



**PROTECTING THE PUBLIC IN A CHANGING COMMUNICATIONS ENVIRONMENT –  
A PUBLIC CONSULTATION – GOVERNMENT PROPOSALS TO ENSURE  
COMMUNICATIONS DATA REMAINS AVAILABLE FOR FUTURE ELECTRONIC  
COMMUNICATIONS SERVICES**

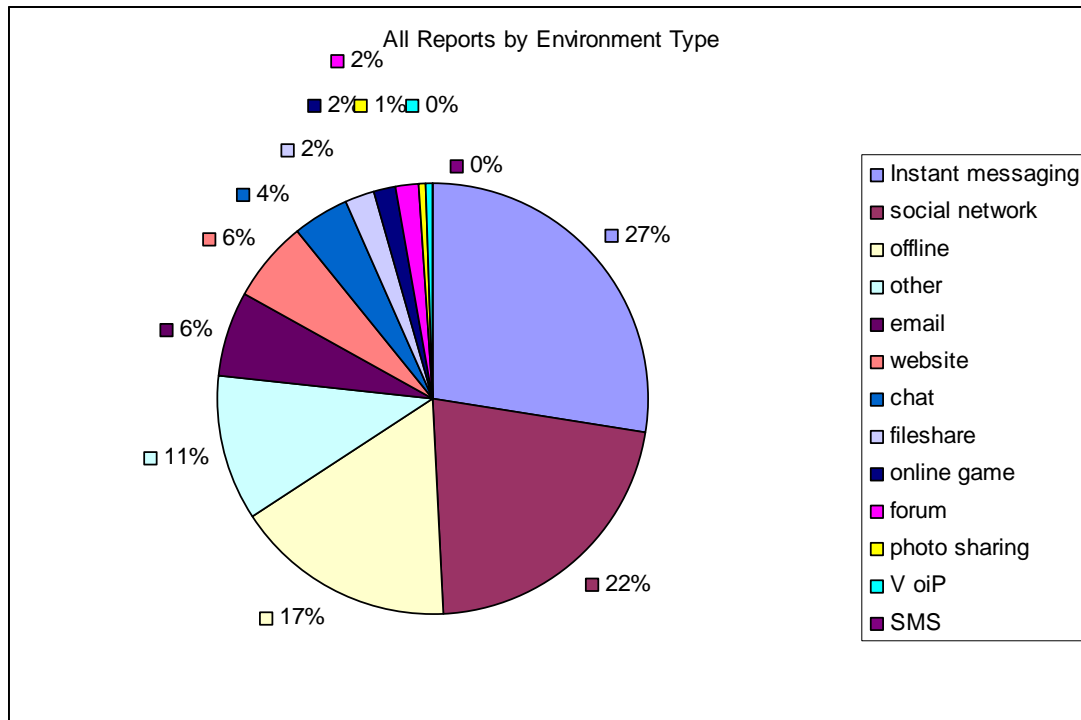
The Child Exploitation and Online Protection Centre provides a holistic response to the issue of child sexual exploitation. By the very nature of developments in children's social environment, large parts of the Centre's work focus around the internet and technology. However, the focus of the Centre remains on behaviour rather than the technology; the internet is a public space in the same way as a park or road and the behaviour of those in that environment is what makes it a good or bad place to be. That being said, there are specific characteristics of the online environment and developments in technology that have created a situation which contains additional risk for the children in it and which offenders are more easily able to exploit. As a result of this, CEOP takes a three pronged approach; understanding offender behaviour, understanding children's behaviour and understanding how these behaviours manifest themselves within and adapt to developments in technology and the online environment.

For children, the internet is an integral part of their world and we can no longer distinguish between the 'real world' and the 'virtual world'; indeed in CEOP we no longer use these terms, as for children, such a distinction does not exist and everything is real, regardless of whether it takes place on or offline. This convergence is strengthened and deepened by children's ability to access the internet 24/7 through a range of devices, many of which enable mobile access to the internet. Devices such as games consoles, laptops and mobiles now provide much greater freedom of movement and of access. At CEOP we see that divisions between types of hardware are becoming obsolete and what we really have are entertainment and access stations, many of which we can carry around with us. This means that not only can people access their online life wherever they may be, but they themselves can be accessed anywhere. Both hardware and software are increasingly containing location based services that enable the user to identify their physical location and have their physical location identified by other users of an application. This has significant implications in the hands of a child sexual offender grooming children online.

Furthermore, the way in which children have accessed internet services once online has to a certain extent driven developments in these services so that once easily distinguishable and clearly delineated services such as social networking sites, gaming sites, chat sites, photo or video sharing sites and instant messenger, now have functions that are interchangeable creating simply 'social sites'

where all services are available as required. The other key development for children and the way they use the internet is that of web2.0 which now allows anyone using the internet to create their own content and post it for everyone to access. Children and young people are far more willing to embrace an online audience and to post information that is accessible by anyone using the internet.

The below table demonstrates the reports received by CEOP from the 'CEOP Report' tab and from other stakeholders broken down by the online environment they relate to. In total this relates to 5360 reports received by CEOP throughout 2008/09.



It is clear from reports made to CEOP that instant messenger is the dominant environment primarily for grooming behaviours. However, it should be remembered that MSN IM has the 'CEOP report' button embedded within it. The significant increase in reports relating to social networking as a proportion of the whole has happened without the 'CEOP Report' button being embedded in any of the major social networking sites and therefore the activity that we see is likely to be only a small percentage of that which is actually occurring.

The implications for offenders and offender behaviour are significant. The internet has made access to children far easier than it was previously and wherever children go, offenders will follow in order to gain access to them. Information from reports received by CEOP suggests that in many occurrences of grooming, offenders will identify and target children within gaming sites or social networking sites and then develop the relationship within a more closed environment such as Instant Messenger. For example whilst reports relating to gaming sites are relatively small in number, there is however an increase in reports of grooming within these sites. Not only does the internet afford offenders unprecedented access to children, but access to information about children that would previously have taken time to obtain. For example an offender can access a child's social networking profile page to find information about the child that will assist in the grooming process, whether it be basic biographical information such as age, location and contact details or by allowing the offender to

pretend an interest in similar bands, or by allowing them to appear to empathise about a particular situation that a child has chatted with their contacts about.

Additionally the internet affords offenders an anonymity that they simply could not access otherwise. This relates not just to the ability to take on a different persona, for example to pretend to be a child or to appear as being younger than they actually are, but also to build up a level of integrity and credibility through establishing reliable contacts and networks. These networks built up in social networking sites ensure that they appear to be a reliable and trustworthy person to know and therefore provide offenders with an improved ability to groom vulnerable children.

Therefore it is clear to see that in the same way the internet has become an integral part of children's lives, so it has for those offenders who target children in the online environment. Child Sexual Offenders will offend against children wherever they are and we see a range of offences committed in the online environment that mirror those that previously could only be committed offline for example online flashing where an offender masturbates on webcam to an unsuspecting child. This has developed to the extent that we now see children who are sexually abused, by offenders, without ever meeting their abuser but who suffer abuse and are traumatised in exactly the same way as those who physically come into contact with their abuser.

Analysis of the images that are seen by our Victim Identification team suggests that children and young people who are victimised online fall into two distinct but non-exclusive groups. The first group may be categorised in terms of those children whose images of abuse have been circulated by child sexual offenders in peer to peer (P2P) exchanges or occasionally through commercial networks. These children tend to be primarily victims of intra-familial or other contact abuse in the offline environment and where the record of that abuse is subsequently circulated by their abuser in the online environment. The second group are those children who are targeted through the online environment and who are subject to grooming which includes incitement or threats to provide images of video footage of themselves carrying out indecent acts.

The scope and range of offending in the online environment is not limited to those crimes where children are targeted; offenders use the internet for a whole host of other activities that support, validate and augment or intensify their offending activities. Offenders' ability to network in the online environment has been prolific with various online environments supporting and providing the infrastructure for such networks. These allow offenders to meet with like minded individuals, to validate their sexual interest in children, share experiences and recommendations for future offending activities and to exchange images. The environments that are used for these activities range from the very public to the very private, with some sharing images in widely available and accessible photo sharing sites, and others using P2P networks or other more hidden and private environments.

We are seeing a significant growth in terms of offenders' use of P2P in order to share images, and it has certainly become the method of choice for the large scale distribution of images with far more images now being transferred via P2P than they are through pay per view websites. Statistics from the Digital Detectives Forum suggest that pay per view websites account for only 7.5% of the material that forensics are discovering on seized computers. Those involved in distribution via P2P platforms are largely unconcerned with the commercial value of the images and the images shared are newer and more exclusive and are prized for being so. Rather offenders involved in this kind of activity are drawn to the group membership and hierarchical culture. For these offenders, the images and videos are a currency in themselves and a route to increased credibility with other offenders that will also allow them access to other images or even other victims.

**Q1 On the basis of this evidence and subject to current safeguards and oversight arrangements, do you agree that communications data is vital for law enforcement, security and intelligence agencies and emergency services in tackling serious crime, preventing terrorism and protecting the public?**

Children are the most vulnerable public group and can be reliant upon services such as CEOP and other law enforcement agencies to trace both their details and those of offenders to afford them protection. In particular, children are often unable to access law enforcement protection in other ways and the ability to discover where abused children are at risk is a fundamental child protection function. Communications data therefore is absolutely vital to our ability to carry out our primary role and without it we would be unable to protect the most vulnerable members of our society from those who prey on them for sexual gratification.

**Q2 Is it right for the Government to maintain this capability by responding to the new communications environment?**

It is not only right that the Government responds to the demands of the communications environment, rather it is essential that law enforcement are able to maintain capability and to ensure they stay ahead of the offender in this respect in order to better protect the public.

Current legislation does not cover the likes of social networking sites (information society services) which form a significant part of both children's and the wider population's internet usage, and also as detailed above the environment where increasing amounts of grooming and other abusive behaviours are taking place. There is currently significant uncertainty around how law enforcement is able to acquire such communications data with some service providers willing to assist but others less so. Any government response must ensure that such services are covered and are included in the RIPA regime. Additionally, the response must be sufficiently flexible to ensure that future changes in the communications environment and in the fragmentation and divergence of communications services do not have an undue effect on law enforcement capability.

**Q3 Do you support the government's approach to maintain our capabilities? Which of the solutions should it adopt?**

The appropriate response to this problem is to ensure that law enforcement maintains the capability to solve crimes, bring offenders to justice and safeguard victims using communications data. Whatever solution the Government decides on must ensure that law enforcement continue to be able to resolve communications data from the online environment, regardless of whether it relates to static or mobile internet access, services based outside the UK but used by the UK public, or any other form of internet service that is used within the UK that may be able to provide communications data to assist in solving crime and protecting the public.

The government must work with communications service providers in order to resolve this issue; indeed some CSPs are already taking the initiative and developing technologies that will provide an understanding of the activities that are occurring on their networks, primarily in order to ensure that they achieve the maximum commercial potential from their networks but also with the ability to

provide greater safety and transparency. It is government's role to ensure that this approach is universal and to promote and develop such initiatives.

One area that must be reviewed is the issue of cost recovery for the acquisition of communications data. It seems anomalous that not only does government pay for CSPs to develop, build and implement data recovery and retention systems, but that law enforcement are then expected to pay to access that data. In effect, government is allowing itself to be double charged. Whilst it is accepted that in order to achieve appropriate data quality and recovery speeds to satisfy law enforcement requirements government should pay for the recovery and retention systems that CSPs implement, the additional charge for the acquisition of this data by law enforcement is a burden that should be reduced where appropriate.

From CEOP's perspective, our work does much to ensure that CSPs' customers remain safe in the online environment and thereby protects their corporate reputations. A number of CSPs have recognised this and have decided to allow CEOP access to communications data for free. Child protection is everyone's responsibility and those that provide services to children should follow the example of others who recognise the benefits of CEOP's work and allow free access to information which is sought in the interest of child protection. Whilst recent developments in cost recovery processes such as the current pilot of a centralised charging regime are welcome, far greater transparency is required. Additionally from a wider law enforcement perspective it is recommended that the cost recovery regime should be moved from a 'per request' basis to a static 'per user' basis so that law enforcement pays for a license to access the data on an annual basis in much the same way as it accesses other databases.

**Q4 Do you believe that the safeguards outlined are sufficient for communications data in the future?**

We believe that the current safeguards are sufficient and the process for the acquisition of communications data ensures that only where proportionate and necessary are rights to privacy invaded. Were additional levels of bureaucracy to be implemented, the ability to access communications data in a timely operational manner would be impeded and its value and use in investigations reduced.

**AQ1 Previous public consultations have set out how vital communications data is to law enforcement, security and intelligence agencies and emergency services in tackling crime, maintaining our national security and safeguarding the public. The government has recently mandated communications service providers within the UK to retain data they process of generate until they are required to disclose it –**

- **Where such communications services do not generate data within the United Kingdom do you agree with the government's proposal to intervene and develop a capability enabling law enforcement and the intelligence agencies to respond to the new communications environment?**
- **If not, why not and can you suggest another way forward?**

- **Would restricting access from internet users within the United Kingdom to communications services situated outside the United Kingdom be justified as a reasonable alternative?**

CEOP is already engaged with a significant number of services that are based outside the UK. It is likely that this situation will only increase with the growing divergence in internet service provision. Where services are based has absolutely no impact on the take up by UK users of such services as evidenced by issues such as cloud computing. The fact that some UK users will access sites and use services based abroad for criminal purposes should not affect the ability of UK law enforcement to acquire this data in order to identify criminals and locate and safeguard victims. Simply preventing UK users from accessing sites based outside the UK is unrealistic and unworkable.

**AQ2 If the Government chose not to intervene – do members of law enforcement believe there is a current or future threat from such communications services being openly available for use by criminals who may be able to exploit these facilities in an attempt to circumvent detection?**

The threat is defined above; it is current, very real and will only increase in the future.

Furthermore, many online sites decline to embed the 'CEOP Report' tab in them despite this being identified as best practise by the Home Secretary's Taskforce on Internet Safety in their Guidelines for Social Networking Sites. Embedding the 'CEOP Report tab' would ensure that children are able to report directly to law enforcement and child protection professionals best placed to take appropriate safeguarding action, as well as acting as a deterrent for offenders. Additionally some of the same sites also fail to report proactively to CEOP, primarily because they are based outside the UK and there are no mandatory reporting requirements. This also has an impact on the ability to acquire communications data as they are not required to comply with RIPA, or fall outside the legislation because they are defined as information society services. Some provide communications data on a voluntary basis but others are less inclined to do so. Therefore for those children in certain social sites who are targeted for abuse, they are unable to report directly to child protection professionals from the site where they are groomed, the site itself takes no responsibility for reporting and even if the child is able to identify that CEOP is an appropriate place to report such behaviour to, CEOP may then be unable to take appropriate action to identify the perpetrators of the abuse. The ability of law enforcement to protect children is thereby hampered significantly by poor child protection policies in the online environment and then compounded by their inability to access communications data that is the only means of identifying the perpetrators of the abuse and their victims.

**AQ3 Do you have examples from recent investigations or operations where you sought access to communications data where –**

- **Data was generated or processed but was not retained or retrievable?**
- **Services accessed by people in the UK but system providing service hosted outside of the UK had a significant delay or obstruction in acquiring data due to prolonged or obstructive legal process?**
- **Services accessed by people in the UK but system providing services hosted outside of the UK but there was a significant security risk in making an approach within the hosting state and so none made?**

The implications of the inability to identify individual alleged to be involved in child sexual abuse are significant. Child sexual offenders are able to continue abusing their victims; victims remain unidentified and subject to continuing abuse and law enforcement are unable to protect the most vulnerable members of society. The effectiveness with which police are able to investigate an offence must not be determined by which service provider the victim or offender has used; such a lottery is unacceptable in the ability of law enforcement in protecting children from sexual abuse.

**AQ4 Do you consider the current legislation (Part I RIPA which related to the (i) interception of communications and (ii) the acquisition and disclosure of communications data) meets your operational needs. For example**

- **Having to differentiate between notices and authorisations despite the processes set out in the Chapter II Code of Practise which partly reduces unnecessary bureaucracy for subscriber information**
- **End user device seized for evidence but the communications service provider and the communications system are outside of the UK**

The difference between notices and authorisations adds unnecessary bureaucracy in the process. Those systems which automate the acquisition process for law enforcement agencies should be adapted to ensure that only the safeguards and authorisation processes written in the Act and Code of Practise are embedded within their automated process and that unnecessary bureaucracy is not included.

In summary, if current capabilities are not maintained, the ability to identify, locate and protect children will be significantly degraded. Government must lead the way in ensuring that this capability is maintained and that the changing communications environment does not create a situation where those who prey on the most vulnerable members of society are allowed to do so with impunity and where law enforcement are unable to react in an effective and timely operational manner to this threat.

CEOP is content for the Home Office to state in the Government's response to the public consultation that CEOP has contributed with a detailed submission. The CEOP response to this consultation is marked as 'Restricted'; however it is recognised that parts of this response may assist the public in understanding the wider issues in relation to the acquisition and use of communications data in protecting the public. It is requested therefore that officials consult with CEOP prior to the inclusion of any extracts or reference to CEOP's paper in the wider Government response.