December 9th, 2018
1 Tevet 5779
Jerusalem

To: The Members of the Joint Committee of the Knesset Committee and the Science and Technology Committee to Discuss the Communications (Telecommunications and Broadcasts) Bill (Amendment – Obligation to Filter Offensive Websites), 5777-2016 (P/20/2522) (P/20/3603)

By email: vkalkala@knesset.gov.il

Greetings,

Re.: Position of the Clinic on Digital Rights and Human Rights in Cyberspace at the Hebrew University regarding the Proposed Laws concerning the Filtering of Websites

1. The desire and the need to protect the public in general, and children in particular, against possible injuries in cyberspace are clear and universally accepted. However, due to technological limitations that lead to overblocking and underblocking, imposing legal liability on ISPs to filter content as a default leads to a violation of basic rights that clearly exceeds the advantages of filtering. (See our detailed position in our response to the original version, attached to this document).

2. According to the updated version of the bill as published in the media, the proposal has indeed been moderated, but there is still no reference to the technological method of implementation of the proposed mechanism. The bill is more moderate in that it is suggested that the ISP be required to contact a subscriber three times and offer the filtering service, with or without an access code, before activating the filtering service as a default. Our position is that this bill also fails to respond to most of the difficulties encountered in the filtering of content, and accordingly should not be advanced. We will discuss below the principle difficulties we find in the updated version as published in the Committee and in the media.

Expansion of the Definition of Offensive Content

3. According to the present version of the law, the definition of offensive content is "indecent content" as defined in the Penal Code, including the depiction of sexual

acts entailing violence, abuse, degradation, humiliation or exploitation, sexual acts with minors, and the depiction of a person or a part of a person's body as an available object for sexual use. It is now proposed that the definition be expanded to "offensive content," thereby including the depiction of sexual relations of any type and the depiction of a person's naked body or sexual organ. Apart from the technological difficulty in creating a filter that distinguishes between such content and other content, as described, the expansion of the definition in this manner conceptually includes information of great importance and social value, such as information about breastfeeding, birth, breast cancer, STDs, and so forth. Accordingly, it should be opposed.

Absence of Public Transparency regarding the Effectiveness of the Filter Mechanisms

4. The discussions of the bill have highlighted the lack of reliable information about the effectiveness of the filtering software. In order to respond to this market failing, and instead of the proposed arrangement, our position is that an independent regular could be charged with undertaking an objective inspection of the quality of the existing filter software. Thus all subscribers, including parents of minors, will be able to take an informed decision regarding the use of the filter software according to their needs.

5. It is further proposed that the ISP be required to provide details about the proposed service and the dangers accruing from the use of the internet and exposure to the offensive content. It is unclear whether the ISP will be required to provide information about additional risks on the internet, such as online pedophilia, websites depicting serious violence, computer games portraying serious violence, etc., for which this bill provides no solution. Moreover, it is not proposed that details be provided regarding the effectiveness of the proposed service, its inherent failings – both in terms of overblocking and in terms of underblocking (such as the fact that it does not apply to applications such as WhatsApp), or the ease with which the service can be circumvented. The absence of this information creates a false representation to parents implying that the proposed service provides protection for the children, and does not enable them to make an informed choice regarding the service they wish to consume and the manner in which they wish to protect their children.

6. It is further proposed that the Minister of Communications establish regulations concerning filter software, inter alia concerning the blocking of offensive content, insofar as possible. It should be clarified that when establishing regulations

regarding filtering, the minister should grant considerable weight to overfiltering and to the damage to freedom of expression and access to information caused by the blocking of legitimate content by filter software. We reiterate that overblocking is particularly damaging, since the subscribers are not aware of the information to which they are not exposed. For example, we would note that civil society organizations in Great Britain reported in 2014 that around 20 percent of the content blocked by the voluntary filter mechanism in use there did not include offensive content.[1]

The Inversion of the Default and the Violation of the Right to Privacy

7. The updated version of the bill establishes a mechanism including several stages before the filter services are provided by default. However, in light of the technological limitations were have described, it is difficult to justify the inversion of the default. If the Committee ensures that ISPs and the Ministry of Communications inform the public effectively regarding the possibility to use the filter software, while at the same time the public is provided with reliable information on the capabilities of this software, it may be assumed that subscribers who wish to use the filter software offered by the ISPs will do so, and there is no need to change the default.

8. It should be noted that prioritizing the use of filter mechanisms is also reflected in the proposal to require ISPs to contact every three months only those subscribers who do not use filter mechanisms, and to inform them of this possibility. Such contact in itself constitutes a violation of the privacy of those users who have chosen for their own reasons not to use this software. If the bill is advanced, ISPs should be required to contact all subscribers and to offer them a simply way to join or cancel the use of filter software, if they so wish. Inverting the default, including by means of a user code, will inevitable create a database on individuals who have ostensibly chosen to be exposed to content defined as offensive, and will stigmatize them accordingly. The dangers inherent in the presence of this information, which is liable to leak to third parties, are obvious.

Absence of an Auditing and Correction Mechanism

9. The updated versions of the bill do not include an effective and rapid method for the public to request the unblocking of content filtered despite the fact that it is not offensive. Similarly, the bill does not include any possibility to report

[1] As published on the website: https://motherboard.vice.com/en_us/article/3dka5n/the-uks-internet-filters-block-1-in-5-websites

overblocking by the filter mechanism. It should be noted that given the quantity of information on the web, the possibility to maintain such a mechanism, providing a response in an appropriate timeframe, is also to be doubted. However, if the bill is advanced, it should also include such an auditing mechanism.

Conclusion

10. The discussion of options for protecting minors and web surfers in general against the dangers presented in this domain is necessary and welcome. However, the proposed mechanism does not provide any response to most of the online dangers (pedophilia, violence, online bullying, etc.); neither does it provide an appropriate response to the dangers of the exposure of minors to offensive content. Accordingly, we suggest that the Committee discuss possible methods for raising awareness and knowledge among the public regarding the dangers present on the web and for its informed use.

11. We also suggest to the Committee that in place of the proposed arrangement, the obligation to notify the public be reinforced, so that full information regarding the possibility to use the existing filter software and regarding its level of effectiveness will be exposed to parents when they decide whether to use the filter software, and which filter software to use insofar as they choose to do so.

Sincerely,

Mr. Ron Shamir

Research Fellow

Cyber Security Research Center,
Hebrew University of Jerusalem

Atty. Dana Yaffe

Clinical Supervisor

Clinic on Digital Rights and Human Rights in Cyberspace, Clinical Legal Education Center and Cyber Security Research Center, Hebrew University of Jerusalem

** This document was written with the assistance of two students at the Clinic on Digital Rights and Human Rights in Cyberspace: Aviv Ben Shahar and Omri Barhum.