Response to the Mozilla DoH Comment Period

Introduction

Opendium supplies British schools with network based online safety systems, in line with the Department for Education's "Keeping Children Safe in Education" statutory guidance, the Home Office's "Prevent" strategy and the UK Safer Internet Centre's "Appropriate Filtering" guidance.

Schools have a number of specific requirements that are frequently overlooked when vendors implement new technologies. We hope that this document can provide some insight into the challenges and allow the right balance to be struck.

Legal Background

English schools are required to follow the statutory guidance provided by the Department for Education, which in turn references guidance provided by the Home Office and the UK Safer Internet Centre. There are similar requirements placed on schools within the all of the UK's devolved administrations.

All schools in the UK have a legal obligation to keep the children under their care safe from online harms, and there are usually both technical and social elements to their strategies.

Firstly, there are some fairly uncontroversial measures, such as blocking unlawful content promoting terrorism and illegal content showing child abuse. The Home Office and Internet Watch Foundation, respectively, provide URI block lists of such content.

Secondly, legal, but grossly inappropriate content, such as pornography, must be considered. Schools have some discretion as to how to handle these kinds of content, and may choose to employ different policies for different age groups. Clearly, some content which is appropriate for older high school students is not appropriate for very young children.

Thirdly, schools are required to work to prevent the children under their care from being radicalised by extremist groups, at the same time as allowing and promoting understanding and discussion of these sensitive topics.

Schools also have a duty of care regarding the children's health in general, and may choose to use software to alert them to concerning online behaviour in conjunction with the usual in-person monitoring and intervention of behaviour by staff. Behavioural profiling in this context is sometimes seen as controversial, but ultimately whether such technologies are appropriate is a decision for the schools, parents and children.

Schools are expected to manage the risks for all devices on their networks, both their own workstations and any personal devices connected under a Bring Your Own Device policy.

Balancing Risks

Encrypted communications are of course extremely important to prevent the harm caused by bad actors. However, the belief that more privacy is *always* better is simply not true. It is important make a distinction between children and adults: by law, children are not expected to be responsible for their own safety. Whilst their guardians shouldn't have an absolute right to invade a child's privacy, it is impossible for them to protect a child who is given absolute privacy.

In recent years, a number of policies and technologies have been imposed upon users by various organisations, in the name of privacy and security. These are laudable goals, but there has frequently been little or no consultation and no inclination to discuss problems once they become apparent. What's more, these new innovations are frequently designed to take choice out of the user's hands.

We very much feel that the right balance should be determined by the end users, parents and schools. Not imposed by governments or "untouchable" organisations. It should be straight forward for users to enable, disable or reconfigure privacy technologies to meet their needs rather than a policy of "absolute privacy at all costs" to be dictated from on high.

Technology

In order to carry out their legal obligations regarding child safeguarding, schools routinely decrypt HTTPS traffic by means of a man-in-the-middle proxy. This cannot be done covertly on personal devices and requires the user to make an active choice to install a certificate.

Google, in particular, are very hostile to HTTPS decryption and have imposed policies upon Android devices which prevent the user from making their own choice. This is of great concern to schools, as around 79% of the terrorist content and up to 92% of the child

abuse images that schools are required to block access to cannot be blocked without the use of HTTPS decryption.

Whilst some online safety systems use DNS filtering, our systems currently do not, and we therefore do not expect to be directly affected by the introduction of DoH as a stand alone technology.

However, when combined, DoH and Encrypted SNI are problematic: For both security and compatibility reasons, its important for the proxy to be able to decide which connections to decrypt and which to pass through. We currently use the Server Name Indication of the TLS handshake to do this.

Encrypted SNI is a proposal being incorporated into TLS 1.3 and would break this functionality, but could be worked around by the school's system monitoring or modifying DNS traffic. However, this workaround would not be possible if DoH is used, unless the DoH server being used were the online safety system itself.

It is also important to recognise that devices may be used both in and out of the school's network, so any configuration changes required to allow the device to be used within the school must not cause the device to break when used elsewhere.

Summary

The main point to take home is that none of these technologies are inherently bad, and it is important to protect the user's privacy; but the choice must be in the hands of the user, so we implore Mozilla and other vendors not to simply impose security settings upon their users, but to make it simple for the user and domain administrator to make their own choices.