Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel [redacted]
Fax [redacted]
http://www.microsoft.com/

Microsoft

MEMORANDUM

To **Leveson Inquiry** **28 February 2012**

From **Microsoft Corporation**

Subject **Further information requested during Mr Ronald Zink's testimony on 7 February 2012**

Microsoft Corporation is grateful for the opportunity to provide its answers to the requests for additional information that were raised with Mr Ronald Zink during his testimony before the *Leveson Inquiry* (the "Inquiry") on 7 February 2012.

To assist the Inquiry we have set out in this Memorandum the precise question asked of Mr Zink, in quotation marks, or where we have paraphrased the questioning, without quotation marks. In each case we provide the reference to Mr Zink's transcript where the question and the surrounding context can be found.

"[I]s it technically possible for the browser to be set by Microsoft so that if somebody types in the offending url, the browser will not connect them to the web page?"

Mr Barr QC (Page 29, line 21 - Page 30, line 3)

We believe that it is worthwhile starting our answer by explaining a little about browsers in general. At the most basic level, a browser is software that runs on a device, such as a personal computer or a mobile phone. This software allows its user to “browse” the internet by accessing web pages that are available at particular internet addresses.

Like most software that runs on an operating system such as the Windows platform, there is nothing stopping a developer from building and distributing their own browser to the public. Equally, it is very common for browsers to be made available at no cost to a user.

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

http://www.microsoft.com/

Microsoft

Microsoft Corporation's Internet Explorer is therefore only one of a number of browsers available including Mozilla's Firefox browser, Google's Chrome browser, and the Opera browser to name a few. It follows that there are many ways that users may access websites other than through Internet Explorer. It is also the case that a user might and often does have more than one browser simultaneously installed on a device. If that user is unable, say, to use one particular browser to access a certain website, that user will easily be able to try to access that same website using an alternative browser.

Looking specifically at Internet Explorer for PC's; this has no default client functionality that can prevent users from navigating to specific internet addresses.

The current PC-based Internet Explorer 9 does include functionality called SmartScreen Filter. The SmartScreen Filter functionality, however, will only warn users if they attempt to browse to an internet address that is known to Microsoft Corporation to be either a phishing or a malware website. The user must explicitly turn on this warning functionality. If a user chooses to turn on SmartScreen, some of the internet addresses to which the user browses are then sent to Microsoft to be checked for phishing and malware. If an address matches a known phishing or malware-containing site, the user is warned.

The scope of SmartScreen is limited to phishing and malware websites, and it cannot be modified for particular geographies. It does not recognize websites with the sort of offending content being considered by the Inquiry. Together with the fact that it can be turned off by a user, means that SmartScreen, and Internet Explorer does not offer a way to prevent a user being connected to a particular web page.

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

http://www.microsoft.com/

Microsoft

Are there protective technologies that prevent users of a browser from seeing problematic material on the web?

Mr Barr QC (Page 30, line 4-8; Page 31, line 9-15)

We have understood this question to refer to whether a browser can prevent certain content on particular web sites from being shown to user, but nevertheless allowing the remainder of the non-problematic material to be visible to the user.

As for Mr Barr QC's first question, the Inquiry should note that Internet Explorer is only one of a number of browsers and developers are able to develop new browsers.

The protective technology being referred to in the question does not exist within Internet Explorer 9. The SmartScreen technology not only does not bar a user from viewing certain content on a website – it warns them about an entire website – it can also be turned off or ignored by its user. This would not make it suitable to prevent users of a browser from seeing problematic material on the web.

Are there ways of using the approach taken with PhotoDNA to deal with material that is recognised by a court to be defamatory or in breach of privacy?

Lord Justice Leveson (Page 31, line 17 - Page 32, line 25)

Mr Zink referred briefly in his testimony to Microsoft's PhotoDNA technology. By us explaining how PhotoDNA functions, the Inquiry will be in a better position to understand our answer to Lord Justice Leveson's question.

Microsoft Corporation has developed a technology to help disrupt the spread of the worst known child sexual abuse images online. Microsoft is proud of its PhotoDNA technology and has donated it to the National Center for Missing & Exploited Children. This PhotoDNA technology works on images, not text. The technology uses a mathematical technique known as robust hashing that works by calculating a unique signature into a “hash” that represents the essence of a particular photo. In the same way that the characteristics of every person’s

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

http://www.microsoft.com/

Microsoft

DNA are different, the signature or “hash value” for every photo is different. This enables the creation of a hash that can identify an image based on its unique characteristics or its “digital DNA.” Although a photo’s hash cannot be used to re-create an image or identify people or items within an image, it can be compared with hashes of other photos as a reliable way to match two different copies of the same image.

This ability to match the distinct characteristics of one digital image with another can be used to help online service providers and others better identify and stop the online distribution of known child sexual abuse images. As will be obvious from our answer, this technology addresses only images. The PhotoDNA technology will not therefore function to match text that is recognized by a court to be defamatory or in breach of privacy.