NGO Submission to
115th Session of the Human Rights Committee
for
Fourth Periodic Report of the Republic of Korea

Open Net Korea

21 September 2015

Introduction

Open Net is a Korean civil society organization established in 2012 to advocate for digital rights and Internet freedom with the goal of making the Internet a platform for openness, freedom and sharing. Korea, with the highest broadband penetration rate in the world, has always threatened to regulate the Internet in the most comprehensive manner as well. Open Net is aspiring to become not only a legal and legislative advocacy organization that fights the regulations but also a think tank that inquires into the reasons for these regulations and "thinks aloud" with the Korean public and the world on what has caused and what will prevent the Internet from becoming a "closed" circuit for some group of people, instead of "open network."

Contact Details:

Open Net

Kyung Sin Park, Director

Kha Yeun Kim, General Counsel

Email: kkim@opennet.or.kr

Tel: +82-2-581-1643

Address: 402, 62-9 Seocho-daero 50-gil, Seocho-gu, Seoul, 06650, Korea

Mandatory Implementation of Filtering Application on Minors' Mobile Phones

This submission specifically concerns a recent mandate by the Korean government which forces minors' mobile phones to be monitored by private parties, which is clearly in violation of ICCPR art. 17 right to privacy and family life. Issue 20(d) of the CCPR/C/KOR/Q/4 deals with the operation of a program that enables teachers to control students' mobile phones, and the concerned mandate requires de facto *a similar program to be installed on minors' mobile phones so that their legal guardians can monitor and control the phones. This issue could not have been raised earlier because the mandate came into force in April this year.*

I. Background

In April 16, 2015, amendments to the Telecommunications Business Act (TBA) and its Enforcement Decree came into effect which made it mandatory for South Korean telecommunications business operators to provide the means to block harmful contents on minors' mobile phones. The mandate was initially proposed by the Korea Communications Commission (KCC), when the government of the Republic of Korea has been seeking to mandate a filtering application for mobile devices used by minors for some time. The grand plan "Measures to Protect Juveniles from Obscenity" to tackle increasing minors' access to obscenity online was announced by the President Office and relevant ministries in March 2012.[1]

Article 32-7 of the TBA states that telecoms must provide means to block harmful or obscene contents when selling mobile phones to juveniles,[2] and prescribes any necessary matters to be specified in the Enforcement Decree.[3]

> **Telecommunications Business Act Article 32-7 (Blocking of Media Products Harmful to Juveniles)**
>
> (1) Any telecommunication business operator using allocated frequencies under the Radio Waves Act must provide the means to block the media products harmful to juveniles under Article 2 Subparagraph 3 of the

[1] "Mandating Obscenity Filtering Software for Juveniles," *Yonhap News*, March 16, 2012, http://news.naver.com/main/read.nhn?mode=LSD&mid=sec&sid1=100&oid=001&aid=0005557080 [in Korean]

[2] "Juveniles" are defined as persons under the age of nineteen, Juvenile Protection Act, Art. 2(1), http://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EC%B2%AD%EC%86%8C%EB%85%84%20%EB%B3%B4%ED%98%B8%EB%B2%95 [in Korean].

[3] Telecommunications Business Act, Art. 32-7, http://www.law.go.kr/lsInfoP.do?lsiSeq=167386&vSct=%EC%A0%84%EA%B8%B0%ED%86%B5%EC%8B%A0%EC%82%AC%EC%97%85%EB%B2%95#0000 [in Korean].

Juvenile Protection Act and the obscene information under Article 44-7(1)1 of the *Act on Promotion of Information and Communications Network Utilization and Information Protection, Etc.* when entering into a contract on telecommunications service with a juvenile under the *Juvenile Protection Act*.

(2) The Korea Communications Commission may inspect the practice of providing blocking means under (1).

(3) Necessary matters such as methods and procedures in providing the blocking means under (1) shall be prescribed by Presidential Decree.

Article 37-8 of the Enforcement Decree, in accordance with Art. 37-2(3) of the TBA, sets out the procedure in more detail. The telecoms must inform juveniles and their legal representatives (normally the parents) about the blocking means, and check the installation of chosen means. However, the Decree does not stop here but further obligates telecoms to notify the legal representatives if the means was deleted or disabled.

Enforcement Decree of the Telecommunications Business Act Article 37-8 (Methods and Procedures for Providing Means to Block Media Products Harmful to Juveniles, etc.)

(1) According to Article 32-7(1) of the Act, a telecommunication business operator entering into a contract on telecommunications service with a juvenile under the *Juvenile Protection Act* must provide means to block the juvenile's access to the media products harmful to juveniles under the *Juvenile Protection Act* and the illegal obscene information under Article 44-7(1)1 of the *Act on Promotion of Information and Communications Network Utilization and Information Protection, Etc.* ("Information harmful to juveniles") through the telecommunication service on the juvenile's mobile communications device such as a software blocking information harmful to juveniles.

(2) Procedures prescribed below must be followed when providing the blocking means under (1):

1. At the point of signing the contract:
    a. Notification to the juvenile and his/her legal representative regarding types, features, etc. of the blocking means; and
    b. Check on the installation of the blocking means.
2. After closing the contract: Monthly notification to the legal representative if the blocking means was deleted or had not been operated for more than 15 days.

According to the Citizen Lab at Munk School of Global Affairs, University of Toronto, "[w]hile the possibility of limiting or monitoring minors' mobile phone communications is encouraged in some jurisdictions, and many commercial products are available, South Korea has gone the furthest among all countries by mandating the installation of digital content blocking applications for minors."[4]

What is problematic, the regulation added the requirement of notifying parents in event that the blocking applications are not in proper operation, and what is even more, the government chose to recommend and promote to the industry as a legal requisite an application *Smart Sheriff* which has several remote control and monitoring features.

[4] Citizen Lab, "Are the Kids Alright? Digital Risks to Minors from South Korea's Smart Sheriff Application," September 20, 2015, https://citizenlab.org/2015/09/digital-risks-south-korea-smart-sheriff/

Since the laws came into effect in April 2015, according to the KCC, approximately 250,000 juveniles subscribed to new smartphone plans in the first two months, and about 200 parents wanted to opt out of the legal requirement.[5] However, the opt-out option is not provided under the law, and while the Enforcement Decree requires monthly notification if the application is not installed, it is yet unclear how the KCC is going to deal with noncompliance. And although the regulatory requirement applied only to new devices being purchased, schools sent letters home with children encouraging their parents to install a monitoring application.[6]

With cooperation on implementation from numerous entities in the public and private sector, the new requirements to filter harmful contents on mobile phones became a pervasive parental monitoring and control mandate. Most filtering applications promoted as the blocking means required under the mandate provide extensive parental monitoring and control features, including *Smart Sheriff*, the one developed under the KCC's support.[7]

II. Violation of the ICCPR Article 17 Right to Privacy and Family Life

Article 17 of the ICCPR states, "no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation." The mandate discussed above is clearly in violation of art. 17, interfering with children's privacy and the parents' family life.

According to the Enforcement Decree, at the point of signing the contract, the telecoms must notify both the juvenile and the legal representative about choices of applications they have and install the app of their choosing. Here is the first serious infringement on parental rights or interference with family as the law does not allow the parents to opt-out, thereby depriving the parents from a chance to make an informed decision on whether to accept such filtering or monitoring apps for their children. The law just assumes or forces consent of the parents, although there must be conscious parents who do not approve of such applications for privacy reasons or technical concerns.

Then the law further compels the telecoms to monitor the phones to ensure that the app is always active. This is a grave invasion on the children's privacy, because it allows private parties to collect excessive information about the juveniles that are not required to meet the purpose of the law – to filter harmful contents online. Moreover, the parents will be notified or spammed nonetheless even if they gave consent to their children for deleting the app. This certainly constitutes interference with family life.

Additionally, *Smart Sheriff* and other similar software enable various monitoring and controlling on the use of the smartphone. In the process, the software accumulates information such as the length of Internet usage, the websites visited, and contents of social media that's been received and sent. This is aggravated by the mobile phone real name law – In the Republic of Korea, all phone

[5] See http://news.bbsi.co.kr/news/articleView.html?idxno=694505 [in Korean].

[6] "Apps that Monitor Kids' Smartphone Use Popular in South Korea," *CBC News*, May 15, 2015, http://www.cbc.ca/news/technology/apps-that-monitor-kids-smartphone-use-popular-in-south-korea-1.3076349.

[7] See http://wiseuser.go.kr/jsp/commList.do?bcode=515&hcode=515&vcode=2565 [in Korean].

numbers are personally identifiable as telecommunication subscription is only allowed on a real name basis.[8] All the information collected will eventually allow a complete profiling of an identified juvenile's online activities, and the juvenile's privacy online will vanish. Moreover, such profiling of our children can be easily exploited by a malicious party.

Furthermore, *Smart Sheriff* and these software carry very serious privacy and security risks whereby cyber-attackers with reasonable levels of time and resources can delete or change the information on the juveniles' phones, monitor the juveniles' online activities, and possibly impersonate others in contacting the juveniles.[9] These security risks, though not caused directly by the government actions, originated from the government mandate of requiring certain software to be installed and be in operation continuously in someone's personal communication devices, which in turn necessitated constant monitoring software. It is uncertain whether the benefit of barring juveniles from viewing adult material justifies the cost of implanting such a comprehensive monitoring and control app in the juveniles' personal communication devices, which engender a horrifying list of risks that requires special constant attention from the technical communities and all other stakeholders involved.

III. Suggested Recommendations

1. The Government of the Republic of Korea should immediately stop enforcing the mandate and provide a reasonable guideline to minimize the privacy and security risks on Korean juveniles.

2. The Government of the Republic of Korea should take steps to repeal or amend Article 32-7 of the Telecommunications Business Act and Article 37-8 of its Enforcement Decree.

[8] TBA, Article 32-4, http://www.law.go.kr/lsInfoP.do?lsiSeq=167386&vSct=%EC%A0%84%EA%B8%B0%ED%86%B5%EC%8B%A0%EC%82%AC%EC%97%85%EB%B2%95#0000 [in Korean]

[9] Citizen Lab, "Are the Kids Alright? Digital Risks to Minors from South Korea's Smart Sheriff Application," September 20, 2015, https://citizenlab.org/2015/09/digital-risks-south-korea-smart-sheriff/