INDEPENDENT INQUIRY INTO CHILD SEXUAL ABUSE

INTERNET INVESTIGATION – PHASE II

CLOSING SUBMISSIONS ON BEHALF OF THE NCA

---

1. The focus of these closing submissions will be on the specific measures that, in the view of the NCA, industry can and should implement to reduce the prevalence of child abuse facilitated by the open web. They aim to identify why those measures are important and why we would respectfully invite the Inquiry to endorse them. But before turning to those measures, may I say a word about the context in which these issues need to be considered.

Scale of the Problem

2. As Mr Jones explained, the scale, severity and complexity of this offending are increasing. There are more images in circulation, more criminals engaged in increasing levels of depravity, and more complex patterns of offending developing every day. This problem is getting worse, on a daily basis, and at an alarming rate.

3. In her opening statement CTI posed the question of whether the increase in NCMEC reports was indicative of an increase in offending or an increase in detection. It is difficult to provide a precise answer to that question but in the NCA's judgment both factors are in play. Many of these offenders follow a process of escalation from images, to contact abuse. You heard the example of Tashan Gallagher, a young man of 31 at the date of conviction, who went from viewing images on the open web of abuse to raping a 6 month old baby in 2 ½ years. The ease with which an individual with a sexual interest in children can start that journey on the open web, on platforms and services that are available in all of our homes, on all of our devices, is scandalous.

4. An analogy that is often used by law enforcement in this area, referred to by Mr Jones, is of building a wall in front of those who would wish to pursue a sexual interest in children.

5. The fact that this is even possible should, we would suggest, be a matter of the very gravest concern to those companies who run, and profit from, these services. It should be a matter of the very gravest concern to those of us who use them, and to those companies who support them with payment for advertising or other services. The prevalence on the open web of images of CSAE, and the use of the open web to groom and live stream abuse of children represents a crisis of modern society. This problem is properly to be regarded as an emergency. It is treated as such by law enforcement. It needs to be treated as such by industry. .

6. That is the context in which the evidence you have heard over the last 2 weeks falls to be assessed. It leads to the question of whether, in the Panel's judgment, this situation is being treated as a crisis by the companies from which you have heard. Google's systems being infected by some form of malware which took its search engine down for an hour or two would be a crisis. A cyber attack which stole the financial information of an internet company's customers would be a crisis. The resources that are devoted by these companies to keeping their platforms and services secure from this type of attack are enormous, and they are remarkably effective. We can perhaps imagine their response were they to fail. And so we pose the question of whether the fact that, on a daily basis, the platforms and services provided by these companies are used to facilitate the sexual abuse of children is treated as the crisis that it undoubtedly constitutes? Is it given the priority it deserves? Does the trajectory of the industry response in this area match the trajectory of its profits? Now it is not the case that the companies from which you have heard over the last two weeks are doing nothing to address this issue, but when their response is considered in its proper context, are they doing enough?

7. So let us be clear, first of all, as to the objective, which is the removal of child sexual abuse material from the open web and to make it as hard as practically possible for live streaming and grooming to take place on the open web. We consider this to be a realistic and achievable objective if the resources, the time and the will are invested.

We are also clear as to how we consider industry should get on the front foot in seeking to achieve this objective, and what follows is a series of clear, specific and measurable proposals for industry to adopt.

8. You have heard a great deal of evidence from industry over the last two weeks, much of it was commendable and I do not wish to talk down the efforts of those individuals who, with the best of intentions, are working hard to improve their companies' child protection response. But you may wish to ask yourself whether you heard evidence from any of the industry witnesses that there was a clear plan to address this crisis. Did any of them come before you and say: "we played a large part in the development of the modern internet, we have reaped vast profits from it and become amongst the largest, richest and most technologically advanced corporations the world has ever seen, we are horrified that it is possible to access child sexual abuse material on platforms and services is being used to groom children and live stream abuse, and here is our plan for eradicating this material from our services and platforms". I would suggest not. So, here is ours.

Pre-Screening

9. First, industry should adopt, wherever technologically possible, the pre-screening of material for both known and first generation images of sexual child abuse. The downloading and sharing of CSAM is a criminal offence. We consider that industry should pre-screen material before it is uploaded onto its services or platforms in order to identify and block any such material, and to report the discovery of such material promptly to law enforcement. We consider that such screening should include all of the currently available techniques for identifying both known, hashed images, and first-generation material. And technology should be developed to improve the effectiveness of the latter. We do not think it is sufficient to wait until some later stage in the uploading or downloading process. Material can go viral very quickly.

10. The point at which pre-screening is undertaken is likely to vary depending upon the nature of the services offered by the company in question. But what is important is that all and any opportunities to scan material are taken. Companies should not be permitted, we would suggest, simply to choose not to scan unencrypted traffic across

their platforms for child sexual abuse material. There is, in our view, no balance to be struck here. If is technologically possible to do it then it should be done. Google, you were told, scan outgoing emails on Gmail but not incoming ones. Why not? The technology is clearly there. There is no legal issue, and certainly not one that could not be addressed by the terms and conditions for use of the service. An individual could send an illegal child sexual abuse image to 100 Gmail addresses with a click of a button. That is a crime with devastating consequences being committed on the network. If a company has the ability to stop that from happening what possible excuse might it have for not doing so.

11. The pre-screening should deploy the full range of detection technology that has been developed to date, including photo DNA, the IWF URL list, hashes of known images (including those from CAID), classifiers and machine learning technology. We recognise that some of this technology is still imperfect. There might be some false positives. There might be some irritated customers who suffered the minor inconvenience of being blocked from uploading a particular image onto their Facebook page. But that would only serve as a tangible incentive to the companies to invest in improving the technology or perhaps, in educating the customer base of the scale and nature of the crisis so as to place any such inconvenience in its proper context.

12. You will need to consider whether you heard any compelling reasons from industry as to why this should not be done. It is technologically possible and no-one suggested otherwise. A number of potential objections have been raised by industry at different times including proportionality, human rights, user experience, customer expectations of privacy, and the business model. None of these, in our view, represents anything like an adequate reason not to operate pre-screening.

13. If industry thinks there is a legal problem with implementing pre-screening then tell us what it is and we will assist, with policy colleagues, to address it. User experience and the business model is no excuse. Indeed general references to human rights make, with respect, no sense at all. These companies are offering a commercial service subject to terms and conditions. Those terms and conditions could make it quite clear that it is a condition of use of the service that images will be pre-screened

to detect child abuse. There is no human right, under the ECHR or elsewhere, that has anything to do with that situation whatsoever.

14. A number of the witnesses who gave evidence in response to this key ask spoke of the balance they said needed to be maintained between their customers expectation of privacy and their desire to screen for CSAM. There is no balance, this is criminal material. When you download it and store it in a file on your computer or device you are committing a criminal offence. The essential social contract under which we all live is that you are free to do as you wish as long as you do not break the law. If a potential customer has a difficulty with that let them go elsewhere.

15. But if there are any legitimate objections to the adoption of pre-screening wherever technologically possible, including at any points at which encrypted material is converted into open (such as transfer to cloud storage or backup), then let them be clearly stated by industry and we will;work together to overcome them. The Online Harms White Paper consultation would provide a good opportunity to do so. If there are no such objections then this is a straightforward, technologically possible measure which can, and should, be implemented straight away.

Research and Development

16. The second of the law enforcement key asks I would like to address is that industry ring-fences a proportion of its R & D budget for work on combatting child sexual abuse. A proportion we would suggest, that corresponds to the extent of the problem, and the public assertions that have been made, including to this Inquiry, not doubt sincerely, as to the priority accorded to the problem by the companies concerned.

17. The evidence given in response to this key ask followed a consistent theme. It was repeatedly asserted that developments in other areas might be transferrable to the child abuse context – although you may wish to consider how many tangible examples of that you were given – and that there were various parts of the business which were at least partially concerned with this issue thereby making it difficult accurately to identify how much was spent. Its 'baked into everything we do' said the Apple witness.

18. May be so, we consider that there are at least 4 key advantages to ring fencing a defined proportion of the budget for this purpose.

19. First, a specific focus on a clearly identified problem is likely to produce greater results than simply waiting to see whether some tangential benefit may fall out of a project aimed at a different problem. The hackathon that took place last year provides an excellent example of how focus of how much can be achieved with a rigorous focus in a short space of time. That forum, we were told by the Microsoft witness, generated an idea as to how to tackle online grooming which has subsequently been developed and is now in testing. We would have thought it self-evident that having a research and development team focussed on the clearly defined question of how can we eradicate CSAM from our platforms would achieve greater progress than waiting to see whether the answers to different questions might generate some transferrable benefits.

20. Second, a ring fenced budget would make it easier to measure and assess progress in this area, and ensure that those involved are accountable for, and recognised for, their acheivements. A company could explain to its shareholders, its customers, the public, and government precisely what it was doing in this regard and precisely what it had achieved. Executives and shareholders would want to see of itself a return on their investment in this area, and that would provide a clear incentive to progress.

21. Third, it would assist all of those with an interest in this area, including customers, to judge how seriously a company was taking this issue. How much is it really prepared to invest. How does that compare with research and development in other areas? Of course investment elsewhere may lead to transferrable benefits, but that is true of every aspect of the companies' operations. A clear and unequivocal statement to the effect that we are spending x% of our annual research and development budget on eradicating child sexual abuse and exploitation from our service or platform would, we suggest, make it perfectly clear how high a priority this was for the company concerned.

22. Fourth, ring fencing of this particular area of development would make collaboration easier across industry. Companies in competition with each other are understandably reluctant to collaborate and share the product of their research and development. However, all of the companies that have given evidence to the Inquiry have said, sincerely we are sure, that the fight against online child sexual abuse and exploitation is a matter which transcends profits or competitive advantage. On that basis a ring fenced R & D team solely focused on the eradication of CSAM at, for example, Google ought to have little difficulty in collaborating with the corresponding team at Microsoft, both of which are working to the shared objective of eliminating such material from the open web.

23. So, having heard the industry response to this key ask, the NCA remains firmly of the view that it is necessary and proportionate.

24. Indeed, if this was the position now, we anticipate that the Inquiry would be more convinced by evidence such as that which we heard from the Apple witness to the effect that she wished from the bottom of her heart that there was some way of identifying a secure means of scanning for CSAM on an encrypted platform. As it is, we fear that the evidence such as this, whilst no doubt sincerely given, inevitably prompts the question, 'how hard have you tried?'

Identity Verification

25. Next, identity verification. We consider that robust age and identity verification procedures are vital in mitigating the online child abuse threat, particularly in respect of encrypted services and platforms where it is one of the few things that can be done to mitigate the enormous difficulties that the adoption of encryption poses for effective law enforcement in this area.

26. None of the platforms or services about which you have heard, operate any meaningful process of age or identity verification. If a child under the age of 13 wishes to open an account on a platform specifically designed for children above that age they need only put in a fake date of birth. That is true for Facebook, YouTube and a host of similar platforms. If an adult wishes to set up an account in a fake identity in order to pretend to be someone else on a social media platform he or she

need only generate an email address or acquire a mobile phone number in order to do so – both of which could hardly be simpler.

27. It is the NCA's assessment, informed by research with offenders, that identity verification acts as a powerful disincentive to online offending. Indeed, that is little more, we would suggest, than common sense.

28. Before turning to the industry evidence you have heard on this issue we would invite the panel to step back and consider the context. A number of the platforms and services about which you have heard operate on an encrypted basis. We have been told that this is what their customers want, and maybe so. There are clearly advantages in maintaining the security of our data. But there is no obligation on a company to operate its platform or service in this way. It is a deliberate choice, one effect of which has been to make it much harder for law enforcement to identify illegal child abuse activity on that platform or service. It is simply not good enough, therefore, for a company which chooses to operate an encrypted service to shrug its shoulders and say that there is nothing it can do. The making of that choice generates a responsibility to mitigate its harmful effects.

29. And one of the ways in which such mitigation can occur is by requiring identity verification. There is nothing technologically complicated about this. Nor, we would suggest, is there anything particularly difficult about the principle. There are a whole range of services which require identity verification from opening an online bank account to claiming a refund when your train is delayed. Numerous types of device require the provision for some form of biometric data, such as a fingerprint. It is not uncommon to be asked for your address when you make a routine purchase in a high street shop. It is not uncommon for children or their parents to have to verify their age when they seek to purchase a reduced price train ticket or entry into a cinema.

30. Why should you want people setting up accounts on your platform using fake identities? Why, if you operate a service designed for children above a certain age, should you have any difficulty whatsoever in requiring children to establish their age when opening an account? What is the legitimate and compelling reason for not doing so that is sufficiently powerful to outweigh the child protection benefit? We

struggle to imagine what it might be, but if there is some legitimate objection to identity and age verification then it is incumbent on industry to identify it clearly and to come up with an alternative means of addressing the problem it has created by the development of encryption. We would suggest that unless and until it does so, then this is a good place to start.

Kite-Marking

31. All of the issues I have addressed up to this point – pre-screening, ring-fenced funding, identity verification – are relevant to the third of the three key law enforcement asks, namely the establishment of some form of kite marking to enable the public, including parents concerned with the online activity of their children, to readily identify which services and platforms are actively engaged in the fight against online child sexual abuse and exploitation and which are not. If you want to run a platform that enables people to set up accounts using fake identities, or allows children to join without verifying their age, then so be it but it should be clear to everyone that this is the choice you have made. Similarly if you choose to allow the uploading of material without screening it for illegal child sexual abuse content, or if you choose not to devote any of your research and development funding exclusively to this problem.

32. We would also suggest that a system of kite marking could reflect the efforts made by the companies concerned to ensure that users of their platforms and services were properly educated as to the available safety features and the steps that parents could take to ensure their children were safe on line. The NCA produces a significant amount of targeted educational material of this nature. There is clearly scope for that material to be actively promoted by industry providers. A kite marking system could address not just the availability of these measures – and there is clearly scope for cross industry collaboration here – but also the extent to which they were effectively promoted by the companies concerned.

33. In short there are considerable benefits to such a scheme and no disadvantages.

Streaming and Grooming

34. Finally, I would like to deal briefly with the particular challenges that arise in respect of live streaming and grooming, and the specific proposals the NCA would invite the Inquiry to consider in this regard.

35. A number of the measures I have already addressed, including identity and age verification and kite-marking, are directly relevant to abuse by grooming and live streaming and would, in the NCA's assessment, serve materially to reduce the prevalence of these forms of abuse on the open web. But in addition to those measures we consider that there are a number of further steps that industry can, and should, take to address the particular challenges posed by grooming and live streaming.

36. First, we consider that there should be a significant increase in the use of live moderation on forums, of the type you heard described in respect of Xbox and Yubo. Anywhere this form of live moderation can be done it should be done. .

37. Second, priority should be given to the development of AI, machine-learning and any other technological capabilities to identify suspicious traffic over encrypted platforms. As you have heard, companies that choose to operate their platforms and services in this way cannot listen to, or moderate, the content of the communications themselves; but there is other data that can be analysed. To take a simple example, apparently one-sided communications between the UK and the Philippines, late at night in the UK would raise obvious concerns. Those concerns might be allayed, or reinforced, by reliable age and identity verification. The provider could then suspend the account pending verification and, where appropriate, make a report to law enforcement. Once again we ask, if you were really serious about ensuring that your platform was not used to facilitate the live streaming of child sexual abuse why would you not do this?

38. Thirdly, and as I have mentioned, these measures need to be backed up with a robust policy of suspension pending verification. Where it is suspected that a particular account is being used to facilitate CSAE, for example, allowing the live streaming of contact abuse the account needs to be disabled straight away and steps taken

immediately to verify that the communication is legitimate. There is no reason why that should not be achievable quickly and efficiently and the request for verification itself will usually be enough to cause the offender to desist.

Concluding Remarks

39. In conclusion, therefore, the NCA considers that there needs to be a fundamental change in outlook and approach on the part of industry, that reflects the scale of crisis with which we are faced and the responsibility of industry to play its part in the eradication of child sexual abuse from the open web.

40. Real progress in this area can only be achieved by deep and extensive collaboration between law enforcement and industry and I would wish to reinforce the point that Mr Jones made repeatedly in the course of his evidence: the NCA is open for business in this regard. If there are things that industry is able to do but is concerned about from a regulatory or legal perspective, communicate those concerns to us and we will work with policy owners to address them. Up until now, far too much of the interaction has been reactive on the part of industry. We need industry to get on the front foot and engage with us actively in finding solutions.

41. Finally, how they should do this in a series of 6 bullet points:

    - One: wherever technologically possible there should be pre-screening of all content for known child sexual abuse material – through the use of hashes and URL lists on the existing databases and using the developing AI and machine learning technology to identify first generation images. This should include all downloads and uploads onto social media platforms, incoming emails, and transfer of material to cloud storage.

    - Two: there should be ring-fencing of a proportion of each company's R&D budget solely and specifically devoted to the eradication of CSAE from the company's platforms and services.

    - Three: rigorous age and identity verification procedures should be implemented to ensure that those individuals who seek to use these

platforms and services are who they say they are, particularly for those platforms and services that operate on an encrypted basis.

- Four: there should be a robust system of kite marking or grading clearly to identify – to shareholders, customers, parents and the public – which services and platforms are safer for children and which are not.

- Five: communications over the open web should be monitored to detect evidence of grooming, through the use of communication analysis and live moderation in open communications, and sophisticated data analysis for encrypted communications, with suspect accounts and forums suspended pending verification.

- Six: communications-related data should be analysed to detect evidence of potential live streaming of abuse, and any such accounts should be suspended pending verification, so as to allow genuine users to establish their bona fides and assist in reducing the number of false positives.

42. We see no reason why these measures could not, or should not, be taken now.

43. May I finally say a word about your legal team. I am sure that the Panel is, by now, well used to the highest standards from its counsel and solicitors but we would respectfully observe that the presentation of the evidence in this complex and technologically challenging area of the Inquiry's work has been exemplary. Furthermore, the NCA has been treated throughout this investigation with the highest standards of professionalism and courtesy by the entire Inquiry team and we would wish to record our thanks and appreciation for that.

44. We look forward to the Inquiry's report in due course and if there is any further assistance we can provide in the meantime then we would be delighted to help in whatever way we can.

NEIL SHELDON QC

24 May 2019