**Comment on the Concept Note for a General Comment on Children’s Rights in relation to the Digital Environment:**

**Protecting children’s rights through detection of child sexual abuse material in the workplace**

*The following comment focuses on the general principle of the right to life, survival and development. It more specifically focuses on the key group of rights: ‘Protection from violence, sexual exploitation and other harm’. It addresses how businesses operating in the digital environment can support the realisation of children’s rights, how States can better fulfil their obligation to children’s rights in relation to the digital environment, and how securing children’s rights in the digital environment is integral to realising children’s rights in other environments.*

**Abstract/Summary**This comment outlines the growing problem of child sexual abuse material and the importance of working in tandem to safeguard children and stop the spread of the material. As child sexual abuse material is distributed and accessed through all available channels, it is becoming increasingly important that all stakeholders, from States to businesses, take effective and concrete action to curb the problem. The workplace has been identified as a risk environment with a unique position to act on this issue. 1 in 500 work computers are used to handle child sexual abuse material. By installing software that can detect this, organisations can protect themselves from crime and risk, also making it possible to identify and safeguard children. Detection on the work computer is also an effective way to overcome the problems otherwise presented by encryption and anonymisation technologies (such as the Darknet), where many other technologies fall short.

***The research basis – The NetClean Report****The primary research basis for this comment is the NetClean Report, a yearly report on child sexual abuse crime produced by NetClean. It is based on a survey with law enforcement professionals working with child sexual abuse crime in more than 30 countries across the world. The 2018 report also included an interview survey with businesses that detect child sexual abuse material on the work computers in their IT-environment. Together those businesses represented nearly 270,000 work computers with software installed to detect child sexual abuse material.*

*The NetClean Report 2018:* <https://www.netclean.com/netclean-report-2018/>

*The NetClean Report 2017:* <https://www.netclean.com/netclean-report-2017/>

*The NetClean Report 2016:* <https://www.netclean.com/the-netclean-report-2016/>

**Digitalisation, connectivity and child sexual abuse material**One of the key areas when considering children’s rights is the right to ‘protection from violence, sexual exploitation and other harm’. Child sexual abuse and child sexual abuse material is central to this.

Increasing digitalisation and connectivity, global internet penetration and easy access to devices such as laptops, smartphones, tablets and thumb drives, has led to countless positive developments and opportunities. However, as is always the case, technology can be used for both good and bad, and this development has also resulted in an immense increase in the volumes of and accessibility to child sexual abuse material.

Three quarters of the surveyed police officers in The NetClean Report 2017 reported an increasing and more demanding workload, primarily due to more investigations and more data. They also reported that their biggest investigations can contain up to a 100 million images, of which 10 million are child sexual abuse images.

**Child sexual abuse material – crime scene and re-victimisation**Child sexual abuse material goes far beyond just being an image or a video. It is a documented crime scene of a serious crime that has extensive and long-term negative impact on the quality of life for the victim depicted. As terrible as the image is, it also presents the opportunity to identify both the child and the perpetrator to ensure that the child is safeguarded. This makes every detected image important.

The spread of child sexual abuse images also causes re-victimisation. A Swedish study by Jonsson, L. and Svedin, C-L. *Barn utsatta för sexuella övergrepp på nätet [translation: Child victims of online sexual abuse]* *(2017)* showed that children who have been sexually abused are even more traumatised if they know that the abuse has been documented. The trauma is further accelerated if they also know that the images have been disseminated online. As a result, it is important that every measure is taken to limit the spread of child sexual abuse material.

**Distribution and consumption of child sexual abuse material**Child sexual abuse material is distributed through all possible channels. It is also downloaded, consumed and distributed through all times of the week and day.

The NetClean Report 2016 showed that peer-to-peer (P2P) is the most common way for child sexual abuse to be distributed (it was mentioned by 90.4% of the surveyed police officers), followed by Darknet/TOR (43%), social media platforms (37.9%), cloud-based services (34.9%), instant messaging (34.9%), e-mail (21.3%), websites on the open internet (17.3%) and physical mail (6.3%).

Also in the 2016 report, the Swedish Internet Service Provider (ISP) Tele2 shared that they blocked 500,000 searches for known websites showcasing child sexual abuse material every month. Data in the 2017 report from ISPs from around the world, show that searches for such websites take place every day of the week, 24 hours a day. There is a peak in searches on Sundays, and also between 10pm and 1am.

The NetClean Report 2018 added the patterns of child sexual abuse material being handled on work computers. It showed that it was most common that employees use their work computer to handle such material outside of working hours, during evenings, holidays and work trips.

**The challenge of anonymisation technologies**  
One of the major challenges to find child sexual abuse material, as well as identify and safeguard children, is encryption and anonymisation technologies such as TOR, VPN and proxy servers. Encryption is a challenge as it is impossible to detect and stop child sexual abuse images in encrypted traffic. Anonymisation technologies are a challenge because they disguise the identity of the user. In the NetClean Report 2016, more than one third of the surveyed police officers pointed to encryption and anonymisation as one of the major challenges and an increasing trend.

**Technologies to stop child sexual abuse material**Law enforcement, policy makers, civil society, NGOs, academic researchers, public sector organisations and private industry all work to try to solve this issue and protect children from harm. However, much more can be done. One of the first steps is to use available technology in the most effective way. Law enforcement tools apart, there are a number of technologies available that are used today to address the problem from different angles, such as crawlers, blocking technologies, filter technologies, artificial intelligence, robust hashing technologies and binary hashing technologies. Those technologies all have strengths and limitations, depending on the context in which they are used. More information on the different technologies and how they work is gathered here: <https://www.netclean.com/technical-model-national-response/>.

Different technology platforms simultaneously present both a risk and an opportunity in tackling this issue. For example, Internet Service Providers (ISP) present a risk as child sexual abuse material is shared through the ISP networks. However, the ISP technology platforms also provide the opportunity to block the material and stop it from spreading. Similarly, the work environment is a risk environment where child sexual abuse material is being handled and shared, but it also presents an opportunity to detect material and safeguard children.

**Technology used to detect child sexual abuse material on work computers**Software that is designed to specifically detect child sexual abuse material can be installed to detect when someone handles child sexual abuse material on a work computer. The software works similarly to an antivirus programme, but instead detects child sexual abuse material. To identify the images, hashing technology is used. When law enforcement investigates child sexual abuse cases, they produce a hash, a unique ‘digital fingerprint’, of each image. These hashes are then added to a database, which is used in the software to match against images handled on the work computer. This means that the software installed on the work computer only detects child sexual abuse material that has been classified by law enforcement. At detection, an alert is sent to designated individuals within the organisation (business or public sector organisation) who handle the incident and report to police.

**The workplace is a risk environment**1 in 500 work computers are used to handle child sexual abuse material (The NetClean Report 2018).

In addition, nearly two thirds of the police officers surveyed in the NetClean Report 2017 answered that offenders in their investigations are usually in employment. The report also showed that offenders come from all professions, all levels within organisations and all segments of society.

This means that organisations are in a unique position to stop crimes from being committed with the use of company devices, while acting as an ethical corporate citizen and safeguarding children. Where many other technologies fall short, detection on work computers is also an effective way to circumvent the problems presented by encryption and anonymisation technologies (such as the Darknet).

It might seem strange that people are willing to risk using their work computers to commit this type of crime. The risk is probably negated by the fact that the work computer is perceived as private. It is not shared with anyone else, neither family members nor colleagues, and it is often a laptop.

The report showed that the most common way of accessing the material is via a USB-stick. It also showed that most frequently the person has turned off the Wi-Fi and disconnected the computer from the network. The average software ‘alert’ is usually for 2-5 images, or sometimes up to 20 images. However, when the computer is examined more closely, more material is usually found. And when detection of images results in a house search, this also frequently unearths more child sexual abuse material in the home (NetClean Report 2018).

**Concrete action by States and businesses to protect children’s rights**Protecting an organisation’s IT-environment by using software to detect child sexual abuse crime, is a concrete action that sustainable, ethical businesses and States can take to protect children’s rights.

States and public sector organisations are in addition responsible for children in their care and must take necessary steps and precautions to ensure that children are protected while in school, daycare, hospital or other public organisation. While consumers of child sexual abuse material and child sexual offenders can be of any age or occupation, one third of the police officers in the NetClean Report 2017 reported that, in their experience, it is more common that offenders work in professions with close proximity to children.

It is also interesting to note that nearly one in five police officers (NetClean Report 2017) stated that offenders that work in professions that require a high degree of knowledge of IT are more common. This experience was mirrored in the business interviews in the 2018 report.

**Safeguarding children against physical sexual abuse**By detecting child sexual abuse material in the workplace, it is also possible to safeguard children against physical sexual abuse in other environments than the digital. Although there is a debate as to the exact number, there is a 30-80 percent correlation between viewing child sexual abuse material and committing hands-on/physical child sexual abuse. Michael C Seto, a Canadian forensic psychologist and author, found in a meta-analysis that more than 50 percent of those who consume child sexual abuse material also commit hands-on offences against children (NetClean Report 2016). Furthermore, 80-90 percent of all child sexual abuse is committed by someone who is known the child, such as a family member or someone else that comes into contact with the child. (The Bureau of Justice Statistics: <https://www.bjs.gov/content/pub/pdf/saycrle.pdf>).

**Conclusion**The work place is a risk environment for sexual exploitation of children. Organisations, States and businesses alike, are in a unique position to take concrete action to protect the rights of children by detecting child sexual abuse material on work computers. Different stakeholders need to contribute to the safeguarding of children in different ways and the workplace environment is a key piece of the puzzle to ensure a brighter future for children.

***About the author/NetClean****NetClean, headquartered in Gothenburg, develops world-leading technology to protect businesses and organisations from child sexual abuse material being handled in the companies’ IT environment. With the help of hash technology, their solution detects child sexual abuse material on the company’s work computers. The technology is used in over 110 countries by big businesses, multinational companies and public sector organisations.*