IWF response to Mozilla's comment period on DNS over HTTPs implementation

1. Introduction

1.1 The Internet Watch Foundation has been critical of attempts by the Internet Engineering Task Force (IETF) around the design of its new technical standard for DoH. We have also criticised technology company's approaches to the introduction of the new standard and tried to work with those companies to ensure the safety and welfare of children is considered at all stages in implementation. We also recognise the steps that companies have taken to improve their response to consider our concerns and welcome the opportunity to respond to Mozilla's open comment period on its implementation.

1.2 We raised our concerns in a series of blogs in June 2019, July 2019, October 2019 and November 2019 and 19 of the Internet Watch Foundation's UK Parliamentary Champions also co-signed a letter, published in the Sunday Times, to the then Secretary of State, Nicky Morgan, about the issue and our concerns for online safety of children. Pressure from child safety organisations like the IWF and the UK Government, led to Mozilla abandoning its attempts to role out DoH by default to the UK market.

1.3 To be clear, the IWF is not calling for DoH to be banned. We recognise there are benefits to securing the DNS system from a cyber security perspective and there are legitimate reasons for wanting to ensure greater privacy online. However, we believe, that the right to privacy is not an absolute right and there are times, when, as a society, when we act to take an individual's right's or freedoms away from them. For example, when they commit a serious crime and are incarcerated for the wider benefit and safety of society.

1.4 When the IETF established the technical standard and companies began to implement the new standard, at both stages in that process, there was a lack of consideration given to what these new standards may mean for the protection of children.This situation could have been prevented from happening by having a more open consultation process in both the development of the standard and how companies intended to implement it. We appreciate balancing the need for privacy and safety is a complex challenge, but it is possible to have both, with appropriate safeguards and checks and balances.

1.5 Our main concern was about the impact DoH could have on online safety and most of the remarks we make on this comment period centre on this. We are particularly concerned with the impact rollout will have on the IWF's URL blocking list and it should not be underestimated how important this service is to keeping internet users safe online and preventing images of sexually abused children being widely available on the surface web. We are also particularly concerned that parental controls which are determined by parents when they establish their internet connection in the UK would also be bypassed without their knowledge through a company's deployment of the new DoH standard in apps, web browsers or even by changing the Trusted Recursive Resolver (TRR) without the knowledge or explicit consent of the end user. Even when an end user does consent, it is also possible that there is a lack of meaningful understanding about exactly what these implications may mean to a non-tech savvy internet user.

1.5 In just one-month last year, April 2020, we saw internet use increase significantly because of the global Covid-19 pandemic and the impact of national lockdowns imposed by Governments became clear. In the UK, the IWF along with our industry partners (just 3 industry partners who provided data) successfully blocked 8.8 million attempts from UK service users to access known child sexual abuse material. Whilst we cannot equate this to individuals directly, what we can tell you is that is a staggering number of attempts across just one country and this list is also deployed globally.

1.6 Finally, whilst we recognise the importance of this comment period to Mozilla's product and policy development, we are concerned that some of the questions have been framed in such a way that very

clearly guides respondents about the policy direction of Mozilla. Privacy considerations are still much more front and centre in its thinking than concerns for the protection of children.

2. About the Internet Watch Foundation (IWF)

2.1. The IWF is a charity that works in partnership with the internet industry, law enforcement and Government to remove (with the co-operation of industry) from the internet child sexual abuse images and videos wherever they are hosted in the world and non-photographic images hosted in the UK.
2.2. The IWF exists for public benefit and performs two unique functions in the UK:

A) We provide a secure and anonymous place for the public to report suspected online child sexual abuse images and videos and;

B) Use the latest technology to search the internet proactively for child sexual abuse images and videos.

2.3. The IWF has a Memorandum of Understanding between the National Police Chiefs' Council (NPCC) and Crown Prosecution Service (CPS) that governs our operations. This ensures immunity from prosecution for our analysts and recognises our role as the "appropriate authority" for the issuing of Notice and Takedown in the UK. Operationally, the IWF is independent of UK Government and law enforcement.

2.4. The IWF also seeks to work globally to solve the problem of child sexual abuse online. We, in partnership with the Global Fund to End Violence Against Children, are currently working with some of the most underdeveloped countries in the world to provide their citizens with a reporting portal in their own local language, which then comes through for assessment to the IWF HQ in Cambridge. There are currently 43 globally and we aim to have 50 by the end of 2021.

2.5. The IWF also plays a vital role in providing the internet industry with several quality-assured technical services to prevent the spread of known child sexual abuse images and videos online and to stop the uploading of new images in the first place. These include image hashing utilising Microsoft's PhotoDNA, a URL blocking list of live webpages, keywords list, domain alerts, payment brand alerts, newsgroup alerts and simultaneous alerts (for US companies only). Key to this is our trusted relationship with the internet industry which enables us to act as a broker between them, Government, and law enforcement.

2.6. Our work is funded almost entirely by the internet industry: 90% of our funding comes from our 152 global Members which include Internet Service Providers (ISPs), search engines, Mobile Network Operators, and manufacturers (MNOs), social media platforms, content service providers, telecommunications companies, software providers and those that join the IWF for CSR reasons.

2.7. The remaining 10% of our funding comes directly from the European Commission's Connecting Europe Facility for our role within the UK Safer Internet Centre, providing a Hotline resource for the UK.

2.8. The IWF is a charity registered in England & Wales with an 11-person Board of Trustees of which, eight are independent members and three are industry representatives. The IWF Hotline is audited by an independent team, led by a judge, every two years and the report published in full on our website.

3. Recommendations

- **That Mozilla carefully considers the safety, protection, and welfare of its users as well as their rights to privacy. It is possible to have both safety and privacy, but privacy is not an absolute right and there are situations when the safety and protection of citizens must be put above privacy concerns, particularly when it comes to the protection of children online.**

- **Trusted Recursive Resolvers (TRRs) providers should be encouraged to join the IWF and take its URL blocking list to prevent access to child sexual abuse material online. This, is not an absolute magic bullet, as access to parental controls also needs to be resolved but would be a welcome step in preventing access to Child Sexual Abuse Material.**

- **Ultimately, the position of the IWF remains unchanged, companies implementing the DoH technical standard should ensure equivalency with whatever protections are currently offered to users through their ISP and where changes are made that they give informed consent and fully understand what this means in line with GDPR.**

4. Online Safety

1. Our current policy states that the provider operating the resolver should not by default block or filter domains unless specifically required by law in the jurisdiction in which the resolver operates. How, if at all, should this requirement change to address legally required blocking in other jurisdictions?

Internet users without technical expertise of how the internet works are highly unlikely to have heard of a Trusted Recursive Resolver or understand the impact that changing a Trusted Recursive Resolver has on their use of the internet. Most internet users - around 90% - will use the resolver provided to them by their internet service provider if you look at the average figures across ISPs.

Whilst internet users, browser providers, ISPs, apps and the like can choose to change their Trusted Recursive Resolver, it does require some technical knowledge and understanding.

The proposal outlined above, and that Mozilla is consulting on, is potentially problematic for the safety and protection of children online. The deployment of the IWF's URL blocking list is on a voluntary basis and made available to companies that join the IWF's membership and can and is deployed globally. The importance of this list is, that we can act prior to the Court process to remove content swiftly and effectively in line with UK law guidelines. We offer people with the ability to appeal the decision to remove content, to our CTO in the first instance and finally if they are not content with the outcome, ultimately Judicial Review.

We believe that it is important that this service is not circumvented by TRR's on the basis that the list is not specifically required by law to be implemented. This list plays a vitally important role in protecting victims of child sexual abuse who have had their suffering further compounded by having permanent records of their abuse spread online to be viewed by others. We would urge Mozilla to ensure that they consider the privacy considerations of those that have been so egregiously harmed as well as that of the service user in the development of its DoH policy.

Whilst it is recognised that individuals who are determined to locate and view criminal imagery online can take steps to deliberately circumvent the blocking or filtering of URLs, the blocking list is also of importance in preventing internet users who may otherwise have accidentally stumbled upon criminal imagery and instead get served with our splash page. The National Crime Agency in the UK estimates that as many as 300,000 people pose a sexual threat to children either online or through contact offending and the 8.8 million requests in just one month to access URLs containing known child sexual abuse imagery, demonstrate the staggering size of this problem. If each one of these attempts had been successful in returning CSAM, then the criminal justice system would simply fall apart trying to enforce and sentence all those offenders. It is vitally important that we take a preventative approach and stop offending from happening not only in our communities, but also in the online environment.

The issue with TRRs adhering to the law in which they are jurisdictionally operating means that TRRs could be established in countries where there is a lack of online safety laws, accountability for companies to ensure safety for their users and where law enforcement mechanisms are weakest. This is a problem that we see regularly - websites dedicated to the distribution of child sexual abuse

content is are frequently hosted in places where, for the same reasons outlined above, it becomes very difficult to remove.

Our recommendation would be that TRRs are encouraged to join the IWF and take the IWF's URL webpage blocking list to ensure that access to Child Sexual Abuse Material is blocked when a service user requests access to that site/image. We would like to see TRRs being held to the same standards of protections for children as you would get from your Internet Service Provider.

It is important, however, to recognise that this will not solve all the problems related to child safety online. More consideration needs to be given to how the implementation of a new TRR will ensure that it won't bypass the vitally important parental controls that are established at the time a parent establishes their internet connection.

2. What harmful outcomes can arise from filtering/blocking through the DNS?

In responding to this, we would like to suggest a reframing of the question. In the context of child protection online, the harmful outcomes that can arise from not blocking or filtering Child Sexual Abuse Material are well-documented, and victims cite the devastating impact on their recovery of knowing images of their abuse are in circulation and being repeatedly reviewed online.

We have also outlined additional considerations in response to question one. Broadly speaking, we believe that Mozilla should be considering the harm and damage done to victims of child sexual abuse and their privacy rights, if this filtering and blocking were not to continue. We also call on Mozilla to consider the implications to a family of someone being arrested on suspicion of viewing indecent images of children, which they may otherwise have been prevented from seeing had blocking and filtering been available. The benefits of blocking also means that we can warn people about their potentially criminal behaviour and the consequences of that behaviour and direct them towards organisations such as the Lucy Faithful Foundation, who can offer support, counselling, and advice in changing potentially criminal online behaviour.

We also want to provide further clarity on how our URL block list works, we do not filter or block at the DNS level, but at webpage level. We recognise that at the infrastructure level, it is much more difficult to take filtering or blocking action for a variety of reasons. The IWF does, however, work with domain name providers, registries, and registrars to improve the response to tackling child sexual abuse and exploitation online.

3. What more rights-protective and technically effective means of protecting users from illegal and harmful content exist beyond DNS based blocking?

One of the most widely discussed and proposed ways of tackling illegal content is device level protections. Whilst this is certainly a possibility and not something which should be ruled out in the future, there are some problematic issues with this. Firstly, it becomes easier for people, particularly paedophiles, to identify and therefore, target devices that have parental controls deployed upon them as they know that these will be devices operated by children and young people and makes them potentially, personally identifiable.

Secondly, this could potentially lead to the need for implementation of even more privacy-intrusive techniques such as deep packet inspection, which is not only extremely expensive, but also time consuming for law enforcement once devices are seized and would potentially delayed justice be being served to perpetrators and in the interests of victims.

Finally, whilst device level protections would be effective at dealing with known child sexual abuse imagery and these could effectively be blocked from view at device level, it does not take into consideration the detection of new imagery, or of situations such as online grooming and sexual

coercion, which may lead to both the exploitation of children and the production of new child sexual abuse imagery and for mechanisms for detection are available in the present protection framework.

4. How could we ensure effective transparency and accountability in situations where TRRs engage in legally required blocking practices? (For example: publicly available transparency reports with blocked domain names by country.)

As mentioned above, the IWF's technical tools and services that it offers to industry are independent of Government, Law Enforcement, and the internet industry itself. This is important because it means that our judgement is free from interference from any of these actors and they all act as a check and balance on the organisation and our outputs. For example, law enforcement and government would not permit us to carry out our work if it were not of a high quality and the industry would not sign up to membership and deploy our services if these were not effective.

We are a transparent organisation, and we exist for public benefit and the public can ultimately hold us accountable for the decisions we make. We have an independent member of our board who is a human rights specialist, we have the right to appeal decisions we have made including judicial review and every two years we are audited by a Senior High Court Judge who makes reports on our processes and structures and makes recommendations for improvement. All these reports are made available on our website in line with our commitment to transparency about what we do.

However, it is important to note, that in the field of tackling child sexual abuse and exploitation online, it would be simply unacceptable to publish a list of blocked domain names by country. This would have the effect of simply directing people towards criminal material which would be deemed to be a criminal offence in most jurisdictions and increase the harm to the children whose sexual abuse is permanently documented in the images which are contained on the webpages on the list.

5. How can we best present information about opt-in filtering endpoints to end users (e.g., for malware blocking or family-friendly blocking)?

It is important to understand that blocking and filtering is not always the blunt instrument that is often suggested and the approach of the IWF is certainly much more nuanced than this. For example, we offer the IWF's URL list to several Universities within our membership. This is precisely because they want to block access to Child Sexual Abuse Material and terrorist content but want to allow students the ability to freely express themselves during their studies. This therefore means that they can shape their networks accordingly to ensure that their students benefit from a full and rigorous academic education that enables them to explore challenging societal issues and ensuring freedom of expression, without committing serious criminal offences related to child sexual abuse and terrorism.

Finally, at the other end of the spectrum we also offer the URL list to filterers who provide this in addition to a range of other services offered out to school networks. This also offers headteachers the ability to pick and choose and shape their networks accordingly, but ultimately ensuring that harm is prevented from being done to children.