UNIVERSITY OF TORONTO

MUNK SCHOOL OF GLOBAL AFFAIRS

Join the Global Conversation

Appendix B: Legal and Policy Issues

Are the Kids Alright? Digital Risks to Minors from South Korea's Smart Sheriff Application

Document Version 1.0
20 September 2015

Legal and Policy Issues

Background

South Korea is one of the most highly connected countries in the world when it comes to mobile phone and Internet access.[1] The relatively small size of the country and high level of economic development have resulted in support and demand for enhanced services such as next-generation connectivity.[2] According to the International Telecommunication Union, 98 percent of South Korean households have Internet access. The number of active mobile phones in the country — 57.2 million — exceeds the total population so the country has a mobile penetration rate of 116 percent.[3] In 2013, a reported 73 percent of the nation's mobile phone subscribers relied on smartphones.[4]

These high levels of adoption apply to almost every segment of the population, including minors. Whereas 36.2 percent of Korean minors had smartphones in 2011, according to government data the number grew to 81.5 percent within two years, with high penetration rates even among elementary school children.[5] A 2014 ITU report found that 99.6 percent of Korean teenagers were born and grew up in a digital environment — the highest figure of any country studied.[6]

The South Korean government has taken steps to control for the negative impacts associated with this rapid growth in connectivity, with particular emphasis on regulating the consumption of digital media among minors. Regulations control not only for illicit content but also for social

---

[1] "ICT Development Index: Korean Youth Rank Top in Digital Native Level," *Business Korea*, October 22, 2014, http://www.businesskorea.co.kr/article/6907/ict-development-index-korean-youth-rank-top-digital-native-level.

[2] Calum Dewar, "4G Driving Data Usage but Not All Markets Reaping the Rewards," GSMA Intelligence, January 20, 2014, https://gsmaintelligence.com/research/2014/01/4g-driving-data-usage-but-not-all-markets-reaping-the-rewards/412/; see also "4G Deployments and Connections Gather Pace," https://gsmaintelligence.com/research/2015/02/4g-deployments-and-connections-gather-pace/476/.

[3] Mobile-cellular Telephone Subscriptions, http://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2015/Mobile_cellular_2000-2014.xls.

[4] Smartphone Penetration (chart), https://think.withgoogle.com/mobileplanet/en/graph/?country=kr&category=DETAILS&topic=Q00&stat=Q00_1&wave=2013&age=all&gender=all&chart_type=&active=age. According to the Korea Communications Commission 2013 annual report, there were 37.52 million smartphone subscribers at the end of 2013 (68.6 percent of all mobile subscribers). See p. 21, http://eng.kcc.go.kr/user.do?mode=view&page=E02020000&dc=E02020000&boardId=1053&cp=1&boardSeq=38653.

[5] Smart Sheriff guidebook by KCC and MOIBA, http://ss.moiba.or.kr/downloadForm.do. See also http://www.yonhapnews.co.kr/society/2014/03/04/0712000000AKR20140304064800005.HTML [in Korean].

[6] "ICT Development Index: Korean Youth Rank Top in Digital Native Level," *Business Korea*, October 22, 2014, http://www.businesskorea.co.kr/article/6907/ict-development-index-korean-youth-rank-top-digital-native-level.

behaviour and address concerns of unhealthy usage patterns among minors.[7] Infamously, South Korea maintains a "shutdown" rule that restricts access to online gaming for minors under the age of sixteen after midnight.[8] In 2013, in response to the rapid rise in smartphone adoption among minors, regulators began focusing on combatting excessive smartphone use. The result was a host of requirements that schools organize "boot camps" where no Internet usage is allowed, teach classes on Internet addiction, and educate those as young as three on how to prevent overuse of digital devices and the Internet.[9]

Technology's potential to assist in curbing undesirable smartphone usage among minors has received significant attention in South Korea. A number of applications are currently available to block content deemed harmful to minors and/or provide parental monitoring functionality,[10] including Smart Sheriff, which was first introduced in 2012.[11] By 2014, schools were piloting a program that required students, with parental approval, to download an application that allowed teachers to remotely track and control students' smartphones, including the ability to lock the phone or allow only emergency calls.[12] This practice was included on the list of issues for assessment during the UN Human Rights Committee's review of South Korea's compliance with the *International Covenant on Civil and Political Rights* in October 2015.[13]

In April 2015, building on existing information controls, the government enacted a new measure requiring telecommunications business operators that enter into service contracts with minors to provide a means of blocking harmful content on the minor's mobile device and ensure that parents receive notifications whenever the blocking means becomes inoperative. This measure has ushered in the wide-ranging use of parental monitoring software in South Korea, with Smart Sheriff one of the most prominent options for fulfilling the mandate. However, in addition to the software's technical shortcomings (see technical appendix), the mandate and its implementation raise significant legal and policy questions that the following analysis explores.

---

[7] See, for example, Geoffrey Cain, "South Korea Worried About Smartphone Addiction," *The Star*, April 14, 2014, https://www.thestar.com/news/world/2014/04/14/south_korea_worried_about_smartphone_addiction.html.

[8] Juvenile Protection Act, art. 26, 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].

[9] "Ultra-wired South Korea Battles Smartphone Addiction," *Daily News*, July 1, 2013, http://www.nydailynews.com/life-style/health/south-korea-battles-smartphone-addiction-article-1.1387062; Youkyung Lee, "South Korea: 160,000 Kids Between Age Five and Nine Are Internet-Addicted," *Huffington Post*, January 27, 2013, http://www.huffingtonpost.com/2012/11/28/south-korea-internet-addicted_n_2202371.html.

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

[11] See https://ss.moiba.or.kr/customer/bbs/list.do; http://www.mogaha.go.kr/frt/bbs/type010/commonSelectBoardArticle.do?bbsId=BBSMSTR_000000000008&nttId=29036 [both pages in Korean].

[12] The app was iSmartKeeper (https://play.google.com/store/apps/details?id=com.netcube.smartkeeper.child&hl=ko). See Karissa Bell, "South Korean Schools Use App to Control Student Smartphone Use," Mashable, March 20, 2014, http://mashable.com/2014/03/20/south-korean-schools/.

[13] Par. 20, http://www.un.org/Docs/journal/asp/ws.asp?m=CCPR/C/KOR/Q/4.

South Korean Information Controls Affecting Minors' Digital Media Consumption

Legal and Regulatory Framework[14]

The primary basis for regulating online information and related measures in South Korea is the *Act on Promotion of Information and Communications Network Utilization and Information Protection, Etc.* (ICNA).[15] The ICNA's self-described purpose is to "contribute to the improvement of citizens' lives and the enhancement of public welfare" by, among other things, "protecting personal information of people using information and communications services, and developing an environment in which people can utilize information and communications networks in a sounder and safer way."[16] It provides the foundation for government-mandated Internet filtering: article 44-7 enumerates prohibitions against the "circulation of unlawful information," which notably includes certain content designated as "harmful to juveniles" under South Korea's *Juvenile Protection Act* and offered for profit, as well as content deemed to be obscenity, defamation, stalking, gambling, in breach of national security, and information aiding criminal behaviour.[17]

The *Juvenile Protection Act*, which defines "juveniles" as persons under the age of nineteen,[18] calls on the government to "formulate and implement policies necessary to clean up environments harmful to juveniles in order to protect juveniles."[19] Such environments encompass "media products harmful to juveniles,"[20] including designated "code, words, sound, or visual information transmitted through a telecommunications system."[21]

The governmental regulator overseeing many of the information controls under ICNA is the Korea Communications Commission ("KCC"). The KCC was established pursuant to the *Act on the Establishment and Operation of Korea Communications Commission* in 2008,[22] combining

---

[14] Throughout this appendix, citations to law include links to original Korean-language sources. English readers may refer to the website http://elaw.klri.re.kr/ for the English translations of these laws; however, the English-language materials may not reflect the most current versions of the laws.

[15] Act on Promotion of Information and Communications Network Utilization and Information Protection, Etc. (ICNA), http://www.law.go.kr/lsInfoP.do?lsiSeq=167388&ancYd=20150120&efYd=20150421&ancNo=13014#0000 [in Korean].

[16] Ibid., art. 1.

[17] Ibid., art. 44-7.

[18] 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].

[19] Ibid., art. (5)(1).

[20] Ibid., art. 2(8). "Media product[s] harmful to juveniles" are in turn defined in article 2(3) as "any of the following media products: (a) Media products determined or identified by the Commission on Youth Protection as harmful to juveniles and publicly notified accordingly by the Minister of Gender Equality and Family under the main sentence of Article 7(1) and Article 11; (b) Media products determined or identified by the competent examining authority as harmful to juveniles and publicly notified accordingly by the Minister of Gender Equality and Family under the proviso to Article 7(1) and Article 11."

[21] Ibid., art. 2(2)(e).

[22] Act on the Establishment and Operation of Korea Communications Commission, http://www.law.go.kr/lsInfoP.do?lsiSeq=168067&ancYd=20150203&efYd=20150203&ancNo=13202#0000 [in Korean].

the Korean Broadcasting Commission and the Ministry of Information and Communication. The KCC is administered by five standing commissioners who set and enforce national regulations on communications.[23] It has the authority under ICNA article 44-7 to order Internet service providers to reject, suspend, or restrict (i.e., remove or block) unlawful information. Anyone who fails to follow such orders will be punished by a maximum of two years' imprisonment or a fine of maximum KRW 20 million (just under $17,000 USD).[24] The ICNA also tasks the KCC with the "development and dissemination of technology for protection of juvenile[s]," and "development and dissemination of content-screening software" for content deemed inappropriate for juveniles that is circulated through information and communication networks.[25] ICNA notes that, to fulfill these tasks, the KCC may "support activities conducted by … organizations of providers or users of information and communications services."[26]

Additionally, the *Act on the Establishment and Operation of KCC* established another authority, the Korea Communications Standards Commission ("KCSC"), for "the purposes of guaranteeing the public nature and fairness of broadcasting contents, creating a sound culture in the areas of information and communications and creating an environment where information and communications are used in an appropriate manner."[27] The KCSC deliberates on matters regarding unlawful information under article 44-7(1) of the ICNA and also on matters "as necessary for nurturing sound communications ethics."[28] Although the KCC has the power to order the removal of unlawful information under article 44-7 of the ICNA, after the KCSC's review of the information, this is rarely executed because the KCSC has a broader standard and procedure that empowers it to censor any information that infringes on "sound communications ethics." The results of KCSC deliberation under that standard are enforced through what are called "corrective requests," which are issued directly to web hosts for content removal and to ISPs for site blocking without going through the KCC. The requests are typically followed.[29] This online information control and censorship regime operated through the KCSC is not subject to judicial review. In practice, restrictions on content are pervasive, with 23,000 Korean web pages deleted and 63,000 sites blocked in 2013, ranging from pornography to North Korean propaganda.[30]

---

[23] Ibid.; Korea Communications Commission, "About KCC," http://eng.kcc.go.kr/user.do?page=E01020100&dc=E01020100.
[24] ICNA, art. 73(5), http://www.law.go.kr/lsInfoP.do?lsiSeq=167388&ancYd=20150120&efYd=20150421&ancNo=13014#0000 [in Korean].
[25] Ibid., art. 41.
[26] Ibid., art. 41(2).
[27] Act on the Establishment and Operation of KCC, art. 18, http://www.law.go.kr/lsInfoP.do?lsiSeq=168067&ancYd=20150203&efYd=20150203&ancNo=13202#0000.
[28] Ibid., art. 21(3),(4).
[29] See Kyung-Sin Park, "Administrative Internet Censorship by KCSC," Open Net Korea, http://opennetkorea.org/en/wp/administrative-censorship; see also Korea Communications Standards Commission, "Report Process," https://www.kocsc.or.kr/eng/report02.php.
[30] "Why South Korea Is Really an Internet Dinosaur," *The Economist*, February 10, 2014, http://www.economist.com/blogs/economist-explains/2014/02/economist-explains-3.

Finally, telecommunications services in South Korea are subject to the *Telecommunications Business Act* (TBA),[31] which imposes licensing requirements, limits foreign ownership, and places operational mandates on service providers.[32] The KCC is responsible for enforcing TBA provisions on consumer rights.[33]

Mandate on Providing Means to Block Harmful Media Products on Juveniles' Mobile Devices

The Korean government has for some time sought to mandate a filtering application for minors' smartphones. On March 16, 2012, the government announced the "Measures to Protect Juveniles from Obscenity," which consisted of ten agendas. Regarding smart devices including smartphones, the government, together with telecoms and a relevant association, was to develop and distribute an obscenity-filtering program.[34] The government also planned to include notification of obscenity-blocking means in the "Green Contract," a mobile plan subscription contract for juveniles.[35] Three months later, the government announced that Smart Sheriff would be distributed freely by the KCC from June 8, 2012,[36] and in October 2012 additionally announced that it planned to amend the TBA to make blocking means mandatory.[37]

In October 2014, the Korean government amended the TBA to include article 32-7, a provision requiring telecommunication businesses to provide the means to block media products harmful to juveniles "when entering into a contract on telecommunications service with a juvenile."[38] According to this amendment, the KCC is authorized to "inspect the practice of providing blocking means."[39]

Telecommunications Business Act Article 32-7 (Blocking of Media Products Harmful to Juveniles)

[31] Telecommunications Business Act, 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].
[32] Kwang Bae Park, "Change of Telecom Regulatory Policy of Korea Upon the Recent Development of Telecom Technology," World Services Group, September 2007, http://www.worldservicesgroup.com/publications.asp?action=article&artid=2098.
[33] Telecommunications Business Act, arts. 50–53, http://www.law.go.kr/lsInfoP.do?lsiSeq=142966&urlMode=engLsInfoR&viewCls=engLsInfoR#0000.
[34] See http://www.mogaha.go.kr/frt/bbs/type010/commonSelectBoardArticle.do?bbsId=BBSMSTR_000000000008&nttId=28838 [in Korean]. In light of subsequent events it is likely that the organization referred to was MOIBA.
[35] Ibid.
[36] See http://www.mogaha.go.kr/frt/bbs/type010/commonSelectBoardArticle.do?bbsId=BBSMSTR_000000000008&nttId=29036 [in Korean].
[37] See http://www.evaluation.go.kr/pmo/news/news01.jsp?mode=view&article_no=41639&board_wrapper=%2Fpmo%2Fnews%2Fnews01.jsp&pager.offset=40&board_no=3&defparam:year=2012 [in Korean].
[38] Telecommunications Business Act, art. 32-7(1), 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.
[39] Ibid, art. 32-7(2).

(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 Juvenile Protection Act and the obscene information under Article 44-7(1)1 of the ICNA 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.

This amendment was first proposed in June 2012 by ten members of the National Assembly.[40] The proposed amendment specifically required telecommunication business operators to verify whether a blocking mechanism had been installed when entering into contracts with juveniles, and to periodically inspect whether the blocking mechanism functioned correctly on juveniles' devices. It additionally provided that, should a blocking mechanism cease to function properly or if the functional status of a blocking mechanism was unclear, a telecommunication business operator must provide, in accordance with a Presidential Decree, a means to limit telecommunication services until a working blocking mechanism was reinstalled.[41]

The bill was accompanied by a review report submitted by a member of the National Assembly Science, ICT, Future Planning, and Telecommunications Committee.[42] The report expressed a concern for social problems arising from exposure of "defenseless juveniles" to obscene or violent web content and smartphone applications by foreign operators.[43] The report based its recommendations on the findings of the KCSC[44] that a total of 18,101 obscene or violent applications existed in 2011 on the Android open market, while only 212 of those applications required adult authentication. The report also explained that comprehensive regulation was

[40] See http://likms.assembly.go.kr/bill/jsp/BillDetail.jsp?bill_id=PRC_C1C2M0S6I2R2U1H8P0R7T1T7P7X4M8 [in Korean]. Two more bills were proposed by the members of the National Assembly in 2013, which were incorporated into the final bill passed in 2014 and discarded. See http://likms.assembly.go.kr/bill/jsp/BillDetail.jsp?bill_id=PRC_Y1W3B0J4D1W1F1Y5S3Q2N3V2S1K9J8 and http://likms.assembly.go.kr/bill/jsp/BillDetail.jsp?bill_id=PRC_J1D3V0N9Z0Q6M1Y7G4W6S0B8P6M6N1 [in Korean].

[41] Telecommunications Business Law Revision Bill, June 22, 2012, http://likms.assembly.go.kr/filegate/servlet/FileGate?bookId=C6F14054-42DC-CF71-9BE0-D48A575FB8B6&type=1 [in Korean].

[42] Telecommunications Business Law Revision Bill Review Report, June 22, 2012, http://likms.assembly.go.kr/filegate/servlet/FileGate?bookId=7CC8DA06-9043-EA2D-E294-7C82B5E3ED06&type=1 [in Korean].

[43] Ibid.

[44] Notably, it was the KCSC that initially recommended a mandatory filtering application, "Clean App," to prevent juveniles from accessing obscenity. KCSC stated that it planned "to recommend the National Assembly and KCC review the law to make Clean App mandatory" in 2011. See http://www.fnnews.com/news/201101111505585473?t=y [in Korean]. Although the bills on blocking means were proposed by members of the National Assembly, it is probable that KCC and KCSC lobbied for some time to make it happen.

necessary because the subjects and devices needing blocking mechanisms were not immediately clear.

The bill underwent several discussions and revisions before ultimately being adopted into law in 2014. However, the National Assembly Science, ICT, Future Planning, and Telecommunications Committee determined that provisions requiring telecommunications businesses to monitor individual smartphones would lead to an invasion of privacy, and that a provision requiring telecommunication business operators to stop service would be an excessive restriction.[45] Those provisions were removed in the final version of the law enacted in October 2014.

Once article 32-7 of the TBA went into effect, the KCC proposed an amendment to the Enforcement Decree of the TBA to require mobile operators to install an application that not only does what the TBA requires — block media products harmful to juveniles — but also notifies parents when such blocking mechanisms become inoperative.[46] The amendment was adopted by the government in April 2015 as article 37-8.[47] According to article 37-8 of the Enforcement Decree,[48] mobile telecommunication business operators must provide the ability to block contents designated as harmful under the *Juvenile Protection Act* and obscene under the ICNA, and engage in monthly notification to a minor's legal representative of any lapse in operation or deletion of the blocking means.

Telecommunications Business Act Enforcement Decree Article 37-8 (Methods and Procedures for Providing Means to Block Media Products Harmful to Juveniles, etc.)[49]

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.

[45] Science, ICT, Future Planning, and Telecommunications Committee Meeting Minutes, February 27, 2014 (PDF available at http://likms.assembly.go.kr/bill/jsp/BillDetail.jsp?bill_id=PRC_C1C2M0S6I2R2U1H8P0R7T1T7P7X4M8 [in Korean]).

[46] See http://www.kcc.go.kr/user.do?mode=view&page=A02030900&dc=K00000001&boardId=1101&boardSeq=40388 [in Korean].

[47] See http://www.lawmaking.go.kr/opnPtcp/govLm/2000000105230?edDtFmt=2015.+8.+20.&stDtFmt=2014.+1.+1.&lsNmKo=%EC%A0%84%EA%B8%B0%ED%86%B5%EC%8B%A0%EC%82%AC%EC%97%85%EB%B2%95&govLmStsScYn=Y [in Korean].

[48] Enforcement Decree of the Telecommunications Business Act, http://www.law.go.kr/lsInfoP.do?lsiSeq=173069&vSct=%EC%A0%84%EA%B8%B0%ED%86%B5%EC%8B%A0%EC%82%AC%EC%97%85%EB%B2%95%20%EC%8B%9C%ED%96%89%EB%A0%B9#0000 [in Korean].

[49] English translation from Kelly Kim, "Warning: Minor Smartphone Spying Law Now Comes into Force," Open Net Korea, April 15, 2015, http://opennetkorea.org/en/wp/1248#sthash.M0W2rVki.dpuf.

2. Procedures prescribed below must be followed when providing the blocking means under (1):
    a. At the point of signing the contract:
        i. Notification to the juvenile and his/her legal representative regarding types, features, etc. of the blocking means; and
        ii. Check on the installation of the blocking means.
3. 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.

This parental notification mandate came into effect on April 16, 2015. Mobile operators posted signs on the doors of their stores highlighting and enforcing the new requirement. 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.[50] Mobile operators also recommended that parents install the parental version of the applications on their own phones when installing the applications on their children's phones, so that parents could use the monitoring and remote control features provided.[51]

According to the KCC, approximately 250,000 juveniles subscribed to new smartphone plans in the two months since the law came into force, and only 200 parents wanted to opt out of the legal requirement. The KCC has stated that the law requires telecommunication business operators to merely install blocking mechanisms, and does not prevent parents from opting out of the blocking apps — the parents could ask the telecommunications business operators not to install the parental monitoring apps or send a written note with their child.[52] While article 37-8 of the Enforcement Decree requires monthly notification to guardians if the application is not installed, there is no clear sanction against the telecommunication service provider or the parent for noncompliance.[53] Rather, the KCC explained in its Impact Analysis of the Enforcement Decree that the monthly notification requirement was intended to discourage juveniles from deleting the apps. It also noted that although all available apps have deletion-proof features, juveniles are known to circumvent them by resetting, rooting, or jailbreaking phones.[54] Given these circumstances, it remains unclear how the requirements of the TBA and Enforcement Decree will ultimately be enforced.

With cooperation on implementation from numerous entities in the public and private sector, the new requirements constitute a pervasive parental monitoring and control mandate. Most entities complying with the legal mandate have done so through use of apps that provide extensive parental monitoring and control features, including the one that the KCC promoted: Smart

[50] "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.
[51] See http://www.civicnews.com/news/articleView.html?idxno=2031 [in Korean].
[52] See http://news.bbsi.co.kr/news/articleView.html?idxno=694505 [in Korean].
[53] Ibid.
[54] Korea Communications Commission, Regulation Impact Analysis of the Partial Amendment to the Enforcement Decree of the Telecommunications Business Act, 2015, p. 38, available at https://drive.google.com/file/d/0B479mpuIy1CeMTVmWExHTEZlczA/view?usp=sharing.

Sheriff. At present, sixteen products are offered to parents and companies attempting to comply with the new requirement, including applications developed by the mobile operators themselves and some at cost.[55] One month into the mandate, these applications were reportedly downloaded at least 480,000 times.[56] With 4.7 million Koreans between the ages of nine and seventeen, the target audience of the program, and a smartphone penetration rate in excess of 80 percent among this population, the monitoring applications' potential user base is in the millions, not including parents themselves installing the application to monitor their children's existing devices.[57]

Smart Sheriff's Role in Fulfilling the Regulatory Mandate

While Smart Sheriff is not the only tool offered to support compliance with the new regulations on provision of means to block harmful content, the Korean government appears to have uniquely supported its development and promotion for quite some time. Smart Sheriff was in development prior to the June 2012 proposals to amend the TBA. After a beta version of the app was released in April 2012, Smart Sheriff was officially launched for Android on June 1, 2012, with an iOS version created soon after.[58] The official developer of the application is the Korean Mobile Internet Business Association (MOIBA), an influential consortium of mobile telecommunication providers and phone manufacturers.[59] The KCC, however, has worked closely with MOIBA on Smart Sheriff, claiming credit for the application in its 2013 annual report:

> The Commission has developed and supplied software (Smart Sheriff) for Android smart phones and iPhone blocking harmful information in order to protect children and youth from illegal or harmful mobile information. The software also enables the control of reckless smart phone use by children or youth by providing functions for querying or blocking the access list of apps or Internet sites or limiting the number of access hours, in order to enable parents to control the smart phone use of their children. It has made it easier for parents to guide or control their children's use of smart phones using software that blocks harmful information.[60]

The KCC appears to have provided significant financial support for the app's development, reportedly spending KRW 980 million in 2013, KRW 1.2 billion in 2014, and KRW 1 billion in

---

[55] Most users complying with the law appear to select either Smart Sheriff or the apps provided by mobile operators SKTelecom and KT. See http://wiseuser.go.kr/jsp/commList.do?bcode=515&hcode=515&vcode=2565 [in Korean].
[56] "Prying Parents: Phone Monitoring Apps Flourish in South Korea," *Japan Times*, May 19, 2015, http://www.japantimes.co.jp/news/2015/05/19/asia-pacific/social-issues-asia-pacific/prying-parents-phone-monitoring-apps-flourish-s-korea/.
[57] Korean Statistical Information Service, Statistical Database, Population Projections, http://kosis.kr/eng/statisticsList/statisticsList_01List.jsp?vwcd=MT_ETITLE&parmTabId=M_01_01#SubCont; Smart Sheriff guidebook by KCC and MOIBA, http://ss.moiba.or.kr/downloadForm.do [in Korean].
[58] See https://ss.moiba.or.kr/customer/bbs/list.do [in Korean].
[59] See www.moiba.or.kr [in Korean].
[60] Korea Communications Commission, 2013 Annual Report, p. 109, http://eng.kcc.go.kr/user.do?mode=view&page=E02020000&dc=E02020000&boardId=1053&cp=1&boardSeq=38653.

2015 (totaling KRW 3.18 billion, approximately USD 2.7 million) on a project involving Smart Sheriff and an additional application (S-Dream).[61]

The KCC was also heavily involved in piloting and promoting the application. In 2012 the government announced that Smart Sheriff would be distributed freely by KCC from June 8 of that year.[62] In 2013, together with MOIBA and other agencies, the KCC "supplied Smart Sheriff to forty-one elementary and junior high schools in Gyeonggi Province"[63] as part of efforts to create a "Secure Cyber Zone," and announced that it was responsible for improving the functionality and advancing the capabilities of Smart Sheriff as a part of that holistic effort.[64] It engaged in additional promotional activities as well:

> The Commission published Helping My Child to Use a Smart Phone Safety [*sic*] and Correctly, a guidebook on the use of software (Smart Sheriff) designed to block illegal or harmful information and to prevent addiction, and distributed it to schools, Internet addiction response centers, regional Will Centers, education boards, and regional resident centers in a drive to encourage them to use it. The Commission staged diverse promotional activities aimed at informing the general public about the guidebook more widely by publicizing it through portals, blogs, cafés, intellectual circles and online news articles that are easily accessed for information, and highly popular radio CMs (four broadcasting programs, including 'FM March with Hwang, Jeong-min').[65]

Indeed, the 2012 announcement video for Smart Sheriff includes the KCC, Ministry of Government Administration and Home Affairs (MOGAHA), and Korea's three major mobile providers as MOIBA's launch partners.[66]

---

[61] See http://www.sisainlive.com/news/articleView.html?idxno=23878 [in Korean].
[62] See http://www.mogaha.go.kr/frt/bbs/type010/commonSelectBoardArticle.do?bbsId=BBSMSTR_000000000008&nttId=29036 [in Korean].
[63] Korea Communications Commission, 2013 Annual Report, p. 110, http://eng.kcc.go.kr/user.do?mode=view&page=E02020000&dc=E02020000&boardId=1053&cp=1&boardSeq=38653.
[64] See http://www.kcc.go.kr/user.do?mode=view&page=A05030000&dc=K05030000&boardId=1113&cp=1&boardSeq=36393 [in Korean].
[65] Korea Communications Commission, 2013 Annual Report, p. 111, http://eng.kcc.go.kr/user.do?mode=view&page=E02020000&dc=E02020000&boardId=1053&cp=1&boardSeq=38653.
[66] See https://www.youtube.com/watch?v=MVFwXWYjcN4 [in Korean].

Figure 1: Launch partners identified in the Smart Sheriff introduction, video still.

Source: https://www.youtube.com/watch?v=MVFwXWYjcN4 (July 22, 2012)

Smart Sheriff was thus not only marketed in relation to the new law[67] but also received publicity by virtue of MOIBA sponsorship and Korean government support.

MOIBA, in turn, appears to have outsourced the application's development rather than creating the software itself. The official contact information in mobile application stores and websites for Smart Sheriff is connected to employees and addresses associated with MOIBA. However, the package name, file copyrights, and program classes of the Android applications make recurrent references to "Cleanwave," "101GT," and "Wigsys." This information matches a membership entry for MOIBA for a company called "101GT," with a listed domain name of "wigsys.co.kr"

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

and a point of contact listed as "Choi Sihun."[68] Wig Systems Corp., a Seoul-based software development firm, was founded in 2009 as 101GT[69] and is a member of MOIBA. Wig Systems began developing a blocking system for harmful information for the association in 2011, and MOIBA has confirmed that third parties developed Smart Sheriff.[70] According to a previous announcement, Smart Sheriff was initially offered under the domain name "www.cleanwave.or.kr."[71] A similar site "101GT.co.kr" is registered and associated with school applications on various mobile application stores. However, these domains are offline, and both the domain names wigsys.co.kr and www.cleanwave.or.kr expired earlier this year.

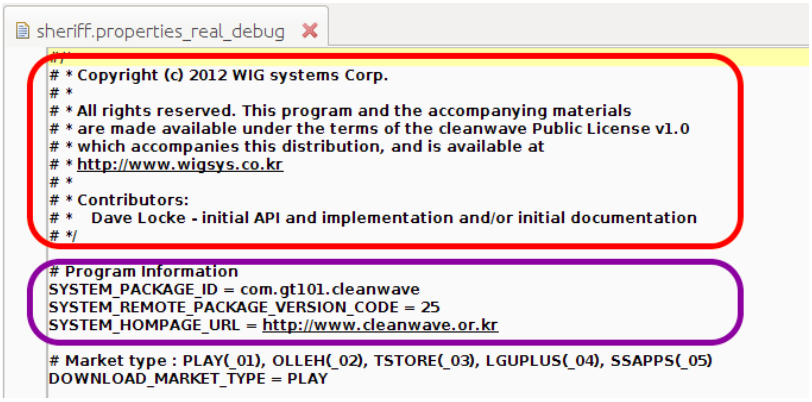

Figure 2: Copyright and authorship information from configuration files citing GT101/WIG Sys

Source: Smart Sheriff decompiled application package (v. 1.7.4)

Data Protection and Information Security Requirements

The numerous technical flaws discovered in the Smart Sheriff application (see the technical appendix) raise questions about whether the software is compliant with South Korean data protection and information security regulations, as well as with the representations made in the Smart Sheriff terms of service and privacy policy.

[68] "MOIBA Members — Membership Alliance Information of the Board of Directors and Major Membership Alliance who are acting under alliances," http://www.moiba.or.kr/eng/main.jsp?ect_code=31153111&shape=&page=6&keyword=&cTitle=.
[69] See http://www.saramin.co.kr/zf_user/recruit/company-info/idx/5138105 [in Korean].
[70] See http://www.jobkorea.co.kr/Recruit/Co_Read/C/uxwave?Oem_Code=C1 [in Korean].
[71] See notice dated April 30, 2012 on https://ss.moiba.or.kr/customer/bbs/list.do [in Korean].

Legal and Regulatory Framework

South Korea maintains some of the strongest legal protections for customer data in the world.[72] In 2011, the National Assembly passed the *Personal Information Protection Act* (PIPA), which enumerates principles for handling personally identifiable information by any "public institution, corporate body, organization, individual, etc."[73] PIPA defines personal information as "information that pertains to a living person, including the full name, resident registration number, images, etc., by which the individual in question can be identified, (including information by which the individual in question cannot be identified but can be identified through simple combination with other information)."[74]

PIPA put into place firm regulatory structures and policies to prevent "any harmful effect from collecting personal information for any purpose other than the intended purpose, misusing, abusing, or excessively monitoring and tracking, etc. personal information, thereby protecting human dignity and personal privacy."[75] The law enumerates responsibilities for personal information managers,[76] including requirements for obtaining consent on the collection of personal information, restrictions on the type of information that can be collected, and penalties for noncompliance.

PIPA also includes requirements for maintaining the technical security of the personal information collected by these entities. Article 29 mandates that a personal information manager must "take technical, administrative and physical measures necessary for securing safety, as prescribed by Presidential Decree, in order to prevent personal information from loss, theft, leakage, alteration or damage."

The safety measures required for personal information are enumerated in the subsequent Enforcement Decree:

1. To set up and implement the internal management plan for the safe processing of personal information;
2. To control access to personal information and restrict the authority to access hereto;
3. To adopt such encryption technology as to store and transmit the personal information in safety, and other measures equivalent hereto;
4. To retain log-in records in order to respond data breach incidents and to take measures to prevent the forgery and falsification hereof;

---

[72] See, for example, "South Korea: Amended PIPA Now in Force Combat Data Breaches," Data Guidance, August 7, 2014, http://www.dataguidance.com/dataguidance_privacy_this_week.asp?id=2697; and Graham Greenleaf and Whon-Il Park, "Korea's New Act: Asia's Toughest Data Privacy Law," Social Science Research Network, July 19, 2012, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2120983.

[73] Personal Information Protection Act (PIPA), art. 2(5), http://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EA%B0%9C%EC%9D%B8%EC%A0%95%EB%B3%B4%EB%B3%B4%ED%98%B8%EB%B2%95(10465) [in Korean].

[74] Ibid., art. 2(1).

[75] Ibid., art. 5(1).

[76] "The term 'personal information manager' means a public institution, corporate body, organization, individual, etc. who manages personal information directly or via another person to administer personal information files as part of his/her duties . . . ." Ibid., Art. 2(5).

5. To install and upgrade security programs to protect personal information;
6. To take such physical measures as storage to keep personal information in safety or locking system.[77]

PIPA also established the Personal Information Protection Committee (PIPC) under the direct jurisdiction of the president to monitor for PIPA violations and deliberate on other matters concerning the protection of personal information.[78] While no fines have been recommended by the PIPC, violations of certain PIPA provisions carry a potential penalty ranging from 10 to 30 million won (approximately USD 8,000–25,000) and a maximum of two years in prison.[79] If a representative, agent, or employee of a corporation commits a violation in connection with the business of that corporation, the corporation can also be fined if it is found to have "been negligent in giving due attention and supervision concerning the relevant duties to prevent such violation."[80]

[77] Enforcement Decree of PIPA, art. 30(1), http://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EA%B0%9C%EC%9D%B8%EC%A0%95%EB%B3%B4%EB%B3%B4%ED%98%B8%EB%B2%95%EC%8B%9C%ED%96%89%EB%A0%B9 (English translation at http://koreanlii.or.kr/w/images/d/d7/DPAct_EnforceDecree.pdf).

[78] PIPA, arts. 7-8, http://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EA%B0%9C%EC%9D%B8%EC%A0%95%EB%B3%B4%EB%B3%B4%ED%98%B8%EB%B2%95(10465) [in Korean]; see also "About the Commission," http://www.pipc.go.kr/cmt/english/introduction/chairman.do. PIPC's primary action to date was its assessment in 2012, in concert with the KCC, that the personal information collection performed by Google may be in violation of PIPA. See "Personal Information Protection Commission, Expressed Concern over Google's Violation of Personal Information Protection Policy," PIPC News and Topics, http://www.pipc.go.kr/cmt/english/news/selectBoardList.do?bbsId=BBSMSTR_000000000080; see also "KCC Considering Administrative Action against Google," *Business Korea*, January 17, 2014, http://www.businesskorea.co.kr/article/2991/kcc-and-privacy-kcc-considering-administrative-action-against-google.

[79] See PIPA, arts. 73(1) and 75(2)(6) [concerning penalties for breach of PIPA arts. 24(3) and 29], http://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EA%B0%9C%EC%9D%B8%EC%A0%95%EB%B3%B4%EB%B3%B4%ED%98%B8%EB%B2%95(10465) [in Korean].

[80] PIPA, art. 74(2), http://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EA%B0%9C%EC%9D%B8%EC%A0%95%EB%B3%B4%EB%B3%B4%ED%98%B8%EB%B2%95(10465) [in Korean].

For information and communications service providers,[81] the ICNA builds upon and supersedes the privacy requirements established in PIPA.[82] In addition to the regulation of digital content, the ICNA sets out requirements for the protection of personal data and networks, most notably in chapter IV on "Protection of Personal Information." Article 30 of that chapter describes the rights of users, including the user's right to revoke consent to a service provider "to collect, use, furnish, or dispose otherwise of his/her personal information," and to demand that the provider allow for the inspection and correction of information collected from that user.[83] Concerning the personal information of minors, article 31 mandates that the collection and use of personal information from a child less than fourteen years of age requires consent from the child's legal representative. That legal representative may exercise the same rights of inspection, correction, and revocation of consent laid out in article 30 "with respect to personal information of the relevant child."[84]

Additionally, ICNA article 28(1) lists the technical and administrative protective measures required for handling personal information, including encryption of that data:

1. Establishment and implementation of an internal control plan for handling personal information in a safe way;
2. Installation and operation of an access control device, such as a system for blocking intrusion to cut off illegal access to personal information;
3. Measures for preventing fabrication and alteration of access records;
4. Measures for security by using encryption technology and other methods for safe storage and transmission of personal information;

---

[81] ICNA defines "providers of information and communications services" as "the telecommunications business operators under subparagraph 8 of Article 2 of the Telecommunications Business Act and other persons who provide information or intermediate the provision of information for profit by utilizing services rendered by a telecommunications business operator." See ICNA, art. 2(1)(3), http://www.law.go.kr/lsInfoP.do?lsiSeq=167388&ancYd=20150120&efYd=20150421&ancNo=13014#0000 (English translation at http://elaw.klri.re.kr/kor_service/lawView.do?hseq=25446&lang=ENG). The TBA, in turn, defines "telecommunications business operator" as "an entity that provides telecommunications services upon obtaining a license, or completing registration or reporting (including cases of exemption from reporting) under this Act." See TBA, art. 2(8), 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 (English translation at http://elaw.klri.re.kr/kor_service/lawView.do?hseq=25944&lang=ENG). It is unclear whether an association such as MOIBA, which has provided free software to the public, falls within these definitions and is therefore subject to ICNA provisions. However, it is possible that Smart Sheriff constitutes a value-added telecommunications service triggering registration and reporting requirements, albeit with possible exemptions, under the TBA (see TBA, arts. 2(12), 22), which would render MOIBA a "telecommunications business operator" and therefore a "provider of information and communications services" under ICNA. Accordingly, we include discussion of the data protection provisions of ICNA that may be applicable to Smart Sheriff and MOIBA.

[82] ICNA, art. 5, http://www.law.go.kr/lsInfoP.do?lsiSeq=167388&ancYd=20150120&efYd=20150421&ancNo=13014#0000 [in Korean]; PIPA, art. 6, http://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EA%B0%9C%EC%9D%B8%EC%A0%95%EB%B3%B4%EB%B3%B4%ED%98%B8%EB%B2%95(10465) [in Korean].

[83] ICNA, art. 30, http://www.law.go.kr/lsInfoP.do?lsiSeq=167388&ancYd=20150120&efYd=20150421&ancNo=13014#0000 [in Korean].

[84] Ibid., art. 31.

5. Measures for preventing intrusion of computer viruses, including installation and operation of antivirus software;
6. Other protective measures necessary for securing safety of personal information.[85]

If personal information is lost, stolen, leaked, altered, or mutilated because the measures under this article 28 were not taken, the KCC may fine the service provider.[86] In cases where a user seeks compensation for damages as a result of an ICNA chapter IV violation, a service provider "may not be discharged from liability, unless it proves that there was no intentional act nor negligence on its part."[87]

The Enforcement Decree of ICNA was amended on November 28, 2014, and includes provisions on compliance with the ICNA chapter IV requirements.[88] According to the decree, to establish "measures for security by using encryption technology and other methods for safe storage and transmission of personal information" under ICNA article 28(1), service providers must ensure:

1. one-way encrypted storage of passwords;
2. encrypted storage of information notified by the KCC such as RRNs, account numbers, and bio-information (information regarding physical or behavioral characteristics such as fingerprints, iris, voice, handwriting, etc. by which an individual can be identified);
3. measures such as building a secure server when transmitting users' personal information and certification information through the information and communications network; and,
4. other security measures using encryption technology.[89]

The Enforcement Decree also mandates that the KCC publish guidelines on the minimum standard of protective measures required,[90] which the KCC has released as "Guidelines on Technical and Managerial Protective Measures for Personal Information."[91] Article 6 of the guidelines prescribes encryption measures required for personal information:

1. Service providers or similar shall store password by one-way encryption to prevent decryption.
2. Service providers or similar shall encrypt and store the following information by using safe encryption algorithm:
    a. Resident Registration Number
    b. Passport number
    c. Driver's license number
    d. Alien registration number
    e. Credit card number
    f. Account number
    g. Bio-information

---

[85] Ibid., art. 28(1) (English translation at http://elaw.klri.re.kr/kor_service/lawView.do?hseq=25446&lang=ENG).
[86] Ibid., art. 64-3(1)(6).
[87] Ibid., art. 32 (English translation at http://elaw.klri.re.kr/kor_service/lawView.do?hseq=25446&lang=ENG).
[88] Enforcement Decree of ICNA, http://www.law.go.kr/lsInfoP.do?lsiSeq=164340&vSct=%EC%A0%95%EB%B3%B4%ED%86%B5%EC%8B%A0%EB%A7%9D#0000 (available only in Korean).
[89] Ibid., art. 15(4).
[90] Ibid., art. 15(6).
[91] Guidelines on Technical and Managerial Protective Measures for Personal Information, http://www.law.go.kr/admRulLsInfoP.do?admRulSeq=2100000019404 (available only in Korean).

3. Service providers or similar shall encrypt users' personal information and certification information when transmitting them through the information and communications network by building a safe secure server, etc. The secure server must have one of the following features:
    a. Installation of SSL (Secure Socket Layer) certificate on the web server to encrypt information being transmitted
    b. Installation of an encryption application program on the web server to encrypt information being transmitted
4. Service providers or similar shall encrypt users' personal information when it is stored on PCs, mobile devices, sub-data storage devices, etc.[92]

The ICNA also established the Korea Internet and Security Agency (KISA).[93] The KISA is tasked with carrying out a variety of duties related to Internet connectivity, including "support for the protection of stored information of the Internet users,"[94] "support for development and proliferation of protection technology,"[95] and "public relations activities, education, and training for using and protecting the information and telecommunications network."[96] On its website, KISA states: "We are protecting the personal lives of citizens from damages of leakage, exposure and abuse of personal information. Illegally leaked, exposed personal information can be maliciously used for identity theft, voice phishing and illegal SPAM that can cause mental and financial damages."[97] KISA executes its personal information protection and information security mandates through specialized subdivisions of the agency, such as the Korea Internet Security Center, which has code analysis and security-risk monitoring teams available to small- and medium-sized businesses and nonprofits.[98]

Smart Sheriff Terms of Service and Privacy Policy

Smart Sheriff's terms of use, and its policies on privacy and information collection and usage,[99] are displayed to potential members upon registering for the Smart Sheriff application.[100] A

---

[92] Ibid., art. 6.
[93] ICNA, art. 52, http://www.law.go.kr/lsInfoP.do?lsiSeq=167388&ancYd=20150120&efYd=20150421&ancNo=13014#0000 [in Korean].
[94] Ibid., art. 52(3)(14) (English translation at http://elaw.klri.re.kr/kor_service/lawView.do?hseq=25446&lang=ENG).
[95] Ibid., art. 52(3)(8) (English translation at http://elaw.klri.re.kr/kor_service/lawView.do?hseq=25446&lang=ENG).

[96] Ibid., art. 52(3)(4) (English translation at http://elaw.klri.re.kr/kor_service/lawView.do?hseq=25446&lang=ENG); see also Yoon Sung-won, "Internet Agency to Offer Web Tech Guidelines," *Korea Times*, July 16, 2015, https://www.koreatimes.co.kr/www/news/tech/2015/07/133_182908.html.

[97] Korea Internet and Security Agency, "Internet Security: Protection of the Citizens' Personal Information," https://www.kisa.or.kr/eng/activities/internetsecurity.jsp#.
[98] Korea Internet Security Center, "Organization," http://eng.krcert.or.kr/krcert_cc/organization.jsp; Korea Internet Security Center, "Web Vulnerability Inspection Service," http://eng.krcert.or.kr/service/web.jsp.
[99] ICNA article 27-2 requires that service providers establish and disclose their policies for handling users' personal information, including matters related to the automated collection of personal information. See ICNA, art. 27-2, http://www.law.go.kr/lsInfoP.do?lsiSeq=167388&ancYd=20150120&efYd=20150421&ancNo=13014#0000 (English translation at http://elaw.klri.re.kr/kor_service/lawView.do?hseq=25446&lang=ENG).
[100] See the Smart Sheriff registration page: https://ss.moiba.or.kr/member/memberJoin_01.do (available in Korean only).

different page explaining Smart Sheriff's treatment of personal information, published and effective as of April 9, 2015, is available on the Smart Sheriff website as well.[101] The primary difference between the policies presented in this April 9 document and those displayed via the Smart Sheriff application registration is that the April 9 document contains a detailed article 5 on measures to protect user privacy.

MOIBA claims in this article 5 to have "put in place technical measures to prevent leakage, loss, theft, or falsification of personal information in processing Member's information."[102] The technical measures specified are:

- Member's personal information is protected by password, and accessing and changing the personal information is only possible for the member, the legal representative, or the guardian who knows the password. However, this excludes situations where the member, the legal representative, or the guardian contacts the company by phone or email to request access or changes to their personal information.
- MOIBA prevents any data breach or damage on Members' personal information by adopting the latest antivirus program.
- MOIBA protects transmission of personal information on the network by encrypted communication, etc.
- MOIBA controls any unauthorized external access by an intrusion blocking system to prevent data breach by hacking, etc.[103]

Smart Sheriff's policies also describe the types of data that are retained by the service. According to the terms of use, the child version of the Smart Sheriff application provides for the automatic collection of information about applications installed on the child's smartphone, package identifier, version number, and application name. The policies further describe the automatic and mandatory collection of data related to account password, member name, phone number, child's date of birth, IP addresses of service access, and log file information such as access time, for a retention period of a year.[104]

Finally, under the terms of the Smart Sheriff user agreement on "Providing Personal Information to Third Parties," user data may be shared with the relevant Office of Education and the student's school for purposes of smartphone addiction counselling, and with telecommunications business operators for the purpose of complying with the notification obligations of the mandate on installation of means for blocking harmful content.[105]

Smart Sheriff Terms of Service and Privacy Policy: Translated Excerpts

Items of Personal Information Collected and Methods of Collection[106]

[101] "Treatment of Personal Information," https://ss.moiba.or.kr/popup/popupPers.do (available in Korean only).
[102] Ibid., art. 5(1).
[103] Ibid., art. 5(1)(1).
[104] See https://ss.moiba.or.kr/member/memberJoin_01.do (available in Korean only). For an English translation of excerpts of the policy text, see Smart Sheriff Terms of Service and Privacy Policy: Translated Excerpts below.
[105] See lower left quadrant of https://ss.moiba.or.kr/member/memberJoin_01.do (available in Korean only).
[106] See upper right quadrant of https://ss.moiba.or.kr/member/memberJoin_01.do (available in Korean only).

A. Items of Personal Information Collected

Items below are collected at the point of subscription to facilitate the use of the service:

1) Mandatorily collected items: password, name, phone number, date of birth (of the child)
2) Optionally collected items: email, address, etc.
3) Automatically collected items: IP addresses, logfiles such as access time, etc. and so forth

B. Methods of Collection

Personal Information is collected according to the methods specified below:

1) It is automatically collected when Member is using the service, or when it is voluntarily provided by Member.
2) Through email, phone call, fax, Customer Service Center bulletin board, website, etc.

Retention of Personal Information[107]

The subscriber's personal information will be discarded without delay after fulfilling its purpose of collection and use. However, the information below is retained for the specified period for the following reasons:

1) Personal information retained at the time of signing off

- Items: mobile phone number, email, reported postings, sign-in date, and sign-off date
- Reasons: to deal with complaints regarding signing off, to prevent re-signing in of bad members, and to cooperate with disputes regarding defamation
- Period: 1 year

2) According to the Communications Secrets Protection Act, the information below[108] is retained for three months:

- Log data of the computer communications or the Internet relating to the use the telecommunications services by the users of computer communications or the Internet
- Tracking data on the access point required to identify the location of information communications apparatus the user of computer communications or the Internet is using to access the information communications networks

[107] See upper right quadrant of https://ss.moiba.or.kr/member/memberJoin_01.do (available in Korean only).
[108] These data constitute "communication confirmation data" under the Communications Secrets Protection Act. See Enforcement Decree of the Communications Secrets Protection Act, art. 41(2)(2), http://elaw.klri.re.kr/kor_service/lawView.do?hseq=31478&lang=ENG.

Collected information is shared with third parties, including the school the juvenile is attending and competent Office of Education.

Information Sharing in Smart Sheriff[109]			
Third Party	*Purpose*	*Shared Information*	*Retention and Use*
School at which Member is enrolled	Smartphone addiction counselling	Phone number, automatically collected information (IP address and logfiles)	From the time Member gave individual consent to the earlier of the date the third party stops providing service to Member or the date Member withdraws from the third party's service
Office of Education to which Member belongs			
Telecommunications business operators,[110] Korea MVNO Association	Notification obligation of telecommunications business operators under article 32-7 of Telecommunications Business Act	Child's information (name, MNO, mobile phone number, sign-in date, evidence of deletion) and parent's information (name, MNO, mobile phone number)	

[109] See lower left quadrant of https://ss.moiba.or.kr/member/memberJoin_01.do (available in Korean only).
[110] Thirty-two operators are listed in the table, including SKT, KT, LG U+ (three major telecoms), and mobile virtual network operators (MVNOs). However, the list also includes companies that are not telecoms, such as large hypermarket chains Homeplus and E-Mart.