A Crazy Cyber World: Construction of a Composite Index for Measuring Child Online Protection (COP)

Ada S. Peter, PhD ada_peter@biari.brown.edu; ada.peter@covenantuniversity.edu.ng;
Tolu Kayode-Adedeji kehinde.kayode-adedeji@covenantuniversity.edu.ng;
tolulopekayodeadedeji@gmail.com

Covenant University, Ota Ogun State Nigeria
Word count: 5070
Presented at the 66th International Communication Association Conference (ICA), Fukuoka Japan, 2016.

Abstract

On 17th November 2010, the international telecommunications union (ITU) launched a new Child Online Protection (COP) phase. Years after setting up these guidelines, it is important to develop a composite measure that provides an intuitive understanding of the gaps in child online protection system, creates cross national comparisons for advocacy and action. The enquiry proposes an objective assessment of where each country stands in child online protection across four critical priority areas. These areas include: nationally recognized child online protection strategy/ legislations; Collaboration, cooperation and partnerships; information sharing/reporting mechanism; and capacity building/institutional support. The four areas are reflected in the Child Online Protection Index (COPI) structure which comprises four sub-indexes. Each sub index is in turn measured by five categorical indicators. The indicators are derived or adapted from key institutions active in the information and communications technologies (ICT) sector and in child online safety issues.

Introduction

The International Telecommunications Union (ITU), a lead facilitator for World Summit on the Information Society (WSIS) action line C5 for assisting stakeholders in building confidence and security in the use of ICTs at national, regional and international levels, and a team of contributing authors from institutions active in the information and communications technologies (ICT) sector and in child online safety issues (including Children's Charities' Coalition on Internet Safety (CHIS), Child Helpline International (CHI), International Centre for Missing & Exploited Children (ICMEC), Interpol and United Nations Interregional Crime and Justice Research Institute (UNICRI), prepared action guidelines for key actors in child online protection (ITU, 2009).

By the 17th November 2010, the ITU launched a new Child Online Protection (COP) phase. The new phase aimed to encourage the development of national COP centers, awareness campaigns and community forums to create a safe environment for young users of the Internet. The launch of COP initiative is not unlikely related to the addictive use of the internet even among children. As at 2009, over 60 percent of children and young people at least use chat rooms daily and 75 percent of these children online are willing to share personal information about themselves and their family in exchange for goods and services. Statistically, 20 percent of these children have been identified to be targets of predators each year (ITU, 2009).

Over half a decade after setting up such guidelines, it is pertinent to measure the performance of member states based on their subscribed obligations to protect and realize the rights of children online as laid out in the UN Convention on the Rights of the Child, adopted by UN General Assembly resolution 44/25 of 20 November 1989 and the World Summit on Information Society (WSIS).

However, to the best of the researchers' knowledge, there is no existing composite indicator exclusively measuring the performance of member states on the seven critical constructs of child online protection. A child online protection (COP) composite index is crucial because it provides an evidence-based approach to policy debates on child online protection, provides an instrument that directly and promptly identifies needs and gaps in child protection systems and creates a tool for cross-national comparisons for advocacy, funding purposes and illustration of complex and sometimes elusive issues surrounding child online protection.. Composite indicators (CIs) which compare country performance are increasingly recognized as a useful tool in policy analysis and public communication.

Thus the objective of this study is to construct a composite measure which provides an intuitive understanding of the gaps in child online protection system, creates cross national comparisons for advocacy and action and explores, clarifies and summarizes in a simple manner, the complexities and multi-dimensional issues surrounding the child online protection. This makes it possible for global and local stakeholders to get a tractable and representative sense of the prevailing situation of child online protection in a given country as it stands in comparison with others. More so, converting child online protection from being largely a catchphrase to a measurable term, can spur fruitful process of dialogue over policy development and policy implementation. In the long-term, the commitment to regularly produce and update the quantitative ratings of various countries based on child online protection may facilitate communication with ordinary citizens including stakeholders in countries with both high and low internet penetration.

Conceptual Framework

The adoption of the Rio de Janeiro Declaration/Call for Action to Prevent and Stop Sexual Exploitation of Children and Adolescents at the 3rd World Congress against the Sexual Exploitation of Children and Adolescents, in November, 2008 is partly an evidence of the global recognition of the critical importance of child online protection in the era of massively-available broadband Internet. The Rio de Janeiro Declaration and other considerable body of international laws and instruments including the UN convention on the rights of the child, mandates global action to protect children both generally, and also specifically in relation to the internet.

While specific approaches to child protection vary by jurisdiction, efforts to date to protect children online have focused on four key actors namely Government/Policymakers, Industry, Parents/Guardians/ Educators and Children. For instance, specific guidelines were prepared for these four key actors by the International Telecommunications Union (ITU) and a team of contributing authors from leading institutions active in the information and communications technologies (ICT) sector and in child online safety issues such as Children's Charities' Coalition on Internet Safety (CHIS), Child Helpline International (CHI), International Centre for Missing & Exploited Children (ICMEC), Interpol and United Nations Interregional Crime and Justice Research Institute (UNICRI).

The four key actors were framed in the following ways. Government actors refers to national governments and policy making institution that are member states with subscribed obligations to protect and realize the rights of children as laid out in the UN Convention on the Rights of the Child, adopted by UN General Assembly resolution 44/25 of 20 November 1989 and the World Summit on Information Society (WSIS). The industry captures companies that are developing or providing new technology products and services. Parents, guardians and educators captures all individuals in these category including organizations such as schools, public libraries, health centers, shopping malls and major retail centers since they all provide accessible venues for the presentation of safety information.

The guidelines developed for these key actors address issues facing all persons under the age of 18 in all parts of the world since the UN Convention on the Rights of the Child defines a child as being any person under the age of 18. The UN convention on the rights of the child also applies to every child without discrimination, whatever their ethnicity, gender, religion, language, abilities or any other status and places key importance on parents, caregivers, governments and service providers

Hence the COPI framework is based the UNHR Optional Protocol to the Conventions of the Rights of the Child, the Child Pact Coalition for Child Protection, the ITU National Cybersecurity Strategy Guide Framework/Country Profiles and the Child Online Protection (COP) guideline for key actors prepared by the International Telecommunications Union (ITU) and institutions active in the information and communications technologies (ICT) sector and in child online safety issues such as Children's Charities' Coalition on Internet Safety (CHIS),

Child Helpline International (CHI), International Centre for Missing & Exploited Children (ICMEC), Interpol and United Nations Interregional Crime and Justice Research Institute (UNICRI).

From the existing framework, the study identified seven critical pillars necessary for the protection of the child online and enabling the safeties of the child. These critical pillars include declaration of a national child online protection strategy and policies, availability of information sharing and reporting mechanism between actors, availability of technical tools for children to stay safer, public education/awareness and capacity building on child abusive materials.

National strategy for COP: The national child online protection strategy describes the the possession, production and distribution of child abuse materials (CAM) in each of the countries understudy and outlines the necessary steps, programs, initiatives and other strategic plans that must be implemented to address the the demand for CAM. Ideally, it captures outlawing "grooming" or other forms of remote enticement of legal minors into inappropriate sexual contact or sexual activity; outlawing the possession, production and distribution of CAM, irrespective of the intent to distribute; taking additional steps to disrupt or reduce the traffic in CAM, for example by establishing a national hotline and by deploying measures which will block access to web sites and Usenet Newsgroups known to contain or advertise the availability of CAM. An actionable national child online protection strategy recognizes the need to commit limited resources (e.g., political will, money, time, and people) as well as providing long term support for victims.

Information sharing and reporting mechanism

Information sharing enables the exchange of actionable intelligence/information between government and all key actors. Individual nations are expected to employ cross-sector and cross-stakeholder coordination mechanisms to address critical interdependencies, including incident situational awareness and cross- sector and cross-stakeholder incident management. Ideally each nation should have a strong in rapid assistance mechanisms such as a "Notice and Takedown" regime which allows ISPs, ESPs, domain registrars and web hosts to close an offending site or cancel an email account upon request

Legislations, regulations and policies

This concept captures the existence of specific legislations that criminalize CAM which includes offences specific to the use of technology and the Internet as it relates to CAM. Ideally the legislations should also make provisions in the law for a greater commitment of resources in order to enforce these specific laws and for training for judicial, prosecutorial and law enforcement officials who will invariably be challenged to keep up with the use of technology by offenders. The adopted legislations should clearly and precisely define a child and CAM; create criminal offences and penalties for CAM possession, manufacture, distribution and/or accomplices of same.

Collaborations, cooperation, and partnerships: This refers to officially recognized local and international public and private sector partnerships; inter alia, information exchange, creation of knowledge, sharing of best practices, assistance in developing multi-stakeholder and provisions of bilateral mutual legal assistance treaties or multilateral conventions.

Technical Measures and Standards: This captures access to technical tools for children to stay safer E.g. child safety soft wares, age verification, filtering programs, parental control tools, age-differentiated experiences with password-protected content, block/allow lists, purchase/time controls, opt-out functions, filtering and moderating.

Public education and Awareness: this pillar captures evidence of established Public Education and Awareness Activities by government and industry, existence and publication of codes of good practice for all relevant stakeholders, evidence of customer education on how to manage concerns relating to internet.

Method of computation and structure of the Child Online Protection Index (COPI)

In accordance with previous work in the field of child online protection, the Child Online Protection Index (COPI) is essentially a composite indicator, aggregating 39 indicators within seven sub-indexes for an objective assessment of where each country stands in child online protection across seven critical priority areas.

To construct the sub-index, the study simply adapts elements that appear at least in two of all four ITU COP initiatives and guidelines for key actors and in at least two of the following frameworks: ITU's National Cybersecurity Strategy Guide Framework/Country Profiles, the UNHR Optional Protocol to the Conventions of the Rights of the Child the Child Pact Coalition for Child Protection, the International Centre for Missing & Exploited Children (ICMEC) annual reports on "Child Pornography: Model Legislation & Global Review, Children's Charities' Coalition on Internet Safety (CHIS), Child Helpline International (CHI), International Centre for Missing & Exploited Children (ICMEC), Interpol and United Nations Interregional Crime and Justice Research Institute (UNICRI).

Then the indicators were derived selected on the basis of the relevance of each indicator to contributing to the main objectives/framework of each sub-index and data availability/quality.

Accordingly, COPI implements an objective assessment of where each country stands in child online protection across four critical priority actors and seven pillars. The actors include government/ policy makers, industry, parents/guardian/ educators and children while the pillars include nationally recognized child online protection strategy; legislations, policies and regulations; collaboration, cooperation and partnerships; technical measures; information

sharing/reporting mechanism; public education and awareness; capacity building/ institutional support,. These seven pillars are reflected in the COPI structure which comprises seven sub-indexes measured by 39 categorical indicators. See table 1 for detailed description.

For the purpose of collecting data, the COPI uses the multiple questioning approach which are categorical only at the indicator level. For instance, to objectively explore and assess where a country stands in child online protection across the seven areas the seven areas are converted to the following questions (referred to as sub index).

a. Is there a well-articulated and operational national child online protection strategy?
b. What is the nature of legislative provisions for COP in each country
c. What technical measures and standards exist in the country?
d. Has the country ratified or acceded to cooperation, collaborations, international treaties and or multilateral conventions to combat child abusive materials (CAM)?
e. Is there an information sharing and reporting mechanisms between the government and industry?
f. What are the established capacity building, public education and awareness activities to protect children from CAM?

Afterwards, each of the above sub-index are examined in details by transforming the individual indicators to questions like the examples below

a. Existence of a national strategy for child online protection the sub-index is measured with the following items:

1. Is there an officially recognized national child online safety strategy that captures multi-stakeholders interest and identifies the need to commit limited resources (e.g., political will, money, time, and people)?
2. Is the Strategy operational? Have commercial-sector entities affected by and responsible for implementation of the plan been identified?
3. Does the COP strategy include law enforcement crime prevention strategies, school-based and social programs, and awareness strategies especially on the criminality of the production, possession or distribution of CAM?
4. Does the COP strategy include long term support for victims?
5. Is a percentage of the national GDP dedicated to child online protection?
6. Is there an officially recognized agency responsible for implementing the national COP strategy, roadmap and policy?
7. Are there officially and nationally recognized24 hours/7 days a week) national hotlines and reporting requirements?
8. Is there a nationally recognized outlaw on “grooming” or other forms of remote enticement of legal minors into inappropriate sexual contact or sexual activity?

b. Legislations, Policies and regulations: The following questions explore the area in greater detail.

1. Is there an existing comprehensive national legal framework focusing on Online Child Protection and signed into law by a president?
2. Does the existing legislation criminalize CAM?
3. Does the existing legislation make provisions in the law for a greater commitment of resources to enforce specific COP laws and train judicial, prosecutorial and law enforcement officials?
4. Does the existing legislation clearly define a 'child' and CAM?
5. Does the existing legislation create criminal offences and penalties for CAM possession, manufacture, distribution and/or accomplices of same?
6. Is there a well-established *mutatis mutandi* (body of laws which makes it clear that any and every crime that can be committed against a child in the real world can also be committed on the Internet or on any other electronic network?
7. Is there a well-articulated local and cultural online data protection and privacy rules for legal minors?
8. Are there evidences of corresponding laws to treaty agreements with other countries?

c. Collaborations, cooperation and partnerships: The following items examine this concept

1. Is there an evidence of commitments to bilateral mutual legal assistance treaties or multilateral conventions?
2. Are there evidences of existence of a cross-sector and cross- stakeholder coordination mechanisms to address critical interdependencies on child online protection?
3. Are there evidences of existing collaborations between government, industry and educators to build parents' abilities to support and speak with their children about being responsible digital citizens and ICT users?
4. Are there officially recognized public and private sector partnerships?

d. Information sharing and reporting mechanisms: The following questions explore the sub-index in greater detail.

1. Are there mechanisms (reporting schema, technology, etc.) for cross-sector incident-information sharing, both operational (near-real-time) and forensic (post-facto)?
2. Is there a "Notice and Takedown" regime that allows ISPs, ESPs, domain registrars and web hosts to close an offending site or cancel an email account upon request?
3. Is there established and widely promoted means for reporting illegal content found on the Internet e.g. a national hotline?
4. Are there reporting mechanisms for online predatory behaviour (OPB)?

e. Technical measures and standards: This sub-index is explored in greater detail by addressing the following questions:

1. An existing access to technical tools for children to stay safer? E.g. child safety soft wares, age verification, filtering programs, parental control tools, age-differentiated experiences with password-protected content, block/allow lists, purchase/time controls, opt-out functions, filtering and moderating?
2. Are there articulate findings on child rights impacts on different age groups as a result of company operations and the design, development and introduction of products and services – as well as opportunities to support children's rights online?
3. Are there national policies mandating other actors to formulate policies that protect the child online?
4. Are there technical and training support partnerships between the public and private sectors?
5. Is there an officially recognized assurance and monitoring like those -based on the Plan-Do-Check-Act (PDCA) model?

f. Education and awareness: The following items examine this sub-index in greater detail

1. Are there established Public Education and Awareness Activities?
2. Have codes of good practice for all relevant stakeholders been formulated and published via various forms of media?
3. Are existing public education efforts educating customers on how to manage concerns relating to Internet usage – including spam, data theft and inappropriate contact such as bullying and grooming?
4. Are the public education efforts describing what actions customers can take and how they can raise concerns on inappropriate use?
5. Are the public education mechanisms educating parents on how to become involved in their children's ICT activities, particularly those of younger children, for example, providing parents with the ability to review children's privacy settings and with information on age verification?
6. Are there provisions of local materials for use in schools and homes to educate and enhance children's use of information and communication technologies and help children develop critical thinking that enables them to behave safely and responsibly when using ICT services?

g. Capacity building: The following items examine this sub-index

1. Is there an officially recognized national or sector-specific research and development (R&D)?
2. Is there a well-established process for training of law enforcement officials investigating Internet for CAM?
3. Is there access to appropriate forensic facilities to enable law enforcement officials to extract and interpret relevant digital data?

4. Are there officially recognized national or sector-specific university/ professional training programs/degree in child online protection/information security or similar program for online child protection standards, best practices and guidelines to secure technical standards?
5. Is there an annual child online protection report**,** threat assessment of security and protection defying CAM?

Another consideration in the construction of the COPI is the assignment of weights to the indicators in order to produce the final index. The COPI adopts the multiple questioning approach. That is each sub-index was measured through another 4-8 sets questions (also referred to as items or indicators). For each of the items measuring a sub- index, the highest possible score is the division of 1 by the total number items measuring that sub-index. For instance, there are 8 items measuring the legislation sub index, thus the highest possible score for each indicator measuring legislation is calculated as 1÷8 (1 divided by 8) = 0.125. Reason is that COPI distributes equal weights among the seven sub-indexes and among the indicators in each sub index. Equal weighting means that each item of data used by an index is averaged in order to produce a final score. Thus, in the case of the legislation sub-index, 0.125 is the highest possible score for each indicator which indicates existence, 50 percent of 0.125 (0.0625) may be allotted to brewing efforts to establish the item while and 0 will be assigned to none existence of the item. Thus, in the case of the sum of items measuring each sub-index, such as legislation, the highest possible score is 1 and the lowest possible score is zero (zero at each sub-index level indicates insignificant performance for the country).

Summarily, all the indicators shown in table 1 are measured on a scale of 0 - 1, were 0 corresponds to non-existence (or non- availability) and 1 to best possible outcome. However, 50 percent of the highest possible score for each indicator may be assigned to that indicator if the data shows efforts towards establishing the best possible outcome.

In the case of the sum of all sub-indexes, the highest possible score is 7 indicating stiff resistance against child abusive materials and insistent protection of the child online. The lowest possible score zero at this level indicates compromise of a child's safety online and high exposure of children in such country to CAM.

Calculating final score

The final computation of the COPI is based on successive aggregation of scores; from the indicator level (i.e. the most disaggregated level) to the COPI score (i.e. the highest level). Unless otherwise noted, arithmetic mean may be used to aggregate individual indicators under each sub index and also for higher aggregation levels (sub-indexes). Hence, the final COPI score of each nation is a simple average of the seven composing sub index scores, while each sub index's score is a simple average of those of the composing indicators. In doing this, we assume

that all Index sub-indexes give a similar contribution to a national child online protection endeavor

The highest possible average score 7 indicates national stiff resistance and insistent protection against child abusive materials (CAM). The lowest possible score zero at this level indicates excessive compromise of a child's safety online and exposure of children in such country to CAM. However average scores below 3.5 indicates feeble and jerry-built attempts to protect the child online and average scores above 3.5 but below 5 indicates robust and creditable efforts to protect the child online.

Throughout the use of the instrument, scores in the various dimensions can be reported with a precision of three decimal points.

It is important however to state that another phase of this study accounts for series of diagnostic tests to demonstrate the robustness of the new measure and assess the degree of construct validity.

Table 1 Structure of the Child Online Protection Index

S/N	Sub index	Indicators	Weights	Few Data Sources
1.	**Declaration of a national strategy for child online protection**	• Existence of an officially recognized and operational national child online safety strategy that captures multi-stakeholders interest and identifies the need to commit limited resources (e.g., political will, money, time, and people)	**1/8**	**Primary sources: field survey, content analysis of selected internet-related national and company policies and internet related regulatory organizations** **Secondary sources: National data sets on child online protection;** (ITU) National Cybersecurity Strategy Guide Framework/Country Profiles; The International Centre for Missing & Exploited Children (ICMEC) annual reports on "Child Pornography: Model Legislation & Global Review
		• Identification of commercial-sector entities affected by and responsible for implementation of the plan		
		• Evidence that COP strategy includes law enforcement crime prevention strategies, school-based and social programs, and awareness strategies especially on the criminality of the production, possession or distribution of CAM	**1/8**	
		• Evidence that the strategy includes long term support for victims	**1/8**	
		• Existing percentage of national GDP dedicated to child online protection?	**1/8**	
		• Evidence of an officially and nationally recognized24 hours/7 days a week) national hotlines and reporting requirements	**1/8**	
		• Evidence of national of outlaw on "grooming" or other forms of remote enticement of legal minors into inappropriate sexual contact or sexual activity.	**1/8**	
		• An officially recognized agency responsible for implementing the national COP strategy, roadmap and policy	**1/8**	

2.	**Legislations, regulations, policies**	• Evidence of an existing comprehensive national legal framework focusing on Online Child Protection passed and signed into law by a president	**1/8**	**Primary sources: field survey, content analysis of selected internet related national/regulatory and company policies Secondary sources: National /international data sets on child online protection,** (ITU) National Cybersecurity Strategy Guide Framework/Country Profiles; The International Centre for Missing & Exploited Children (ICMEC) annual reports on "Child Pornography: Model Legislation & Global Review
		• Evidence of legislations that criminalize CAM	**1/8**	
		• Evidence of legislations that make provisions in the law for a greater commitment of resources to enforce specific COP laws and train judicial, prosecutorial and law enforcement officials	**1/8**	
		• Does existing legislation clearly define a 'child' and CAM?	**1/8**	
		• An existing legislation that creates criminal offences and penalties for CAM possession, manufacture, distribution and/or accomplices of same?	**1/8**	
		• An existing well-established *mutatis mutandi* (body of laws which makes it clear that any and every crime that can be committed against a child in the real world can also be committed on the Internet or on any other electronic network.	**1/8**	
		• Evidences of corresponding laws to treaty agreements with other countries?	**1/8**	
3.	**Collaborations, cooperation, and partnerships**	• Evidence of commitments to bilateral mutual legal assistance treaties or multilateral conventions?	**1/4**	**Primary sources: field survey, content analysis of selected internet related company policies and internet related regulatory organizations Secondary sources: National /international data sets on child online protection;** (ITU)
		• Evidences of cross-sector and cross- stakeholder coordination mechanisms to address critical interdependencies on child online protection	**1/4**	
		• Evidences of existing collaborations between	**1/4**	

		government, industry and educators to build parents' abilities to support and speak with their children about being responsible digital citizens and ICT users • Existence of officially recognized public and private sector partnerships	**1/4**	National Cybersecurity Strategy Guide Framework/Country Profiles
4.	**Information sharing and enforcement mechanism**	• Existence of mechanisms (reporting schema, technology, etc.) for cross-sector incident-information sharing, both operational (near-real-time) and forensic (post-facto)	**1/4**	**Primary sources: field survey, content analysis of selected internet related company policies and internet related regulatory organizations** **Secondary sources: National data sets on child online protection,**
		• Evidence of a "Notice and Takedown" regime to allow ISPs, ESPs, domain registrars and web hosts to close an offending site or cancel an email account upon request	**1/4**	
		• An evidence of an established and widely promoted means for reporting illegal content found on the Internet e.g. a national hotline	**1/4**	
		• Existing evidence of reporting mechanism for online predatory behaviour (OPB)	**1/4**	
5.	**Technical Measures and Standards**	**a.** An existing access to technical tools for children to stay safer? E.g. child safety soft wares, age verification, filtering programs, parental control tools, age-differentiated experiences with password-protected content, block/allow lists, purchase/time controls, opt-out functions, filtering and moderating.	**1/5**	
		b. Existing articulate findings on child rights impacts on different age groups as a result of company operations and the design, development and introduction of products and services – as well as opportunities to support	**1/5**	

		children's rights online	
		c. Evidences of child protection national policy for other actors policy formulations and commitments (e.g., human rights, privacy, marketing and relevant codes of conduct).	**1/5**
		d. Evidence of technical and training support partnerships between the public and private sectors	**1/5**
		e. An officially recognized assurance and monitoring like using the ISO/IEC 27001-based Plan-Do-Check-Act (PDCA) model	**1/5**
6.	**Public Education and Awareness**	• Evidences of established Public Education and Awareness Activities by government and industry	**1/6**
		• Evidence of creating national awareness on the criminality of the production, possession or distribution of CAM	**1/6**
		• Existence and publication of codes of good practice for all relevant stakeholders	**1/6**
		• Evidence of customer education on how to manage concerns relating to Internet usage – including spam, data theft and inappropriate contact such as bullying and grooming –	**1/6**
		• Evidence of parent public education on how to become involved in their children's ICT activities, particularly those of younger children, for example, providing parents with the ability to review children's privacy settings and with information on age verification.	**1/6**
		• Existing provision of local	**1/6**

		materials for use in schools and homes to educate and enhance children's use of information and communication technologies and help children develop critical thinking that enables them to behave safely and responsibly when using ICT services		
7.	**Capacity Building**	• An officially recognized national or sector-specific child online protection research and development (R&D) programs/projects at universities with a dedicated percentage of GDP or Government Project.	**1/5**	**Primary sources: field survey, content analysis of selected internet related company policies and internet related regulatory organizations Secondary sources: national data sets on child online protection,**
		• An officially recognized national or sector-specific university/ professional training programs/degree child online standards, best practices and guidelines to secure technical standards	**1/5**	
		• Evidence of a well-established process for training of law enforcement officials investigating Internet for CAM?	**1/5**	
		• Existing access to appropriate forensic facilities to enable law enforcement officials to extract and interpret relevant digital data	**1/5**	
		• Evidence of an annual child online protection report**,** threat assessment of security and protection defying CAM	**1/5**	

Conclusion

It suffices to state that COPI only seeks to measure the existence of each indicator in each country and thus ranking should be based on existence not the quality or effectiveness of such indicators to protecting children online in any nation. Nonetheless, examining the effectiveness of these efforts may be an important gap for subsequent studies.

More so, the seven pillars outlined above do not constitute the only means of dividing the broad construct of child online protection, but one that is conceptually coherent and in accordance with previous work in the field

References

International Telecommunication Union. (2009). The ICT Development Index. Measuring the information society. Geneva. Retrieved from https://www.itu.int/en/ITU-D/Statistics/Documents/publications/mis2009/MIS2009_w5.pdf

United Nations Human Right (2000) UNHR Optional Protocol to the conventions of the rights of the child. Retrieved from www.ohchr.org/EN/professionalinterest/Pages/OPACCRC.aspx

International Telecommunication Union. (2016) Child online protection. Retrieved from www.itu.int/en/cop/Pages/defaault.aspx

Wamala, F. (2011) ITU National Cyber security strategy guide. International Telecommunication Union. Retrieved from www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecuritystrategyGuide.pdf

International Telecommunication Union (2010). Child Online Protection statistical framework and indicators. Retrieved from www.itu.int/dms-pub/itu-d/opb/ind/D-IND-COP.01-11-2010-PDF-E.pdf

International Telecommunication Union (2009) Guidelines for Policy Makers on Child Online Protection. Retrieved from https://www.itu.int/en/cop/Documents/guidelines-policy%20makers-e.pdf

International Telecommunication Union (2014) Guidelines for Industry on Child Online Protection. Retrieved from https://www.itu.int/en/cop/Documents/bD_Broch_INDUSTRY_0909.pdf

Dasuki, M., S., (2014) National Cybersecurity Policy. Retrieved from https://cert.gov.ng/images/uploads/NATIONAL_CYBESECURITY_POLICY.pdf

International Telecommunication Union. (2009)The World in 2009: ICT facts and figures. Retrieved from https://www.itu.int/ITU-D/ict/material/Telecom09_flyer.pdf