

Smart Sheriff Case

Kelly Kim

General Counsel

Open Net

Opennet.or.kr / OpennetKorea.org

Enforcement Decree of the TBA

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 ICNA (“Information harmful to juveniles”) through the telecommunication service on the juvenile’s mobile communications device such as a software blocking information harmful to juveniles.

Enforcement Decree of the TBA

Article 37–8 (Methods and Procedures for Providing Means to Block Media Products Harmful to Juveniles, etc.)

(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 and features 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.

Smart Sheriff by MOIBA and KCC



Open Net's Efforts



Smartphone Sheriff app in South Korea

15 June 2015 Last updated at 01:09 BST

Many parents would like to know exactly what their children are up to, especially when they are online.

오픈넷 포럼

청소년 스마트폰 필터링, 어디까지 차단해봤니?

-개정 전기통신사업법 시행령에 대한 입법적 보완책을 중심으로

일시: 2015.06.22(월) 19:30 ~ 21:30
장소: 스타트업 얼라이언스
주최: 사단법인 오픈넷

발제 1. 개정 전기통신사업법 시행령의 헌법적 검토 및 입법적 보완필요성
박지환 (사)오픈넷 변호사

발제 2. 청소년 스마트폰 필터링 수단의 기술적 검토
이준행 커뮤니티 일간위스트 개발자

토론
한상희 건국대학교 법학전문대학원 교수
최선경 방송통신위원회 인터넷윤리팀장
서희석 부산대학교 법학전문대학원 교수

문의: 오픈넷 사무국 02-581-1643, master@opennet.or.kr

Citizen Lab's Report on Smart Sheriff



Are the Kids Alright?

DIGITAL RISKS TO MINORS FROM SOUTH KOREA'S
SMART SHERIFF APPLICATION

20 September 2015

Collin Anderson (independent researcher), Masashi Crete-Nishihata (Citizen Lab), Chris Dehghanpoor (Lookout Inc.), Ronald J. Deibert (Citizen Lab), Sarah McKune (Citizen Lab), Davi Ottenheimer (flyingpenguin), and John Scott-Railton (Citizen Lab)

Citizen Lab's Report on Smart Sheriff

Responsible Disclosure

On 3 August 2015, Citizen Lab notified MOIBA of the issues identified in the two security audits. Following established standards for vulnerability disclosure, we set a publication deadline for a minimum of 45 days after our initial disclosure of vulnerabilities to the vendor.⁴

On 5 August a MOIBA representative replied and provided an initial timeline for addressing fifteen of the vulnerabilities. On 6 August MOIBA released an updated version of the application (v1.7.6) that supported HTTPS.⁵ An additional update (v1.7.7) released on 25 August claimed to address additional vulnerabilities.⁶

According to the most recent timeline provided to the Citizen Lab by MOIBA on 20 September 2015, patches should be in place for twenty of the issues identified, with sixteen published. Two further patches are scheduled shortly after the publication of this report. However, we have not fully verified whether all patches have been implemented, and MOIBA has not fully apprised us of the manner in which the vulnerabilities were addressed. We urge caution against further public use and promotion of the application until an independent and thorough audit of Smart Sheriff can be conducted.

On 4 September MOIBA was notified of this report's intended publication date and was sent a copy for review to ensure that no personally identifying information was inadvertently disclosed. As of the date of publication, we have not received any further correspondence from MOIBA.

Thank you!

8kkim8@gmail.com