PROTECTING CHILDREN IN A DIGITAL AGE:

THE MISUSE OF TECHNOLOGY IN THE ABUSE AND EXPLOITATION OF CHILDREN

(PAPER PRESENTED AT THE TWENTIETH SESSION OF THE CCPCJ-VIENNA, 11-15 **APRIL 2011**

BY DORCAS ODUOR SDPC (KENYA)

(Thematic discussion on protecting children in a digital age: the misuse of technology in the abuse and exploitation of children)

1. It is no longer moot that the Internet is a medium through which a variety of computer-related crimes and other forms of child abuse and exploitation are perpetrated. These morally and legally reprehensible activities include child pornography, and other sexually explicit and offensive material aimed at luring children into deviant behavior or outright criminal conduct. Child prostitution and sex tourism are closely associated with cyber crime, as indeed is the recruitment of children and young people into terrorist organizations and/or organized criminal gangs. The technology is also used to recruit couriers for narcotic drugs. This whole scene is a worldwide phenomenon. However, it is more prevalent in the West because the *per capita* access to computers is greater than in developing countries. For that reason alone, it is not an over-simplification to say that more cases of child abuse and exploitation of the insidious kind, using computers, have been recorded in the more affluent societies.

2. However, that is not to say that there are no cases of abuse and exploitation of children, using new digital media and technologies in developing countries. Indeed, it is probably true to say that the danger is probably much more heightened in the developing world. The reason is simply that, while the risk factors are the same as, or equal to, those confronting juveniles in the West, there are fewer

mechanisms for the protection of a similar group in developing countries. The causes of this situation are probably beyond the scope of this discussion, and I will not deal with them here.

3. One of the major ways by which governments have sought to confront the scourge of cyber-crime has been in the promulgation of appropriate legislation. In Kenya, for instance, for the first time since the country's independence, on 27th August, 2010, a new Constitution was promulgated in which there has been specific recognition of children's rights. A 'child' is defined as meaning, an individual who has not attained the age of 18 years. Under Article 53 of the Constitution the rights which accrue to children include protection from abuse, neglect, all forms of violence and inhuman treatment. The language employed is sufficiently wide to cover the whole range of responsibility by parents, teachers or any other people who may be in the position of such authority figures. It is also likely to apply notwithstanding any weakness or gaps in any legislation. The Constitution also makes all those rights justifiable *per se,* the paramount consideration only being a child's best interest. To make robust the implementation of those provisions and other laws, the Constitution goes further to require that the administration of all laws must be subject to and governed material values and principles of governance which include human dignity, human rights and protection of the marginalized (Art 10(2)(b)). And, finally the Constitution imports the general rules of international law are automatically part of the law of Kenya as is any treaty or convention ratified by Kenya (Art. 2(5) and (6); **Macharia v. R.G. Appeal No. 497 of 2007)**. In the premises, on paper at any rate, there appears to be adequate legislative provision for the prevention and protection of children against abuse or exploitation.

4. The main statute relative to children is the Children Act (No. 8 of 2001). It provides for a child's right to parental care (s. 6);

entitlement to protection from both physical and psychological abuse, neglect and any other form of exploitation including sale, trafficking (s 13); protection from sexual exploitation and use in prostitution, inducement or coercion to engage in sexual activity, and exposure to obscene materials (s. 15). These provisions, read together with those of the Kenya Communications Act (No. 2 of 1998) provide a strong legislative framework for the protection of children against abuse and exploitation. Section 29 of the Act makes it an offence, punishable by imprisonment and/or fines, for a person who by means of a licensed telecommunication system (which means a system for the conveyance, through the agency of electronic, magnetic, electro-magnetic, electro-chemical or electro-mechanical energy) sends a message or other matter that is grossly offensive or of an indecent, obscene or menacing character.

5. Yet, notwithstanding that the legal framework, a huge swathe of challenges still remain, making the effective enforcement of preventive measures very difficult. Ironically, one of the greatest challenges is subsumed the greatest need for most emerging nations, namely, education. So important is education – as the basic vehicle for national development – that in Kenya, entitlement to free and compulsory basic education is a fundamental constitutional right (Art 53(1)(b)). The pride of most schools is the introduction into their curriculum of information and communication technology (ICT) studies, which, in turn, exposes children at a very early age to computers and – inevitably – to the Internet. The dilemma which faces the schools, therefore, is how to regulate the learning so as not to put the children in danger of predators. This, taken in light of waning parental authority over their school going children (particularly in rural communities in which illiteracy is rife amongst the older members of the community, who then defer to their more educated children –notably sons - in a phenomenon which sociologists have dubbed "social inversion") means that the children are often

unsupervised by their parents, and left very much to their own devices In the circumstances, while one of the preventive measures against abuse in the digital world is parental supervision, in the context outlined above none exists and so children have almost absolute freedom to do what they like. Their urban counterparts are often too immersed in the rat race to give any or any sufficient, time to their children. They would rather the children were well occupied with video and computer games than interrupt their busy schedules.

6. The next big challenge is the sheer size of the problem. The perpetrators of the crimes do not use only one form of medium to reach the children. Apart from computers, there are mobile phones. For instance, the expansion of mobile telephony in Kenya is so massive and rapid that investigators struggle to keep up with the contraband being conveyed within this medium. . It is estimated that about three out of every five young people in the rural areas, and four and a half of their counterparts in the urban centers, own at least one mobile phone. In a period of less than thirty years the virtual environment in Kenya has moved from a single mobile telephone service provider to three, with an ever expanding coverage to the remote reaches of the rural countryside. And, the advent of number portability, and the accompanying ease with which a person may move from one service provider to another, heralds the explosion in the number of users(most of whom are mainly young people) coming into the market in very near future. It is estimated that as many as 15 million additional users are expected to join in. The falling cost of telephony, in the wake of the infernal price wars currently being waged between service providers, it is now relatively cheap to make a call, and even cheaper to send a short text message. Thus accessibility to very young ages has grown exponentially in the recent times.

7. This situation is exacerbated by the increasing sophistication of the methods by which predators are able to reach and prey on young people. The fact that it is possible to send text messages from an intermediary source, thereby camouflaging the real sender, means that the criminals are able to disguise their identities – initially, at any rate – and assume that of a trusted friend or relative is peculiarly worrying. Ever increasing incidents of thugs calling members of the family or friends of somebody and informing them to go to a particular location where they are then robbed is gaining currency in Kenya. So, are cases of hackers invading the phone book of a computer user and pretend to be their friend or relative in financial trouble needing help. To detect, analyze and inhibit these kinds of activities requires equipment and knowledge which is not readily available in the criminal justice systems of many poor nations. Such resources as may be available are often stretched to the limit. Often investigators have to make an election as to the crimes to be investigated, given the capacity available. It is not surprising that priority will usually fall upon the crimes which can be investigated within the investigator's known competencies. It is to those areas the fight against lawlessness is likely to be directed, and much less against cyber-crime, which is likely to be more complex.

8. The size of the problem does not denote only the sophistication of the offences. It is more typically the volume of the material which is hurtling through cyberspace. While the writer has not been able to ascertain the number of short text messages which are exchanged in Kenya on any one day, there is no doubt that they are in millions. One service provider who operates mobile money transfer service has mentioned that up to Kshs. 900,000,000/- is transferred throughout the country in any one day. The maximum amount which could be transferred by any one message is Kshs.30,000/-. This would put the number of transactions to 30,000 a day. If that figure is extrapolated to the three service providers, it would come up to 90,000 short

texts. But that is only in respect of money transfers. These are the minority, the bulk being the usual social texts. And, this gives some idea about the volumes of the texts which the investigators have to scrutinize in order to detect criminal content.

9. Indeed it is also on the question of criminal content which lies more complexity. The language used by the predators is usually esoteric and enigmatic, and is deliberately so to avoid detection. Local investigators need to know the language used by criminals engaged in cross-border cyber-crime. Even locally, while employing common words to convey their messages criminal gangs will have meanings of words which are specific to their trade. Accordingly, the detection, apprehension or the inter-diction of suspects tests both the investigative and prosecutorial environment almost in equal measure. Hence the need for investigators to train in the methods used by criminals and the language employed to undertake their activities. Without the collaboration of the much more advanced jurisdictions, the combat against cyber-crime becomes a mere pipe dream.

10. The collaboration may take many forms. It could be the sharing of information or intelligence, training courses and/or mutual legal assistance. Training the investigators is a good start, but is in itself insufficient. Where some evidence has been uncovered, and is available, there is need for units of specialized prosecutors, well versed in the intricacies of prosecutions of this nature, to undertake the prosecutions. Experience in Kenya, where a vast majority of criminal cases (which are heard in Magistrate Courts) are prosecuted by police officers, has shown that the prosecutors are almost always without any special training in tackling cyber-crime cases. The success rate in such prosecutions has not been impressive, even deplorable. The fact that, it is usual that these crimes are committed by well organized and well funded criminal groups, which are adept at concealing not only their identities but also their

localities, calls for prosecutors who not only know how the integrity of the secured evidence may maintained before and throughout the trial in court.

11. Interdiction is another problem. Whereas some successes have been recorded in cases in which the police, acting in conjunction with internet service providers (ISP), have been able to trace and capture perpetrators of offences who are using mobile phones, such successes have not been seen much with respect to computer crime. This is certainly another sector which would benefit from the collaboration with other stronger law enforcement agencies.

12. These digital offences are by definition borderless. Investigators have to contend with laws min different jurisdictions and the complex conflict of laws issues which arise. There are times when cross-border co-operation is not as easy, or even possible. Where there is no legitimate or recognized authority in a neighboring State, or if it is in turmoil, tracing back into the country may prove difficult. The instant nature of the communication, across wide expanses of territory -sometimes across continents - and the ubiquitous ness of the perpetrators, greatly widens the areas for which international co-operation is required. It also exposes the need for inter-agency co-operation both within national borders and internationally. The detection or interdiction of cyber-crime cannot be restricted to only one agency, such as the police. There must be cross-pollination, not only of ideas and intelligence but on all fronts. The crimes are far too sophisticated and widespread for any one agency, acting alone, to combat with any degree of success. Thus, the police would require the assistance of tax as well as customs and immigration authorities. It is the only way by which the anonymity of the perpetrators can be infiltrated and exposed. The inter-agency co-operation would also instigate and encourage them to look more critically into their areas of specialization, hopefully leading up to a

culture of research and development in both investigative and prosecutorial efforts.

13. Further, in order to combat the vice of the misuse of technology to abuse and exploit children, there must be greater advocacy. The co-operation of internet service providers will be required. There is a general reluctance by ISPs to do that. They see this as an invasion of the privacy of their clients and customers. It may also negatively impact their businesses. A ready example of this was the strong objection which Blackberry voiced against requests by some governments in the Middle East and Far Eastern Asian governments to decipher some of their material. There is a clear conflict of interest between the needs of an investigator into cyber-crime and a supplier bound by fiduciary responsibilities. In view of the expansive Bill of Rights in the Constitution of Kenya, this becomes are real concern. It is noteworthy that in particular, Article 24, which provides for the limitation of rights and fundamental freedoms, only allows such infraction only by law which is justifiable in an open and democratic society based on human dignity, equality and freedom, taking into account all relevant factors, including the nature of the right or fundamental freedom; the importance and purpose of the limitation; the need to ensure that the enjoyment of rights and fundamental freedoms by any individual does not prejudice the rights and fundamental freedoms of others; and the relation between the limitation and its purpose and whether there are less restrictive means to achieve the purpose. Obviously, it would take a rigorous exposition of the law in a constitution reference to deal with all the issues which would be thrown up by an application to compel an ISP to permit intrusion by the law enforcement agency.

14. There is also the reticence by parents and guardians to go public on crimes relating to their children or wards. This is usually on the fear of stigmatization of the child, should it be known that he or she has

been a subject of abuse or exploitation. This is despite sterling attempts by the law and law enforcement agencies to keep confidential the identities of victims of such abuse or exploitation. The lack or paucity of good counseling services for both the victims and their relatives will continue to make this a major drawback to the fight against pedophilia.

15. There is a lot more which one could say on this subject. It is a fast evolving area of concern, not only for law enforcement authorities, but also for families, communities and nations. Never before has a more insidious foe wormed its way into the very fabric of what makes us us. The virus engendered by child pornography, for example, not only propels them into anti-social, promiscuous activity, but eventually leads to violence, and degrades them as people, both in the eyes of others, and, worse still, in their own. I cannot conceive of anything more dangerous than a person who sees no worth in himself or herself. Ultimately, unless dealt with firmly, this vice promises to unleash upon the entire civilization an apocalypse big enough to destroy the human race. And that is no exaggeration. We have no choice but to confront this germ with everything at our disposal.

DORCAS ODUOR
SENIOR PROSECUTION COUNSEL
KENYA