such devices.

The group discussions were focused on seven questions and Table 1 gives the summarized responses and suggestions from the group discussions.

TABLE I. **WORKSHOP OUTCOMES**

Description	*Responses*	*Roles/How*
1. Key players to be involved in the COP project	**1.Government ministries** ➢ Education ➢ Gender and child welfare ➢ Health and social welfare ➢ Defence , safety and security ➢ ICT **2.Private sector**	➢ Legislation and Law enforcement ➢ Awareness ➢ Counselling ➢ Funding
	3.CRAN **4.ISP**	➢ Licensing condition and considerations ➢ Content control and awareness
	5.Students (learners)	➢ Awareness
	6.Parents and educators	➢ Awareness and parental control
	7. Society	➢ Be educated ➢ Monitor awareness levels in minors
2. Legal issues on Cop, Laws to be introduced	➢ No framework and or an Act of parliament specific for COP ➢ Once the Law or an ACT is passed then CRAN to come up with framework ➢ Law enforcement agencies (Police, securities …etc.) to be trained ➢ CRAN to strongly govern the licensing of materials developed by IT companies	
3. Need for COP Platform/Centre	➢ COP centre in collaboration with Childline Namibia(116) ➢ Interactive website to be developed by the Polytechnic team and incorporate with social medias ➢ Radios and TV as media of awareness ➢ Counselling centres to collaborate with the COP centre or be incorporated into COP. ➢ Hotline to be linked to both the Police and COP centre	
4. What is the strategy for Namibia?	➢ Needs more research to be done taking into considerations : ▪ Current Government initiatives towards COP ▪ Suggested possible solutions ▪ More awareness and input from communities ▪ Identifying the Namibian COP problem ➢ Need more case studies from other countries	
5. Any Framework to be adopted for Namibia	➢ Need more research and case studies from other countries	
6. COP survey to be conducted in major cities?	➢ Need to be done everywhere including rural areas ➢ Need a holistic approach(not localized)	
7. Other key areas	➢ Research time line, responsibility and target group	

The open discussion came up with the following agreement:

- A website for COP should be created for awareness campaigns and logging of incidents.
- A database for logging COP issues must be created
- Responsibilities for the stakeholders in coming up with COP program for Namibia.
- A follow-up meeting to be held to the way forward.
- Research on possible frameworks for COP in Namibia to be conducted by the Polytechnic of Namibia
-

V. CONCLUSION AND FUTUTRE WORK

The workshop was an eye opener as to the amount of work that has to be aligned to the needs on the ground. Generalising the situation and working towards a generic solution will not yield the intended results in a broader sense. As hinted by the workshop findings, everybody from the manufacturers of technology, gadgets to the very children themselves need to be involved in the whole solution equation. The non-existence of legally binding and protecting laws against, crimes and cyber activities that eventually spill into COP concerns, is a serious cause for concern, the relevant stakeholders should be weary of such developments and take full responsibility in ensuring such laws are enhanced and enshrined in the binding and statutory structures of the country as well as aligning them with the international laws to a greater extent. A free platform for expression of violations of COP laws is among the deliverables this research is going to work towards in the future and hope to come up with, a Website portal for information and reporting.Children cyberspace (content for children?) Technology and regulatory impact assessment tools can be incorporated on the same environment to ensure a containment of the exposure of children to uncensored information sources. The workshop findings are very informative and activity oriented, if most of the key activities hinted are executed to the later, a practical solution should be delivered as a result.

ACKNOWLEDGMENT

We would like to thank all the invited guests for taking time to attend the workshop and for their invaluable views and comments on the issue of Child Online Protection. We would also like to thank all members of Polytechnic of Namibia's Forensic Computing and Security research cluster who helped in organising and hosting the workshop. Finally we thank the Polytechnic of Namibia for availing the funds, time and facilities to host the workshop..

REFERENCES

[1] OECD, *The protection of child online*, Report on risks faced by child online and policies to protect them.,OECD , Publishing, 2012.
[2] Annals of the American Academy of Political and Social Science, *Children's rights and the internet*, pp 56-70, 2001.
[3] M. Cunningham, *Next generation privacy: The internet of things, data exhaust, and reforming regulation by risk of harm*, Concordia University School of Law, Groningen Journal of International law , Vol 2, Ed 2, Jan 14, 2015.
[4] C.Y. Cultura, *Next generation of smart machines: a survey of enabling technologies*, Humberto Calderon,ISSN:2077-3323, June 2014,pp 89-119.
[5] S.Keith and M.E.Martin, *Cyber-bullying: creating a culture of respect in a cyberworld*, Reclaiming children and youth, Vol.13:4, Winter 2005, pp 224-228.
[6] J. Wolak, D. Finkelhor, K. S. Mitchell, M. L.Ybarra. (2010). *Online "Predators"and their victims myths, Realities, and implications for prevention and treatment*, Psychology of violence, Vol 1, ISSN:2152-0828, 2010, pp 13-35
[7] M. Madden,A. Lenhart, M. Dugan, S. Cortesi, Yrs Gasser, *Teens and Technology 2013*, Pew Research Center, The Berkman Center for internet & Society at Harbard University, 2013, pp 1-9.
[8] ITU COP, *About the child online protection initiative*, ITU COP., in press
[9] S. Mitra and V. Rana, *Children and the internet: experiments with minimally invasive education in india*, British Journal of Educational Technology, Vol 32, Issue 2, 2001, pp 221-232.
[10] H. I.Toure, *World Telecommunication development conference opening ceremony*, Dubai, UAE, Speech by ITU secretary –General, 30 March, 2014.
[11] B. Sihanya, *Protecting children in cyberspace in Kenya whose responsibility is it?*, Report of the workshop organised by communication commission of Kenya(cck), Hotel intercontinental, Nairobi, Kenya, June 8th-9th 2011.
[12] A. D. Thierer, *Five online safety task forces agree: Education, Empowerment & self-regulation are the answer*, Social Science Research Network. George Mason university-mercatus center, Progress and freedom foundation progress on point paper, Vol 16, No.13, July 2009
[13] ACCSI, *African Children Cyber Safety Initiative Mandate*, ACCSI- African Children Cyber Safety Initiative Mandate., in press
[14] CEOP, " CEOP - About Us," CEOP Command., in press
[15] M. S. Eastin, B. S.Greenberg and L.Hofschire, *Parenting the internet*, Journal of communication, Vol 56, Issue 3, Sept 2006, pp 486-504.
[16] COPPA, *COPPA - Children's Online Privacy Protection Act.*, in press
[17] T. Byron, *Safer Children in a Digital World*, Children and New Technology, 2008.
[18] M. A.Haji, *Protecting children in cyberspace: Whose responsibility is it?*, Child online protection workshop, Intercontinental , Hotel, Nairobi, Communications Commission of Kenya, 8th-9th June, 2011,
[19] UNICEF Office of Research, *Child Safety Online: Global challenges*, Florence, Italy: UNICEF Innocenti Research Centre, 2012.
[20] Mercy, *Protecting children in cyberspace: Whose responsibility is it*?, Child online protection workshop, Intercontinental , Hotel, Nairobi, Communications Commission of Kenya, 8th-9th June, 2011.

