To: The Members of the Knesset Economy Committee

Ms. Leah Veron, Secretary of the Knesset Committee

By email: vkalkala@knesset.gov.il

Greetings,

Re.: Position of the Clinic on Digital Rights and Human Rights in Cyberspace at the Hebrew University[1] regarding the Proposed Law concerning the Filtering of Websites

Introduction

1. The Knesset Economy Committee has recently discussed two bills relating to the filtering of content by internet service providers (ISPs): The Communications (Telecommunication and Broadcasts) Bill (Amendment – Obligation to Filter Injurious Websites), 5776-2016, tabled by MK Shuli Moalem and others; and the Communications (Telecommunication and Broadcasts) Bill (Amendment – Filtering of Gambling Sites and Content Displaying Obscenity on the Internet), 5777-2016, tabled by MK Makhlouf Miki Zohar.

2. The proposing Members of Knesset expanded on the idea underlying the two bills at a discussion held by the Knesset Economy Committee on July 9, 2018. During the discussion, MK Miki Zohar presented the idea that every internet subscriber should be proactively given a secret code by the internet company for the use of an unsuitable website. In order to surf a website that the filtering software has determined to be offensive, it will be necessary to enter the code provided by the internet company. The Member of Knesset adds that the state would fund all the internet companies, according to the number of subscribers, by 10 million shekels a year in order to cover the costs of this mechanism. In our opinion, this cannot cure the flaws in the bill, as we will detail below. In any case, since to the best of our knowledge a proposal has not yet been presented reflecting this idea, we will discuss in general terms the proposal that is currently relevant, to the best of our understanding.

3. 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. It is no

[1] The Clinic on Digital Rights and Human Rights in Cyberspace at the Hebrew University began to operate in the current academic year, in cooperation between the Cyber Law Program at the Cyber Security Research Center (H-CSRCL) and the Clinical Legal Education Center (CLEC) in the Faculty of Law at the Hebrew University of Jerusalem, and with partial funding from Google.

secret that cyberspace has brought new threats, and that the way to confront all these threats has not yet been found; this includes the dangers accruing from pornography. However, we believe that the bill raises several significant difficulties that have not been addressed by the model presented by MK Zohar. We believe that the damage caused to basic rights through the proposed arrangement exceeds the scope of protection it claims to provide, and accordingly it should not be advanced.

In this respect, we share the position presented to the Committee by the Ministry of Justice and the Ministry of Communications, as well as by several civil society organizations, regarding the serious damage to freedom of expression, freedom of information, and the right to privacy – all constitutional basic rights – caused by the proposal. It should also be emphasized, as explained in detail to the Committee members, that comparative law reviews on the subject did not find arrangements similar to that proposed in other democratic countries.

4. This damage is caused, among other reasons, due to the inherent technological limitations of this filter software to identify and define "offensive content;" the simple manner in which it is possible to circumvent these filtering services; and concern at a "slippery slope" regarding the state's involvement in access to information on the internet.

5. We will focus firstly on the technological limitations of the filter mechanisms, before proposing ways to optimize the arrangement already established in law, according to which ISPs are obliged to provide filtering software to customers who wish to use it. We shall detail this below:

Technological Difficulties

6. The bill does not address the manner of filtering or the manner of supervision of the filtering in order to ensure its quality. In technological terms, several methods exist for filtering information in internet traffic: information can be blocked according to its communications details, such as the blocking of the website's IP or URL address; and various possibilities exist for filtering by content, such as the blocking of words defined as offensive. Each of these methods has advantages and disadvantages. What they all share in common is that all of them ultimately lead to "under-filtering" – that is, it is possible to circumvent the filtering mechanism, so that users are exposed to content defined as offensive. More seriously, they all also lead to "over-blocking" -that is, completely legitimate content is blocked and users have no access to this legitimate content.

7. Over the years, examples have been published of canonical content that has been blocked by automatic filtering mechanism after being identified as pornographic content. Thus for example, the Pulitzer-prize winning photograph by photographer Nick Ut of Vietnamese children fleeing from a bombardment, taken in 1972, was automatically filtered by the automatic mechanism used by Facebook.[2] Another example is the masterpiece Liberty Leading the People.[3] Many such examples can be found. Other common errors by these filtering mechanisms relate both to content of considerable social value – information about STDs, breast cancer, breastfeeding, and information about single-sex couples. Thus, for example, a photograph of a family showing two mothers and their children on a bed was filtered.[4]

8. In addition to these examples, it is difficult to find reliable and detailed information about the effectiveness of this filtering software, and particularly regarding the filtering program the Committee intends to use. A study undertaken at the University of California – Berkeley in 2007[5] exposed significant gaps between the software programs according to the content examined in the study, as well as the limitations of this software. The study found that some filter mechanisms are "efficient," blocking over 90 percent of content defined as offensive and some 23 percent of content not defined as offensive. This undoubtedly constitutes a large proportion of the information held on the internet. This is without addressing the ways in which these filtering software programs define offensive material. As illustrated above, certain programs classify legitimate content, such as photographs of same-sex couples, as offensive. It should be noted that civil society organizations in Great Britain, where a voluntary filtering mechanism has been introduced by ISPs, raise an alarming phenomenon of the over-blocking of websites.[6] The blocking of information by ISPs is particularly disturbing, since internet users are not even aware what material has not been exposed to them, so that it is difficult to criticize or supervise this mechanism. Moreover, inverting the default position so that ISPs will provide a filtering service unless they have been requested otherwise creates

[2] See for example: https://gizmodo.com/facebook-admits-pulitzer-winning-photograph-is-not-chil-1786441732
[3] See for example: http://www.thelocal.fr/20180319/facebook-sorry-for-blocking-french-masterpiece-over-nudity
[4] See for example: https://gcn.ie/lesbian-family-photo-reported-blocked-instagram
[5] Philip B. Stark, The Effectiveness of Internet Content Filters, Department of Statistics, University of California, Berkeley. Available at https://www.stat.berkeley.edu/~stark/Preprints/filter07.pdf
[6] See for example: https://www.blocked.org.uk

an incentive to use filtering software that creates over-blocking in order to avoid legal exposure.

9. Secondly, alongside the danger of over-blocking as described above, the scope of protection provided by these filtering software programs against offenses on the internet is also very restricted. Many offenses in cyberspace, including exposure to pornographic content, occur in social networks or in various programs for the transmission of messages, which are not influenced by the filtering. Other offenses to which minors are exposed online, such as pedophilia, actually take place on dedicated websites for children. The bill provides no response to such offenses. It should be recalled that software or definitions exist permitting the easy circumvention of the proposed filtering mechanism, such as the use of a VPN. The use of such software is very simple, even for untrained users, but is liable to expose the users to additional online dangers to which they were not previously exposed without their knowledge, such as ransomware.

10. It can be assumed that as such filtering software is used extensively, the online behavior of users will change. Injurious websites that operate systematically will develop technological means to overcome the blockage, while websites blocked due to errors in the filtering software will not know how to do this. Moreover, innocent users who begin to use various software programs in order to circumvent filtering are liable to be exposed to dangers in cyberspace to which they were not previously exposed.

Exhausting the Current Arrangement

11. From the information presented to date to the Committee, it would seem that the arrangement that already exists in law, requiring ISPs to provide free a filtering service to their customers, has not been exhausted. Most online users are not even aware of the possibility to receive the filtering service, let alone of its advantages and disadvantages. Accordingly, we would suggest to the Committee members, in place of the proposal, to establish a neutral supervisory mechanism that will provide reliable and neutral information about the filtering software offered by the ISPs or on the free market and to enhance knowledge, awareness, and transparency regarding these services. Such a mechanism should routinely examine the quality of the filtering software programs that are used, and particularly their overblocking. Such a supervisory mechanism will enable each user to choose filtering software programs according to their own needs, suited to the profile of the online use they require. Without receiving objective and reliable information from a neutral source about the quality of the existing

filtering software, the decision regarding the installation of filtering software – both by the Committee members and by the various users – is unsubstantiated, and its effectiveness is highly doubtful. We would also suggest to the Committee members that a team of experts be established to formulate an action plan for responsible internet use, since the dangers that lurk online for minors are not confined to exposure to offensive material, and the bill offers no response to these dangers.

Conclusion

12. In light of the above, while we identify with the motivation underlying the bill – to defend minors surfing the internet – we believe that the balance in the arrangement proposed in the bill leads to a situation where the proposal's damage to basic rights exceeds its advantages. In place of the proposed arrangement, we suggest the establishment of a neutral supervisory mechanism to raise awareness of the options for filtering software and provide reliable information about their effectiveness.

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.