CEO Coalition to Make the Internet a Better Place for Kids

eNACSO's response to the working groups' interim reports

For more information:
European NGO Alliance for Child Safety Online
Save the Children Denmark
Rosenørns Allé 12
DK-1634 Copenhagen V
info@enacso.eu
www.enacso.eu

eNACSO European NGO Alliance for Child Safety Online

Formateret: Højre

Introduction

When Commissioner Kroes announced the formation of the CEO Coalition on 1st December, 2011, eNACSO applauded both her vision and her determination to push forward the online child safety agenda but within a tight timetable of 18 months. We also praised the evident desire of so many companies to co-operate with the Commissioner's plans. This positive outlook had been prefigured in several companies' earlier decision to create the ICT Principles Coalition which set its focus on a longer timeframe.

The CEO Coalition established five separate working groups:

WG 1: Reporting tools
WG2: Age appropriate privacy settings
WG3: Content classification
WG4: Parental controls
WG5: Notice and take down
eNACSO participated in each group.

Each working group was tasked with bringing forward recommendations for improvements under each of the five headings. The emphasis was placed on practical action and on finding solutions, less on debating structures, frameworks or philosophies.

We welcome and commend Commissioner Kroes's emphasis on achieving results. However, in our view the process has brought into sharp relief a number of broader issues which must be addressed at some point.

The working groups are industry led. Industry members are committed to implementing the recommended outcomes by June, 2013. A major interim review of progress is set for 11th July, 2012, and this paper has been prepared to assist and inform that review. Herein we present copies of the final comments submitted by eNACSO to each individual working group, together with some general observations arising from the process.

For more information:
European NGO Alliance for Child Safety Online
Save the Children Denmark
Rosenørns Allé 12
DK-1634 Copenhagen V
info@enacso.eu
www.enacso.eu

Formateret: Dansk (Danmark)

Formateret: Højre

Overview

Summary

1. eNACSO welcomes the progress being made by the CEO Coalition but is concerned about the uneven levels of engagement by individual companies and working groups.

2. There is a need to start thinking about how the results of these processes will be followed through, in particular with regard to companies not involved or only lightly engaged in the Coalition. For example, could the EU's purchasing power be used to incentivise best practice?

3. Consideration should be given to creating a new body, or a division in an existing one, to be given on-going responsibility for driving forward policy in this space linked to powers to make binding determinations in certain cases.

4. There is a need for research into the ages at which different competencies develop for children and young people to make a range of judgements about how to engage in the online environment.

1. There is a great deal in the CEO Coalition's activities which has been and continues to be very welcome and positive. In a document of this nature it is neither appropriate nor necessary to start listing all the many palpable achievements of the Coalition up to this point. Here we are going to focus on how we can make an even greater success of the process as a whole.

   Thus, at the time of writing, while we have yet to see all of the reports which will be made to 11th July's interim review meeting, we have seen some and a number of concerns have come to the surface. These need to be addressed before the process can be satisfactorily completed.

2. The absence of very many companies from the Coalition processes leaves no room for complacency. But even among those companies that are participating there are very uneven degrees of engagement. This is evident in the nature of some of the working groups' reports.

3. An obvious concern, therefore, questions how the results of the CEO Coalition's self-regulatory process are to be carried forward to companies who are not part of the process or are weakly attached to it?

Formateret: Højre

4. How is compliance or co-operation of the not present or the barely present to be secured if the possibility of new laws and regulations to enforce them are expressly disavowed?

5. If companies confidently expect no follow through action or effective scrutiny there is a real concern that the work of the CEO Coalition will quietly fade away.

6. In the UK, we have witnessed an example of one company, Sulake, owners of Habbo Hotel, breaching their obligations as signatories to the Safer Social Networking Principles. Sulake are also currently parties to the CEO Coalition.

7. eNACSO recommends that the Commission should consider making positive use of its purchasing to power to incentivise good practice. Companies that refused or failed to observe acceptable standards could become ineligible to tender for contracts. Deploying purchasing power to leverage or secure policy goals is a method that is not uncommon in both the public *and* private sectors e.g. to encourage "green" habits or to discourage child labour or other unethical methods in manufacturing or supply processes.

8. The most substantial overarching point we wish to make concerns an aspect of policy to which we refer in our submission to Working Group 3 on content classification. Professor Sonia Livingstone of the LSE has also made a similar observation.

9. The CEO Coalition process presents a timely opportunity for the EU to consider creating a new public interest body, or establishing a new division within an existing one, which could be given specific responsibility for driving forward policy and monitoring implementation in the online child protection space. It should also be given a power to make binding determinations in respect of a range of questions connected with children's use of the internet.

10. European institutions and national Parliaments would retain their rights, their role, their *duty* to make laws or local decisions but, in the context of the way the EU's single market policies work and global markets operate, it is clear to us that all of the major companies share eNACSO's view that much could be gained from an efficient pan-European approach. Smaller countries, smaller markets, often find it difficult to catch the attention of large multi-nationals. A body of the kind we have in mind could help correct that.

11. Any new body would need to be independent of the Commission and at least arms-length from any and all political institutions. It would need to be able to win and retain the confidence of a wide range of stakeholders, not the least of these being the free speech and civil rights communities.

12. If this does not happen, if we fail to separate discussions on the implementation of public policy from the processes by which the policies are determined, we will constantly be bedevilled by understandable anxieties about motives, hidden

Formateret: Højre

agendas and the usual suspicions which are a feature of robust, democratic political life.

13. A new, independent body would need to be properly established and have the capacity to deal with complex challenges, weighing competing claims against each other, initiating evidence gathering or analysing evidence published by third parties, and reaching a final view which would be accepted as being reasonable by the great majority of people.

14. In the USA the Federal Trade Commission has considerable powers to intervene in internet related matters, for example to determine whether or not individual web sites are covered by the provisions of Children's Online Privacy Protection Act and also to determine whether or not particular solutions that companies use meet COPPA 's detailed requirements in terms of providing an acceptable form of parental consent for children to engage in certain online activities. This seems to us to be a model which would merit further examination with a view to adapting it for use in the EU.

15. Within the EU a body of the kind we are referring to, once established, could become a major European and global centre for excellence and expertise. The current series of ad hoc initiatives, such as the Coalition, is straining everyone's capacity to cope to the very limits. Most certainly it favours larger companies with a presence in Brussels and the resources to devote to lobbying.

16. While eNACSO appreciates and supports the reasons why the CEO Coalition is working to the narrow focus provided by the five points, the Commission has a larger important responsibility to co-ordinate activity across all Directorates with an interest in the online space so as to ensure a steady and consistent line of development of policy development.

17. eNACSO also makes a number of similarly high level observations in our response to Working Group 2 on age appropriate privacy settings.

18. We point out that there is a need for research into the age at which different competencies develop to make a range of judgements about how one engages in the online environment, in particular with regard to privacy issues but not limited to that. In-app purchasing and other features of e-commerce may be outside the scope of the Coalition but they are very much within eNACSO's scope and sometimes are very difficult to disentangle from privacy questions.

19. There is significant evidence about how children's capacities develop in other areas e.g. to distinguish between advertising and editorial content, but not in relation to privacy and not in the context of modern, on line social networking and e-commerce. Given the attention these questions receive this is both surprising and regrettable.

20. We say this not least because of the intense related debate taking place around the question of age

Formateret: Højre

verification. If we are to move towards greater use of it, how will we know what to verify and at which ages? It is unlikely that a single age will be appropriate for everything.

21. Finally, eNACSO believes that serious attention needs to be given to finding ways to strengthen the capacity of civil society to play their distinctive and independent part in these processes. Even if we were all living in easier economic times, we are still a long way from being in a position where we can reasonably ask our financial supporters to divert the sort of resources that are needed in this area because that would mean taking those resources away from front line services. Thus within the foreseeable future we are not likely to be in a position to undertake detailed monitoring of the behaviour and policy claims of the internet giants and hardware manufacturers whom we work alongside. The playing field is a long way from being level.

Formateret: Højre

Comments on Working Group 1: reporting tools

Summary

1. There is a need for greater consistency in the look and feel and positioning on the page of reporting tools and mechanisms.
2. A greater degree of consistency across platforms and device-types is also desirable.
3. Icons should be used to highlight and signpost specific issues. Greater emphasis is needed on using accessible language.
4. Reporting illegal content will be important for children but reporting other issues e.g. bullying is likely to be of greater concern to the majority.
5. Web sites and services need to know who their customers are and tailor their offering accordingly i.e. a site with many users who are children should be aware of that and act accordingly.
6. It is important to develop independent metrics and methods of assessing sites' and services' performance in dealing with reports received from children and young people.

1. Every web site and online service has its own colour scheme, its own look and feel, its own way of structuring its relationship with its users and members. It would therefore be inappropriate to suggest that every site or hardware platform had to handle the question of reporting tools in exactly the same way, using exactly the same language, colours and icons.
2. Yet the idea underpinning such a notion has some merit.
3. In almost every country there will be a more or less universally known way of contacting the real world emergency services.
4. The EU is encouraging a common telephone number in every Member State for reporting missing children. Each Member State will also have its own very widely known child helpline.

Formateret: Højre

5. The reason for this type of uniformity is obvious: when people are in distress or they have a problem that requires urgent attention they will often need to be able to react very rapidly, if not instinctively. Those are not the times when you need to start learning a whole new vocabulary or start hunting about for obscure tabs or phone numbers.

6. Consequently eNACSO's is calling for: a greater degree of consistency in relation to the prominence given on different web pages to the reporting tools available as well as their positioning on the page, and a greater degree of consistency both in terms of the language used and the icons deployed to denote where reporting tools are available.

7. The duties of and expectations of web sites are clearly higher if they know they have substantial numbers of children among their users. The percentages are less important than the numbers.

8. The simplicity and accessibility of the systems and language used are vital. Icons have an important role. A set of icons could be agreed and promoted to denote certain classes or types of reporting scenarios and issues?

9. In the case of children, the ability to report illegal content, while important, is unlikely to be as pressing as the ability for them to report various other types of content or behaviour.

10. There are now various excellent models available for how to present reporting tools. Not every issue of concern to a child online will necessarily be of primary concern to the site they happen to be on at the time. Thus it is important that reporting tools and procedures lead seamlessly and swiftly to a range of external agencies that may be able to help with the particular issue the child or young person is then facing.

11. Metrics and independent review processes need to be agreed and established to reassure the public that reports received in relation to child protection issues are being efficiently and expeditiously dealt with.

Formateret: Højre

Comments on Working Group 2: age appropriate privacy settings

Summary

1. Fixed age limits are the only practical way to proceed in the online space.
2. There is no evidence to support the adoption of the age of 13 or any other specific age as a standard. Research is needed but it is unlikely a single age will be appropriate for every issue.
3. To inform this process the Commission should collect together information about the existing age related privacy laws in all EU Member States.
4. Age-based standards without age verification systems are likely to be ineffective and may encourage a false sense of security or even be deceptive.
5. An independent mechanism needs to be developed to assess the efficacy of measures being taken to age verify users or to identify users that are non-compliant by virtue of age.
6. The presumption should be that location services are for adults. They should only be made available to minors following receipt of verified parental consent.
7. "Do not track" and the "right to be forgotten" are important ideas although we are as yet not entirely clear how they might work or are working.

1. This is a discussion about the age at which young people can be considered competent to disclose information about themselves to online commercial or other entities without first obtaining verifiable parental consent to join or use an online service. It applies equally to the use of specific applications or devices, the use of which raises questions which touch or concern the privacy agenda. A location based service

Formateret: Højre

which might disclose information about a legal minor's physical whereabouts is one example.

2. Ideally every individual child would be personally assessed, their actual level of understanding of the consequences and implications of taking one decision or another about privacy would be determined and the privacy rules for each site, online service or device would be set accordingly. This is broadly what international law requires and the domestic laws of many nations also mirror that position. It is tied to the notion of the "evolving capacities" of the child.

3. In some jurisdictions if a child "passes" the capacity test then there is no need to seek or obtain parental consent. Indeed the young person will acquire rights which in no way depend on obtaining parental consent. A company or organization might be breaking the law, breaching the child's right to privacy, if it communicates directly with a parent without the consent of a child that has been judged fully competent to decide something for themselves.

4. However, in the online world it is simply impossible to make subjective assessments child by child and for that reason we accept that fixed ages will need to be attached to certain aspects of policy. Below that line parental consent and engagement will always be required. Above it on a routine basis it would not be.

5. We think it is unlikely that a single age can or should be applied to every aspect of privacy or data protection policy. We think we are likely to need a graded or more granular approach. That would at least get us nearer to the idea of a child's "evolving capacities".

6. The above notwithstanding, it should always be the case that, whatever fixed ages might be assigned to any aspect of privacy policy, were a company to learn that a particular individual in fact did not properly understand the environment they were in or the service they were using, the company should be under an obligation to act swiftly to remedy that situation, either through the provision of extra support or information to the identified individual or by terminating their account.

No direct evidence available

7. There is a great deal of evidence which looks at the ages at which children and young people develop a capacity to distinguish editorial content from advertising, and about their capacity to evaluate promotional claims being made for different products or services. We know, from the works of academics such as Robert Selman, approximately when young people begin to develop a capacity to see the world from the perspective of someone other than themselves. There is also a well-established body of evidence in relation to the age appropriateness of various types of content or games to which young people might be exposed with minimal or no risk e.g. as administered by bodies such as the BBFC, NICAM and PEGI.

Formateret: Højre

8. However, we know of no research evidence which directly supports current practice in relation to any specific age in terms of data disclosures to third parties and a child's or young person's capacity to understand the potential consequences or implications of taking one privacy decision rather than another.

9. This problem is not helped by the lack of accessibility in the language used to present privacy policies but that is a slightly different but nonetheless important point. Our point is even if the language used was concise, crystal clear and prominently displayed on the site, we still have no evidence which helps us understand how it is understood and acted upon by young people. Against such a background the idea that the "rule of 13", or any other age standard, should be adopted as a generalised EU-wide standard is difficult to accept particularly as we already know that such rules as there are are being so widely disregarded. If a new age standard was established ***and*** it was linked to an efficient age verification process we might be in a different place but that seems a very distant prospect at the moment.

10. Research is therefore needed which sheds more light on the range of competencies required by children and young people in relation to providing different types of data online to third parties, with a rough approximation of the ages at which these competencies can be expected to develop among the great majority of children.

11. It is quite possible that 13 is an appropriate standard for many aspects of policy but, equally, as we have suggested, it is possible that a sliding scale is needed to cover different types of data or different types of disclosures. The UK's Bailey Review seemed to be nudging policy in the direction of 16 being a new standard for many things.

12. Armed with new research of the type described everyone would be able to have a more intelligent or solidly based discussion about age appropriate privacy settings.

The "rule of 13"

13. As the responses received to the working group's questionnaire show (see below) the age of 13 is used by only a minority of social networking companies as the minimum age of entry or for membership. However, since one of these companies is Facebook, 13 has become of pivotal importance in most of the discussions about this subject. 13 is often applied as an entry level qualification for other types of service as well.

14. This means at 13 young people are being considered competent to make decisions entirely by themselves about joining a site or service without any prior reference to their parents much less do they need to obtain their parents' permission. Whilst it is true that sites often suggest that young people discuss these things with their parent they do not make this a requirement, neither is there any suggestion that the young person provides proof that they have done so. Such a stance is not

Formateret: Højre

guaranteed to encourage parental engagement.

15. How did 13 come to be so widely adopted as a standard? The "rule of 13" was developed in the USA in the 20th century under the terms of Children's Online Privacy Protection Act of 1998. This was before any social networking sites existed. Although "privacy" in the title, it is not "privacy" as it has come to be understood today. The Act was meant to address one very simple and quite other concern: children's potential exposure to commercial advertising.

16. If a company wanted to collect any personally identifiable information from a child it was understood that this implied the company would follow-through with adverts for its products or services and these ads would be directed at the child. The "rule of 13" said companies could only do that if they first obtained verifiable parental consent from the child's parents.

17. While the "rule of 13" continues to preserve that original objective it has in effect become something completely different. For some web sites it has become the de facto standard beyond which it is assumed the child has full competence to decide for himself or herself what personal information it is acceptable for them to disclose to the rest of the world or which apps and services they wish to use or link to their profile.

18. As far as we are aware the "rule of 13" only exists in the USA, although as already noted it has been picked up and copied elsewhere. Spain has a "rule of 14", the UK has no fixed rule but, in general in the UK, 12 is considered to be the age at which a child can make decisions about passing on personal data about themselves without first needing parental authority.

19. What is the position in each EU Member State? eNACSO has never seen that data presented anywhere. Even the Article 29 Working Group does not seem to have assembled it or, if it has, it is not published.

20. eNACSO is also unclear about the impact of the default privacy practices currently being pursued on those (non-US) sites where there is no lower age limit or an age limit which is less than 13. There is no concrete evidence that children on such sites are at any greater or lesser risk of harm.

21. Moreover, in the absence of age verification systems how meaningful are many of these age based policies anyway? Is there not a risk that they amount to no more than declarations of hope which could create a false sense of security or even be deceptive?

22. The limitations of what a site or service can do to determine a person's age ought to be made clear on every site.

23. An independent mechanism needs to be developed to assess the efficacy of measures being taken to age verify users or to identify users that are non-compliant by virtue of age.

Formateret: Højre

24. Not all children or young people break rules, even age related rules. Having rules, even ones which cannot be enforced, does work for some, perhaps even a majority, but substantial numbers, perhaps particularly of more vulnerable children, may not be adequately protected if the systems being deployed have no way of knowing or detecting what their true age is. Should it not be the case that everything defaults to a certain standard and you have to prove you are an adult or of a given age to have that default standard altered or lifted?

25. Beyond that and absent such data it is not easy to be very precise about individual aspects of privacy policy although we believe the principles sets out in the USA's draft Consumer Privacy Bill seem about right:

26. **Individual control:** The right to decide how personal data is used. Companies obliged to provide "clear and simple choices" to enable "meaningful decisions".

27. **Transparency:** Access to "easily understandable" information on what companies do with your data and, crucially, why the need it and when they will delete it.

28. **Context:** The use of personal information should account for the context in which it was given, including age and "familiarity with technology".

29. **Security:** Personal data needs to be held securely.

30. **Access and accuracy:** Consumers should have "reasonable access" to their personal data and be able to make changes to inaccurate information.

31. **Collection:** Companies should only collect data that they need; and to dispose, or make anonymous, data when they no longer need it.

32. **Accountability:** Companies need to hold employees responsible for following the Bill of Rights, including training and audits.

    http://bit.ly/usgovstandard

33. More specifically we believe any location related data which can be linked to a personal profile or posting ought to be considered adult in nature by default and it can only be waived for under 18s if verifiable parental consent has been obtained.

34. Broadly-speaking we can see great merit in the idea of "Do Not Track" becoming the default, if not for everyone then at least for minors. The "right to be forgotten" also sounds attractive although we would be keen to discuss how, in practice, this would work. In many countries it is a criminal offence to refer to any convictions a person might have obtained as a minor. For certain classes of offence it is a crime to refer to any convictions after a certain amount of time has elapsed. They are generally called "spent". It would be odd and undesirable if, by contrast, youthful indiscretions that were not crimes could nonetheless haunt and

Formateret: Højre

harm someone for the rest of their life.

35. What is of pressing concern, however, is how and when privacy related issues are communicated to children and young people. More accessible language presented in a timely way, making greater use of icons, are likely to be fruitful lines of endeavour.

Formateret: Højre

Responses to WG2's questionnaire

1. WG2 designed a questionnaire. It was sent to companies in the following six categories:
    - Content providers
    - Games Platforms
    - Hardware Manufacturers
    - Social networks
    - Software providers
    - Telecoms Operators – ISPs
2. We do not know how many companies received the questionnaire but 33 responded.
3. Of the 33, 4 said "N/a" (not applicable) to every question in the questionnaire or did not provide an answer. These were: Opera, BskyB, Liberty/Global and Vivendi. Nokia replied N/a to every question but indicated that it planned to introduce a range of (unspecified) measures in 2013, some of which are likely to be relevant to the question of privacy settings.

General observations

4. Below is an analysis and commentary on the replies received. However, it must be stressed that in the time available it has not been possible to verify or check all of the statements made. These have therefore been taken at face value and on trust. That is not really a satisfactory position for a self-regulatory process to be in in the longer term.
5. At some point it would also be useful to collect information showing what individual sites do to try to police and enforce their age-related privacy policies.
6. Our responses and comments are based on our direct experience of working with children, young people and families, supplemented by the research evidence provided by, for example, EU Kids Online data.

Content providers

7. 6 companies replied. 3 said "N/a" to every question. These were BskyB, Liberty/Global and Vivendi.
8. The three that replied more fully were Daily Motion (France & 33 countries), Mediaset (Italy) and RTL (Holland and 8 countries).
9. *Daily Motion* is a video sharing site. It only applies an age limit in the US (13). It is not clear what differences there are as between the offering in the US and other territories in which it

Formateret: Højre

operates. It would be good to know if there are any.

10. We are told that profile visibility is "limited" and that it is not possible to search for minors although when one joins Daily Motion there is no *requirement* to declare your age. Otherwise one "can" set a video to private. No information is provided about the default position although "some pieces of information (e.g. last name and date of birth) can be made public or private at all times."

11. *Mediaset* is a video sharing site. Profiles of sub-18s are not visible on the site and that minors' data is not available. We are told that almost all of the key functions are pre-moderated and that sub-18s cannot upload videos, although they can make comment on them. Neither can videos featuring sub-18s be posted to the site.

12. *RTL* is focused on video content. It maintains that there is no profile visibility or other visible information about users. Neither can anyone post comments or photographs.

Games platforms

13. 2 companies responded: Microsoft X Box and Nintendo.

14. *Nintendo* maintain that they do not ask for age related data and no settings are dependent on the age of the users. Some applications can allow the sharing of data but where this happens the would-be poster is notified and such communications can be blocked, which presumably means by defult they are not blocked.

15. *Xbox* has extensive privacy controls available. However, everything hinges on the initial decisions made when creating the users' profiles. The defaults follow three categories: child, teen and adult.

Hardware manufacturers

16. 5 companies responded: Apple, Nokia, LG, RIM and Samsung

17. *Apple* have made available an extensive set of controls which are broadly similar for both their PCs and their mobile devices. In particular Apple point out parents can set up their child's profile (as indeed is the case for every company's sites and services). It is not easy to deduce from Apple's answers what the default position is in either the mobile or PC environment or how extensively parents need to engage to create an age appropriate range of privacy settings from the available tools.

18. *LG* have plans to introduce new (unspecified) measures in 2013 in relation to their mobile handsets and they point out that a parental pin lock is available at the moment. In relation to PCs the main component for controlling the settings are within the operating system or the applications. No information is provided about the default privacy position either in the mobile or PC environment.

19. *Nokia* said "N/a" to every question but indicated that it would be introducing (unspecified) measures in 2013.

Formateret: Højre

20. *RIM* does not make PCs, only mobile phone handsets and related items. Reference is made to a large and impressive range of parental controls which will be available although a date is not specified. No information is provided about the default privacy position.

21. *Samsung* provide the identical answer to every question: it is already possible to control access to a range of services and additional developments are on-going. No information is provided about the default privacy position either in the mobile or PC environment.

Social networks

22. Understandably this contains the largest number of replies and the largest amount of information.

23. Some of the statements provided are interesting e.g. on a company's advertising policy, but no obvious link is made between that policy and the operation of the site's age appropriate *privacy* settings. It is useful to know what sorts of advertisements a child will *not* be seeing, but it would be more useful to know how a minor's data is rendered to or used by those companies that do advertise, and the same applies in relation to third party apps which are allowed to work on the site. A similar observation might be made with equal force about third-party games applications e.g. what data is required by or is passed on to the provider and how is it used by them? Do the social networking sites place any limitations on the games providers and how are these and the policy in general policed?

24. 9 companies responded: Facebook, Google+, Hyves, Netlog , RTL, Skyrock, Stardoll, Sulake, Tuenti

25. 3 companies operate with no minimum age (Hyves, Netlog and Stardoll), 1 operates with 12 as the minimum age (Skyrock), leaving aside Spain, 3 have 13 (Facebook, Google+ and Sulake) and 2 have 14 (RTL and Tuenti). In relation to Spain Facebook and Google+ declare 14 as their minimum age. Tuenti allows under 14s with parental consent. It would be interesting to know how many sub-14s have enrolled with Tuenti having gone through their parental consent procedure.

26. For sub-18s it is not possible to find someone via a public search engine in every case bar one: RTL seemingly allows 16+ users to opt in to that facility.

27. The possibility to search on the site varies from zero restrictions (Facebook and Google+) to limitations based on whether or not you already know someone e.g. with RTL you can only search for under 18s if you are already a friend or a "student you tagged".

28. Some sites publish no personal information about anyone (Stardoll and Sulake) or sub-18s, or in the case of Hyves sub-16s.

29. In general there appears to be limits on the extent to which adults who are not friends and other people can search for minors they don't know,

Formateret: Højre

but a wide variety of practices are being followed. The same is true in relation to the information about a person that is made visible and in respect of the practise of tagging. Facebook allows friends of friends to tag minors, others allow only friends to tag friends, some do not allow tagging at all. If someone who is not a friend tags you within Google+ you must agree to the post before it can go up although it was not clear if any special provisions applied where the "tagee" or the "tager" was a minor.

30. No site publishes a minor's email address or Messenger handle although some clarification from Facebook would be welcome in relation to the operation of their Messenger and email services. Posts and status updates linked to minors' your profiles tend to be restricted by default only to friends although that can vary e.g. on Tuenti if you post to a page or an event it will be available more widely.

31. With regard to location data again the practice varies. On Facebook and Google+ location data is not turned on by default, but it can be turned on by a minor and linked to posts. Hyves allows minors to switch on location although it is not clear how the location data is then broadcast or used. Netlog does not turn on location by default but it is not clear if that means is can be turned on by a minor later. Tuenti only allows location data to be transmitted to friends but, apparently, *" If you look for someone on the search engine and you get results, you will see their location even if you're not friends with them."* Stardoll does not use or publish location data. RTL allows minors to turn on location data and, uniquely, Skyrock turns on location data by default.

Software providers

32. 3 companies responded: Apple, Opera and Windows Live.

33. *Apple* makes clear that sub-13s are not allowed to create an Apple ID or use iTunes. iTunes acts as a hub for a range of Apple functions. As with Apple's earlier entry (above) the company provides an extensive set of controls under hardware but it is not clear how extensively parents need to engage to create an age appropriate range of privacy settings from the available tools.

34. *Opera* said the questions were not relevant to them although they did point out that they provide a section in their privacy policy guidelines which explains that Opera has no means of confirming a person's age and that parents should be involved.

35. *Windows Live* has an extensive range of privacy settings and controls. All new accounts default to private. It is not clear what messaging on the new privacy settings was sent to existing users.

Telecom Operators – ISPs

36. 8 companies responded. They all got close to saying "N/a" to every question seemingly largely on the basis that the services which they provide are all the subject of

Formateret: Højre

contracts and these could only be made with persons aged 18 or above.

37. 7 of the 8 companies provided identical answers. These were: Deutsche Telekom, France Telecom/Orange, Telefonica, Telenor, Telecom Italia, TeliaSonera and Vodafone.

38. The 8th – KPN – said the same as the others but added a little bit of extra detail. The first extra detail was in relation to their iTV service which works through a set top box.

39. KPN's set top box appears to have a good default position although its comments relate largely to content questions rather than privacy as such. However, as KPN is the only company to have provided any input in relation to TV services there are few conclusions we can draw which are likely to be of any wider value.

40. KPN also provide information about the browser they have developed for children and they also inform us they have parental control features. No information is provided about any privacy aspects of these controls and the web link provided takes us to a page which is in Dutch. However, using Google's translation service, it was not instantly apparent where the information on age appropriate privacy settings were located, although there was lots of information about individual risks such as phishing. Three screen shots of the KPN service are provided for reference.

41. Although most if not all of the 8 companies that responded are both fixed line and mobile operators, the comments seem largely to be confined to the mobile space. The only concrete reference to privacy practices is given in relation to the mobile space and this is in a reference to the "future implementation" of a GSMA policy adopted in 2011: "Mobile Privacy Principles". In that document the following very broad statement appears:

Children and Adolescents

An application or service that is directed at children and adolescents should ensure that the collection, access and use of personal information is appropriate in all given circumstances and compatible with national law.

42. It would be fair to say that there has been comparatively little involvement of or focus on the position of fixed line ISPs in the current processes. In part this is because of the growing importance of the mobile space but nonetheless for the foreseeable future fixed line ISPs will continue to be of enormous importance in this debate.

43. However, in relation to the position of the mobile phone companies, before the CEO Coalition's work is concluded it would be good to know what exactly is the legal basis of their relationship with the tens of millions of their customers who are under 18?

44. What data do they have about the ages of their customers and could this be used to read across to individual services, whether supplied by themselves or others, in a way which

Formateret: Højre

would enhance the privacy component e.g. if Deutsche Telekom or Telecom Italia knew that a particular handset was registered to a 12 year old and that child attempted to access a web site or service that was known to be restricted to persons aged 13 or above, could it be stopped or some other action taken e.g. to alert a parent?

Formateret: Højre

Comments on Working Group 3: content classification

Summary

1. Illegal content does not need to be classified. It shouldn't be visible or accessible in the first place. Universal content need not be classified but there are advantages to be gained from it being so.
2. In relation to user generated content (ugc) classification could be problematic on many sites if it implies any form of prior editorial control or approval.
3. The main challenge for ugc is to get more companies to engage proactively with enforcing their terms and conditions. This requires clarification of the eCommerce Directive.
4. The principal challenge is in relation to commercial content which is legal but may be age inappropriate or give offence to certain types or classes of persons.
5. eNACSO considers a new and trusted body is needed to help with making determinations in this space. The USA's FTC may provide a model that could be adapted.

1. Any measures which lead to higher and more accurate levels of content classification are to be welcomed and encouraged.
2. However, for the purposes of this discussion it is important to distinguish between several different types of content that might be found on the internet:
    a. Illegal content
    b. Content which is suitable for everyone or ought to be accessible to everyone e.g. helplines, news and educational channels
    c. Legal content published by commercial entities or other organizations which is not suitable for children or which some people may consider offensive

Formateret: Højre

d. User generated content (UGC), which can of course encompass any or all of the above

3. Content classification systems have no part to play in relation to categorising illegal content. The material simply should not be there to begin with irrespective of who the publisher happens to be.

4. The focus, in this context, therefore should be on systems which allow illegal material to be identified and removed as rapidly as possible. Technical tools can play a major part both in preventing initial uploading or in detecting any postings that might slip through. This is issue is being specifically addressed by Working Group 5 so we will make no further comments on the matter here.

5. There is little urgency about classifying content which falls under category b, although there is no doubt some utility to be obtained from it being classified.

6. The difficulty arises principally in relation to content in c and d.

7. However, we think it is important to distinguish between concerns around content which is published by commercial entities or organizations and user generated content.

8. eNACSO accepts that the definition of what constitutes a "commercial entity or an organization" may sometimes be a little difficult to define when it comes to publishing content online. Indeed the same could be said about material which should be included in category b. For this reason, and others, maybe now is the time for the EU to consider constituting a new body or a division within an existing one which could make binding determinations on matters of this kind.

9. Such a body would need to be independent of the Commission and arms-length from any and all political institutions. It would need to be able to win and retain the confidence of a wide range of stakeholders, not the least of these being the free speech and civil rights communities.

10. The putative new body would need to be properly established and have the capacity to deal with complex issues, weighing competing claims against each other and reaching a final view which would be accepted as being fair and reasonable by the great majority of people.

11. We note that, for example, in the USA the FTC has the power to intervene in internet related issues e.g. to determine whether or not individual sites are covered by the provisions of COPPA and whether or not particular solutions meet the COPPA requirements.

12. Within the EU a body of the kind we are referring to, once established, could perhaps also take on a wider role in both assisting with and guiding the development of policy in this area as well as more generally in the field of online child safety. The current series of ad hoc initiatives can be quite confusing and is straining everyone's capacity to cope to the very limits.

Formateret: Højre

13. In any event, returning to the main theme, we do not think it is possible to apply the same considerations to both UGC and commercially generated content or content published by a wide range of organizations.

14. To be more precise, whilst commercial content or content posted by organizations ought to be "pre-moderated" and therefore would be susceptible to be being classified prior to posting, that is not possible in relation to UGC, or even if it was possible it would not be appropriate in very many environments as it would imply or require a degree of prior editorial control. That is completely antithetical to the idea of UGC.

15. The focus of Working Group 3 and the CEO Coalition should be on commercially generated content or content produced by organizations.

16. However, at root, one of the reasons why this is an issue in many quarters is because of the way the eCommerce Directive has been interpreted by corporate lawyers.

17. Many companies refuse to inspect the content of their site proactively looking for content which may be in breach of their terms and conditions because they believe if they do it will render them open to liability for everything on the site. This is because some courts in a number of EU Member States have interpreted the eCommerce Directive as meaning that any kind of inspection of web content potentially makes the web site owner the legal publisher of all of it. For this reason sites insist they will only inspect content which is alleged to contravene their rules if it has been reported to them i.e. they will inspect content only reactively. This can mean that bad content, content which breaches the site's terms and conditions or is even illegal can remain on public view for substantial periods of time. That cannot be right.

18. We do not believe this was ever the intention behind the eCommerce Directive and we note that many companies in fact share our view and do proactively inspect the content on their site. They are willing to accept the risk of incurring liability in order to preserve their brand values. We therefore think that the Commission should speed up the clarification of the eCommerce Directive and urge Commissioners Kroes and Barnier to resolve this within this Commission.

19. The position should be that a company can only be liable for any content found on their properties if they have actual knowledge of its existence or if, having that knowledge, they failed to act expeditiously to remove it.

20. If, instead of sitting back waiting for a complaint to be received, all companies were energetically patrolling their sites to ensure that all content on it, UGC or not, conformed with their terms and conditions, this would to a substantial degree address the anxieties which lie behind much of the demand for better content classification systems.

Formateret: Højre

Comments on Working Group 4: parental controls

Summary

1. The data on current practices need to be presented and referenced by platform, device type service type and take up.
2. Definitions may need to be tightened but there are enough source documents available to obviate the need for a great deal of further study.
3. "Default on" should not be ruled out as an option, not least because over a quarter of the companies that responded to the questionnaire already offer it in places.
4. Children will not always be a "minority of users" on every service but, even if they were, final recommendations cannot be limited by an overriding desire not to inconvenience adults.
5. The needs of vulnerable children have to be addressed. They are a significant percentage of total users and a very large number of human beings.
6. Education and awareness will always be of paramount importance but there are certain families and situations where technical tools may offer the best or even the only hope.
7. Care needs to be taken over reporting helpline and similar sites which normally guarantee anonymity to their users.

1. The UK Prime Minister invited Professor Tanya Byron to review the risks that British children face from the internet and videogames. The review, "Safer Children in a Digital World" was published in 2008.

2. In her report Professor Byron states (Paragraph 4.60, Page 94)

   "I do not recommend that the UK pursue a policy of blocking non-illegal material at a network level at present.

   However, this may need to be reviewed if the other measures

Formateret: Højre

recommended in this report fail to have an impact on the number and frequency of children coming across harmful or inappropriate content online." (emphasis added)

3. It is significant that, as early as 2008, Tanya Byron was saying default on was an option if the industry did not deliver and come up with something that worked to keep inappropriate material away from children. The implication was that this should be done within a reasonable timeframe.

4. In 2004, Professor Sonia Livingstone published the results of a survey she had carried out on UK parents' "wish list" for a safer internet. 85% wanted to see "tougher laws on online pornography" and two thirds wanted improved filtering software, and more than half want more effective means to limit and monitor their children's usage of the internet. In April this year, another survey in the UK carried out by YouGov, showed that vast numbers of parents continue not to want their children to have ready access to pornography on the internet.

5. European data reveals a similar pattern. In the latest EU Kids' Online survey, to be published shortly, we learned that 31% of parents of 9-16 year olds still "worry a lot" about their child seeing inappropriate content, and at 30% it's not so very different for the parents of teens. This data is consistent with what child protection NGOs and professional have been calling for and informs our views set out in this paper.

6. Before finalising this section of our larger document we had the benefit of reading the email and attachments (minus Appendix 2) circulated by Bob Smagge on behalf of the Group thus we have adapted our comments and framed them in part as a response to WG4's paper of 4th July, 2012.

7. No single Working Group is any more or less important than any other. However WG4 is especially significant because of its immediate focus on protective tools and what companies are or will be doing with them.

8. We all need to fix in our minds that in the converged world that is fast approaching or arguably is already with us it will become increasingly important to establish a common standard of child protection which will to the greatest degree possible apply in all environments. In the meantime we have to continue looking at this problem by device, platform and service but in the longer term we need to leave this approach behind.

9. How and with what device a child connects to the internet is less important than the fact that the child is connecting. Parents, teachers and children should not have to learn a whole new vocabulary to get to an acceptably safe point depending on the method of connection. "Seamless safety" should be the watchword.

Formateret: Højre

Responses to WG4's questionnaire

1. Altogether 23 companies appear to have provided information to this working group.

2. 19 companies provided information about parental controls they were already offering or they indicated they already had something in place. These were as follows: Apple, BT, Daily Motion, Deutsche Telekom, France Telecom-Orange, Google, KPN, Mediaset, Microsoft, Nintendo, RIM, Sky, Stardoll, Telecom Italia, Telefonica, Telenor, Teliasonera, Vivendi/SFR, and Vodafone. In several instances a number of these companies also indicated they had plans for new or enhanced child safety products or features in the pipeline.

3. 4 companies indicated they intended to offer parental controls or were working on something, implying that at the moment they did not have an offering. These were: LG Electronics, Nokia, Opera and Samsung.

4. 2 companies, Daily Motion and Mediaset, indicated that their solution was turned on by default. In their responses other companies did not register that they had any solutions that were turned on by default but it is known that in some markets that is precisely what happens e.g. in the UK. This would apply to Deutsche Telecom, France Telecom-Orange, Telefonica and Vodafone, making a total of at least six companies that have parental controls or a child safety offering which operates by default.

5. It is impossible for an organization like eNACSO, or we suspect many other NGOs, to do any sort of detailed evaluation or checking of the many different statements or claims shown in companies' responses in respect of any of the parental control offerings currently available or in relation to those which are en route to market. We have to take everything on trust. Moreover the way the information has been presented makes attempting any comparisons extremely difficult.

Better presentation

6. For the next review document it would be appreciated if a more systematic attempt could be made to present and distinguish between what companies are currently doing or are proposing to do both by the nature of the service they provide or are planning to provide and by the hardware platform concerned e.g. mobile phone handsets could be grouped together, mobile networks could be aligned and similarly with games consoles, browsers, search engines, tablets, laptops, desktop

Formateret: Højre

computers, ISP or ISP-type and other connectivity services.

7. It really does not make any sense to put Opera, Stardoll and Apple in the same framework or to try to fit them into one.

8. The beginnings of such an approach are visible on the final page but it needs to be better structured if it is to be useful in the debate. It would also be helpful to see data on the take up of these tools and initiatives taken by companies to promote thems.

Substantive comments

9. The first page outlines the work carried out by the working group and highlights proposal for next steps. eNACSO is concerned at the suggestion that the group

   Organize a "vendor workshop" in the Autumn of 2012 to discuss generic design requirements on what might constitute "good" parental controls. An invitation will be sent out to a significant cross section of vendors active in this field.

10. We would draw WG4's attention to three key documents which contain a great many insights and tell us a great deal about what makes up good parental controls. These documents are:

    a. The European Framework for safer mobile use by younger teenagers and children

    b. The Safer Social Networking Principles

    c. The SIP-BENCH 2 project for benchmarking parental control tools for the online protection of children

11. Given the tight timescales around this process, it might be more efficient and effective to use existing information of this kind. We note that many of the companies taking part in this process are signatories to one or more of the documents mentioned.

12. From the above it is likely that WG4 would distil something rather like the criteria set out at the bottom of page two (and SIP is referred to) but, right now, the list of criteria given there looks a little thin or incomplete. Of course allowances would need to be made for differences in the platforms or online environments. Perhaps it would be more sensible to look at this question vertically by service type or by hardware type rather than in a great ill-defined mass?

13. Either way we can see that the working group would likely benefit from agreeing a basic array of features which would qualify as potentially being a good "parental controls" but a parental control that ticks every box may still be of little practical value if the user interface is user unfriendly. SIP-BENCH picks this up this point.

14. We wish to register one final, preliminary point which we think is of great importance when discussing parental controls.

Formateret: Højre

15. We have stated elsewhere that children have their own independent legal rights to access and publish information or to communicate or associate with other people.

16. Inevitably the use of parental controls and in particular monitoring tools *could* be used in ways which might interfere with those rights. This has been the case since filtering and monitoring tools were first developed. It is a matter which, ultimately, has to be resolved as best it can be in each family but there is no avoiding the fact that an abusive parent, adult or third party could use this type of software in an oppressive, potentially illegal way.

17. Filtering companies, or companies putting together family safety applications, therefore need to tread with some care. For example in the UK, and doubtless in other countries also, we have telephone helplines and where, by long established practice, if a person rings them it will never show up on the list of phone calls that have been made. Consequently if a child were to ring, for example, Childline (the NSPCC's helpline for children) from their home phone or their mobile there would be no evidence of it. Those same services and similar ones which also operate online aim to adhere to a similar principle. We believe there is a strong case for similar provisions to be made in the online space i.e. if a person visits an officially recognised web site dealing with certain matters, the fact of that visit should not ordinarily be the subject of a report of any kind by parental controls or other software.

Formateret: Højre

Options for producing parental controls

1. This section responds in detail to the comments by WG4 in 'Options for introducing deployment of parental controls'

2. We note WG4 concerns around compatibility with existing (inter)national legislation around "default on".

3. It is unhelpful for unsubstantiated, un-sourced objections to be made to doing things in the field of child protection on the basis of vague legal objections which are said to exist in unspecified countries. If there are particular legal objections to specific measures in individual jurisdictions these should be properly referenced in order that everyone can take a view of their weight or moment. At the same time we would hope that if something does turn out to be illegal in only one country or in a small minority of countries that is no reason not to pursue it in those countries where it is legal if there is enough support for the core idea itself.

4. At the highest level international law or standards provide an excellent starting point. For example the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue stated that 'legitimate types of information…may be restricted' in order to 'to protect the rights of children'.

5. The starting point must be, therefore, an assumption that we will only support the use of good tools that are proportionate, work both well and legally on the platform or with the device for which they were intended.

6. We cannot get into a priori arguments about the legitimacy or legality of using parental controls within the parental controls working group. The discussion should be focusing on how we improve the take up and use of good parental controls which are appropriate for a given service or a given situation and how we achieve higher levels of parental awareness and engagement with these issues.

7. We now turn our attention to a statement which is of significant concern. We would like to see it removed. This is the reference to children only being a "minority of users" and how, if things were designed specially for them, the majority would have to take "additional steps to opt out" and this would "hamper" the (majority) user experience.

8. Firstly it is not true that in all cases children are always a minority of users. In several instances they will be the majority. In many more, even though children are a minority i.e. less than 50%, they might nonetheless be present in very large numbers. Percentages can be deceptive. For example, even if only 10% of a service's or a product's users or owners are children, but this might nevertheless amount to 2 million human beings. Is it being suggested that the interests of the 2 million can be disregarded or given minimal or less serious attention?

Formateret: Højre

9. Moreover, providing a safer environment for children might well enhance adult users' experience, giving them more confidence in their service providers and with the internet in general.

10. The purpose of the CEO Coalition is to make the internet better for children and the fact that statements of that kind can be made at this stage of the process is a great concern. Working groups were not given a mandate to develop solutions which d*id not,* to the smallest degree, change anything in such a ways as to inconvenience the majority.

11. We doubt there is a single country in the EU where there are no rules of any kind that might, even if only momentarily, be irritating or annoying for adults but they are overwhelmingly accepted by them because their underlying purpose is well understood: they are there for the protection of children.

12. Perhaps if we all put a bit more marketing effort into explaining things to people companies would worry less about drop off rates.

13. Finally in this section it is extremely disappointing to note that, despite the fact at least six companies, more than a quarter of the total, have already have default on options it is dismissed out of hand as a possible outcome. Everybody endorses default on anti-virus and firewall software why should child protection solutions be treated differently?

14. The authors of WG4's paper essentially opt for the status quo i.e. *Have parental control tools available but only promote them by increasing the availability and awareness.*

15. That is what we have had since 1995. Option 1 is the no change option. We did not need a CEO Coalition or a working group to devise a solution like this.

16. We are glad the authors of WG4's paper therefore recognize that a "certain combination" with Option 2, Active Choice, is acceptable where this stimulates "child-parent interaction". Please note we do not agree with the suggestion that Active Choice should only be applied to new customers. That is essentially to write of hundreds of millions of existing customers.

17. Ways can be found to draw this issue to the current customer base e.g. through firmware updates to routers.

18. But what happens if Active Choice does not stimulate "child-parent interaction"?

19. Parental supervision and education of their children perhaps supplemented by further learning at school or from peers is normally the best possible way of keeping children safe. The safest child is the well informed and well prepared child.

20. More action needs to be taken to ensure as many parents and teachers as possible are encouraged to help their children manage their interactions online. Moreover, we need to encourage parents and teachers to start discussing these issues at a much younger age.

Formateret: Højre

21. Research from EU Kids Online shows that children as young as 7 years are using the internet. However, based on our experience of working directly with some of the most vulnerable groups in society, we know that some schools and parents may be less able to help their children.

22. For the most vulnerable children, therefore, or those already disadvantaged or 'at risk' in their everyday lives, we cannot rely solely parents or the school system. For the most vulnerable children, the responsibility for their well-being must be shared and carried out through using a range of approaches. It is in situations like these that default on can pay enormous dividends. The protection provided by technical tools may be the only protection the children have at all. It is crucial that any parental control tools address the needs of the most vulnerable groups of children.

23. eNACSO supports option 3 'Default On'. Unless parental control software is greatly simplified parents will still be reluctant to install it. And parents should not have to jump through hoops to make their child's internet service as safe as it can be. Of course they have the right to remove any and all controls but the onus should be on them to move towards this less safe environment for their child. It should not work the other way.

24. A default on system would ensure that the responsibility for protecting children online is shared between parents and ISPs, because both have a role to play, and neither one can protect children acting alone.

25. For example, age-rated content, with material classified and filtered as suitable for different ages, could give parents new opportunities to discuss the appropriateness of material with their children. Default on would also help to protect the most vulnerable groups of children for the reason we have highlighted earlier.

Awareness Raising

26. The EU and member states need to play their part alongside industry and NGOs in raising awareness on online safety issues and provide better guidance and support for parents and carers so that they are able to confidently have these discussion with their children.

27. The European Commission should carry out a mapping exercise and identify and promote good practice in this area.

28. Industry should support such initiatives through providing financial resources e. g. by funding awareness raising campaigns.

Challenges

29. We accept there are difficulties in adopting one approach given 'heterogeneity of companies in the coalition, differences in cultures and approaches in different member states' however, this need not be insurmountable if the will is there. The purpose of this coalition is to remove barriers rather than simply accept the status quo.

Formateret: Højre

Working Group 5: notice and take down of child abuse material

Summary

1. Child abuse images pose a special and continuing challenge to the internet community.
2. It is vital that comprehensive data about the scale of the problem are obtained and published so as to guide policy. We suspect the work in this space is hugely under-resourced.
3. An audit should be undertaken of the operation of INHOPE and of each EU-funded hotline and how data which they produce is picked up and utilised by law enforcement.
4. INHOPE and hotlines should be given new operating instructions by the Commission in order to facilitate the production of a usable database of urls known to contain illegal images.
5. We need to find new ways to improve the detection and removal rates of child abuse images in environments other than the web and to improve the rate of identification and rescue of victims.
6. In future technical tools to detect and remove illegal images are likely to be of increasing importance. A reliable country by country assessment of the legality of such methods is essential.

1. Prior to the arrival of the internet the availability of child abuse images was comparatively restricted. The emergence of the internet as a mass medium in the consumer space changed that position dramatically. This is one reason why the internet community has a special responsibility to address the availability of online child abuse images.
2. Of course the internet is simply a tool. It did not create the images in the first place. That required human agency. But the internet has most certainly allowed and encouraged the distribution of child abuse images on a scale which hitherto was unimaginable.
3. We would like to see all of the agencies involved in this field

Formateret: Højre

combining their intelligence to publish the fullest possible account of the true size of the problem. The only data which normally finds its way into the public domain is that which is published by hotlines, but we are acutely aware of the fact that they do not have full visibility of the terrain. They only see what is reported to them whereas law enforcement agencies generally see everything that the hotlines report to them plus they have intelligence they acquire from their own independent activities.

4. Thus the real scale of the challenge is at the moment unknown outside of the police service because no single national or international organization has been in the position to assemble all of the information from all the sources. Efforts should be made to correct this.

5. Absent such authoritative data there will be continuing doubts about the extent to which current efforts by hotlines and law enforcement agencies are matching up to the real needs. Our view is that work in this area is substantially under resourced. Too many cases are going un-investigated. Triage has become the daily reality.

6. We appreciate why law enforcement agencies may be reluctant to disclose certain types of information about activity in this area but, at root, this is a question of public policy. We cannot make good public policy without reliable information.

7. Action to combat online child abuse images is now a legal obligation within the EU. The EU Directive on combating the sexual abuse and sexual exploitation of children and child pornography obliges all Member States to take appropriate steps to ensure the prompt removal of child abuse images from the internet. Under the Directive the Commission too has obligations to report on progress. The recent JHA Council conclusions (Luxembourg, 7 and 8 June 2012) on a Global Alliance against Child Sexual Abuse Online further demonstrates the commitment of Member States to this area of work.

8. The Commission and Member States have encouraged the practice of "Notice and Take Down" (N&TD) as a means of securing the removal of child abuse images from web sites. The notices inform the online service provider of the existence of material on their site which is thought to be illegal and typically the notice also acts as a trigger for police action to identify and arrest the perpetrators and identify and rescue the child victims.

9. Hotlines are key tools in the N&TD system. However, the overall effectiveness of how hotlines work has yet to be conclusively demonstrated. Is there a case for an independent review or audit of INHOPE as well as each hotline in receipt of EU funding, linked to an assessment of how police agencies have been able to take up and use the information provided to them by the hotlines? Would this help us see what gaps remain to be filled?

Formateret: Højre

10. Transparency is vital in this area. Until we know exactly what the position is, how well and how efficiently the existing procedures are working, it is difficult to say with any confidence what, if anything, needs to be improved. Anecdotal evidence abounds but there is still a great deal of uncertainty. This must be addressed.

11. In the interests of greater transparency the European Commission could make an immediate difference by requiring every hotline it helps fund to publish, at least annually:

    i. The number of reports received of allegedly illegal child abuse images
    ii. The number of these reports confirmed as containing illegal child abuse images
    iii. How long it took from receipt of the report to confirming its legal status
    iv. The country in which the servers are based on which the illegal material was found
    v. The number of reports that were passed on to law enforcement or whoever the relevant agency is for further processing or action
    vi. How much time passed between the hotline confirming that a report was illegal and passing it on
    vii. In relation to EU Member States how much time then passed before law enforcement or the hotline issued a notice requiring or suggesting that the illegal content be taken down. As far as possible the same data should be acquired for non-EU Member States.
    viii. How much time then elapsed between the notice being issued and the material being deleted at source
    ix. Where it took more than an agreed amount of time e.g. 12 hours, for an image to be removed following receipt of a notice, the name of the hosting company owning the server should be published

12. INHOPE should gather in all of the above information from every hotline and carry out independent quality controls or quality assurance checks of the data and the operation of member hotlines.

13. INHOPE should arrange for all of the above information to be published country by country and in aggregated form.

14. INHOPE should also aggregate and maintain a list of all the known URLs containing illegal child abuse images. With appropriate security surrounding its transmission and use, that list should be made available to any relevant companies or law enforcement agencies which have an interest in investigating, removing or blocking access to child abuse images.

15. Alternatively, or in addition, the Commission should require every EU funded hotline to notify a central point within the law enforcement community e.g. the new European Cyber Crime Centre, of all of the

Formateret: Højre

above information. Wherever possible and appropriate law enforcement should publish any supplementary data so that, when added to that published by INHOPE, a complete picture of the scale of activity around child abuse images is available to the public and to policy makers, country by country.

16. Historically the web has been the sole or principal focus of activity for hotlines because the web became the single most important source of child abuse images. Given the widespread use of the web and its ease of access it is extremely important that this focus is maintained.

17. However, it is also seems clear that the web is no longer the sole major source of child abuse images. Police officers repeatedly say that Peer2Peer networks in particular, but also other closed environments and Newsgroups are now of at least equal, perhaps even greater importance. Yet few hotlines have either the legal authority or the right training and resources to engage with these alternative sources of illegal images.

18. Perhaps in many countries it would not be possible or appropriate for hotlines to involve themselves in work of this type in any event. Either way the point we wish to register is that the Commission's and the industry's primary or major focus on the web may be falling short of what is required. Collectively we need to reassess how best to make an impact in other relevant parts of the internet.

19. Technical tools and measures are bound to become increasingly important to deal with online child abuse images. However, the increased volume of cases that is implied by a greater level of internal company and law enforcement use of technical tools also implies a need for extra human resources.

20. There is said to be much uncertainty about several legal aspects of how technical measures might be deployed in the fight against child abuse images whether in the stream i.e. as they pass across networks, or when they are being stored.

21. We know, for example, that AOL's method of scanning email attachments to see if they contain illegal images has survived several challenges in US courts. Would the same jurisprudence apply within European courts?

22. Facebook and Microsoft already deploy PhotoDNA. Other companies are also doing so or are planning to. Several companies sell products to businesses that wish to detect known illegal images on their networks.

23. Before the debate on these questions goes very much further it would be useful to obtain authoritative advice on any potential legal complications or challenges. This may need to be done country by country within the EU as well as in relation to EU law. If the law needs changing or clarifying, either within a given country or at EU level, the sooner we know that the better it will be for all of us. The promise of what technical tools can

Formateret: Højre

achieve is too great to pass by without being completely certain of our ground.

---ooo---