UNIVERSITY OF TORONTO

MUNK SCHOOL OF GLOBAL AFFAIRS

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)

Introduction

While South Korea is one of the most highly connected societies in Asia, its government has established an aggressive regulatory regime to control digital content deemed illegal, a national security threat, or harmful to minors.

In April 2015, a mandate came into effect requiring South Korean telecommunications operators to provide the means to block harmful content on minors' mobile phones. The mandate, introduced by South Korea's telecommunications regulatory body, the Korean Communications Commission (KCC), also requires that a minor's parent be notified if the content filtering is disabled. While 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.

Well before the April 2015 mandate, the Korean Mobile Internet Business Association (MOIBA), an influential consortium of mobile telecommunications providers and phone manufacturers, released the Smart Sheriff parental-monitoring application. Smart Sheriff was developed and promoted with the support of the KCC, including funding totaling KRW 3.18 billion (approximately USD $2.7 million) for a project made up of Smart Sheriff and an additional messaging-monitoring application called S-Dream.[1] Smart Sheriff allows parents to remotely block content and monitor and administer applications that a child is able to access on their mobile device, as well as schedule the times of day that the phone can be used.

Smart Sheriff is one of several applications that may fulfill the April 2015 regulatory requirements. Compared to other Korean-language parental-monitoring applications, it is widely used (between 100 and 500 thousand users), and has received substantial publicity from the KCC.[2] Smart Sheriff is an important case for understanding the risks and implications of requiring digital-monitoring services for minors.

This report describes the results of two independent security audits of Smart Sheriff, one by researchers who collaborated at the 2015 Citizen Lab Summer Institute (held at the Munk School of Global Affairs, University of Toronto), and the other by the auditing firm Cure53.[3]

[1] http://www.sisainlive.com/news/articleView.html?idxno=23878 [in Korean].

[2] This user population estimate is based on installation statistics for Smart Sherriff from the Google Play Store at https://play.google.com/store/apps/details?id=com.gt101.cleanwave [in Korean].

[3] The Citizen Lab Summer Institute is an annual research workshop (see https://citizenlab.org/summerinstitute/index.html). Cure53 (https://cure53.de) is a Berlin-based security company

The combined audits identified twenty-six security vulnerabilities in recent versions of Smart Sheriff (versions 1.7.5 and under). These vulnerabilities could be leveraged by a malicious actor to take control of nearly all Smart Sheriff accounts and disrupt service operations. Each vulnerability is fully described in the technical appendix (appendix A) and the wider implications of these findings are discussed in the legal and policy appendix (appendix B).

Technical Findings

The audits identified the following critical security flaws:

- Personally Identifiable Information (PII) and account credentials are not stored, processed, or transmitted securely so they are vulnerable to interception.

- Malicious code can be injected into the application, allowing third parties to perform unauthorized activities.

- Design failures allow parent-set limits to be easily circumvented or disabled.

- Accounts can be registered and managed without proper validation or passwords, which could lead to denial of service or compromise of accounts.

- While website filtering functionality has been supposedly disabled since May 2015, Smart Sheriff still insecurely transmits Web browsing activity to MOIBA which makes the content vulnerable to interception.

- Smart Sheriff's infrastructure is not properly maintained or protected against malicious activity, including brute force attempts and erroneous requests, which could lead to compromise of the service.

Legal and Policy Implications

We identified the following legal and policy implications:

- Smart Sheriff's limited security features fall substantially short of data protection and information security requirements under Korean law.

specializing in thorough and manual penetration tests and code audits covering Web applications, cryptographic implementations, and other soft- and hardware. Cure53's penetration testing research was performed under an ongoing contract from the Open Technology Fund (https://www.opentechfund.org).

- Smart Sheriff's insecure design runs counter to the representations made by MOIBA in Smart Sheriff's terms of service and privacy policy.

- Smart Sheriff's functionality impinges upon its users' privacy rights while exceeding the actual requirements of the April 2015 mandate.

- Taken together, these problems raise concerns under international human rights law.

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

[4] See, for example, "Vulnerability Disclosure Policy," http://www.cert.org/vulnerability-analysis/vul-disclosure.cfm.

[5] https://ss.moiba.or.kr/customer/bbs/info.do?BBS_BOARD_CODE=Notice&BBS_POST_CODE=2949&pop=Y&NOWNUM=3 [in Korean].

[6] https://ss.moiba.or.kr/customer/bbs/info.do?BBS_BOARD_CODE=Notice&BBS_POST_CODE=2984&pop=Y&NOWNUM=1 [in Korean].

inadvertently disclosed. As of the date of publication, we have not received any further correspondence from MOIBA.

Smart Sheriff Overview

Smart Sheriff allows parents to remotely monitor and administer applications on their children's phones, and to schedule the times of day that the phone can be used. It was officially launched for Android in June 2012. An iOS version was created soon after but it has not been updated since 2013 and reportedly has limited usability.

Registration

Once installed, Smart Sheriff requires the following information:

- phone numbers for parent and child
- the child's gender and date of birth
- the child's name
- PIN code for the administration of the account.

After registration, Smart Sheriff routinely transmits usage and configuration information from the phone to the back-end server, including:

- manufacturer, model, and operating system version of the device
- applications installed on the phone and their amount of usage
- websites visited.

Functionality

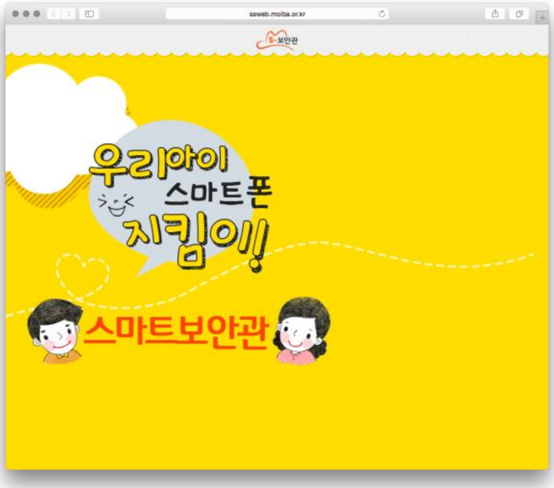
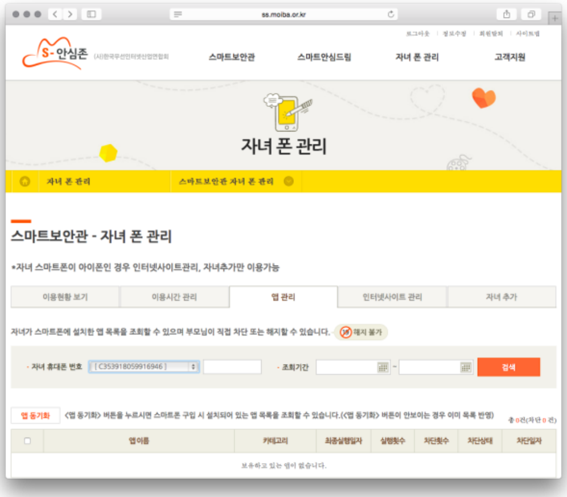
Parents can control applications and schedule usage restrictions in two ways: with the application itself or through a website hosted by MOIBA. Both require the parent's phone number and the PIN code set during registration. On both interfaces, the parent can review the information collected from the child's device and control what applications are accessible.

For the minors, interaction with the application is limited to warning messages that are triggered when they attempt to use prohibited applications or use the phone during restricted times. It appears that the only authorized way to remove the app is through the Web interface.

Descriptions of Smart Sheriff in app stores claim it can filter websites that minors can access.[7] However, these functions have apparently been disabled since 18 May 2015.

[7] https://play.google.com/store/apps/details?id=com.gt101.cleanwave&hl=en [in Korean].

MOIBA indicated that the reason for disabling this functionality was concern over infringement of children's privacy.[8]

 ssweb.moiba.or.kr S-보안관 우리아이 스마트폰 지킴이! 스마트보안관	 ss.moiba.or.kr 로그아웃 | 정보수정 | 회원탈퇴 | 사이트맵 S-안심존 (사)한국무선인터넷산업연합회 스마트보안관 스마트안심드림 자녀 폰 관리 고객지원 자녀 폰 관리 자녀 폰 관리 스마트보안관 자녀 폰 관리 이용현황 보기 이용시간 관리 앱 관리 인터넷사이트 관리 자녀 추가 해지 불가 검색 앱 동기화 스마트보안관 - 자녀 폰 관리 *자녀 스마트폰이 아이폰인 경우 인터넷사이트관리, 자녀추가만 이용가능 자녀가 스마트폰에 설치한 앱 목록을 조회할 수 있으며 부모님이 직접 차단 또는 해지할 수 있습니다. · 자녀 휴대폰 번호 [C353918059916946] · 조회기간 ~ <앱 동기화> 버튼을 누르시면 스마트폰 구입 시 설치되어 있는 앱 목록을 조회할 수 있습니다.(<앱 동기화> 버튼이 안보이는 경우 이미 목록 반영) 총 0건(차단 0 건) □ 앱이름 | 카테고리 | 최종실행일자 | 실행횟수 | 차단횟수 | 차단상태 | 차단일자 보유하고 있는 앱이 없습니다.
Application Interface	Web Interface

Security Audit Results

We identified twenty-six vulnerabilities and design issues that could lead to the compromise of user accounts, disclosure of information, and corruption of infrastructure. The same issues were often present in multiple parts of the application and infrastructure. For example, we identified a potential attack against user accounts via the Smart Sheriff mobile application, then determined that it could also be made against the Web-based parental administration site. These multiple flaws suggest that the application was not fully examined for security issues before being released. Both audits were done in a limited window of time and without access to the original source code.

Many of the vulnerabilities we identified were compounded by a lack of proper protections for accounts and on Smart Sheriff's back-end services, creating systemic, compounding failures with significant implications for users. For example, Smart Sheriff

[8] MOIBA's communication on the matter is found in this user forum, under posting number 1366 https://ss.moiba.or.kr/customer/bbs/list.do [in Korean].

relies on a user's phone number for authentication. However, phone numbers are predictable and a poor substitute for a private code.

Taken together, the flaws that we identified could be exploited by a malicious actor to take control of nearly all Smart Sheriff accounts and disrupt the service's entire operations. For example, a minor child could easily disable their own copy of the application. However, of greater concern, an attacker could also trigger the uninstallation of a copy of Smart Sheriff from nearly every device without users' permission.

We provide high-level overviews of the security issues we identified across three broad categories: (1) failure to properly encrypt data, (2) lack of effective access controls, and (3) lack of infrastructure security.[9]

Failure to Properly Encrypt Data

Sensitive User Data Is Not Encrypted

Smart Sheriff fails to adequately encrypt and protect user data and Personally Identifiable Information (PII), either in storage or in transit. The ways that Smart Sheriff handles PII fall below widely accepted best practices as well as standards set out by Korean law.[10] Our audit found that authentication, registration, and communications with Smart Sheriff's servers are all unencrypted. As a result, names of minors and parents, dates of birth, mobile device information, gender, and telephone numbers are all visible to anyone controlling the network that the device uses. An attacker could capture the data and use them to impersonate Smart Sheriff's server, and issue commands that Smart Sheriff apps would treat as genuine.[11]

Disclosure of User Traffic Records in Plaintext

Smart Sheriff has the ability to monitor and filter access to Web content, although use of this functionality is not currently available for parents. Despite this feature not being operational, the application still sends records of all Web traffic from the child's device to the Smart Sheriff service.

Smart Sheriff establishes a monitoring service on Android to read the browser history as it is recorded and matches requests for websites against a block list. For every page accessed, a request is made to the Smart Sheriff API containing the requested domain,

[9] Each identified vulnerability is indexed with full technical details in the technical appendix (A).

[10] See the legal and policy appendix (B) for details.

[11] See issue 1.1: "No Transport Security in Smart Sheriff Communications" in the technical appendix.

page, and URL parameters, regardless of whether this Web request was performed to an unencrypted (HTTP) or encrypted (HTTPS) website.

In response to this information, a score is returned for each site that determines whether the website should be filtered. If the site matches the block list the user is forwarded a block page. During this communication Smart Sheriff circumvents part of the protective features of HTTPS, thus undermining the security of third-party websites visited by the user by simultaneously exposing the traffic to the network and sending a complete browsing record to MOIBA.[12]

Authentication Not Properly Encrypted and Vulnerable to Attack

Although Smart Sheriff attempts to obfuscate the unique device identifier and parental passcode that are used to authenticate the application to Smart Sheriff's server, the approach used is weak and provides minimal security. The identifier, which is either the phone number or the device's hardware identifier, is obfuscated using an insecure method that is contrary to standard practice.[13]

Keys and obfuscation can be reverse-engineered (or extracted from the decompiled app), allowing an attacker to decrypt any of the protected data or target specific users. Even if the key is not known to an attacker, Smart Sheriff's obfuscation can be fully bypassed through simple and well-known attacks, granting an attacker access to sensitive information.

No Additional Data Storage Protections

Smart Sheriff does not encrypt locally stored user data and instead relies solely on the application data segregation within the Android operating system to provide moderate security assurances. Smart Sheriff does not implement any form of cryptographic protection on its internal storage.[14] Moreover, the application and MOIBA infrastructure do not check for malformed or malicious requests that could compromise the application's integrity. In the course of auditing the application, we were able to collect information on the database schema and back-end services of MOIBA. The ability to retrieve this information calls into question the level of protection afforded to remotely stored data and indicates that there is no encryption for personally identifiable information.

[12] See issue 1.3: "Disclosure of User Traffic Records in Cleartext" in the technical appendix.

[13] This obfuscation uses a secret key to transform the identifier (XOR). For details see issue 2.1: "Smart Sheriff API Discloses Parent Password" and issue 3.1: "Identification to Smart Sheriff API Is Based on Predictable Identifiers " in the technical appendix

[14] See issue 4.2: "Lack of Storage Protections on the Mobile Application" in the technical appendix.

MOIBA Infrastructure Has Inadequate SSL Security

While Smart Sheriff itself did not use transport encryption, MOIBA infrastructure supports secure transmission of traffic through TLS/SSL.[15] However, their servers fail to meet common security standards. The deployment is based on obsolete and insecure protocols that are vulnerable to attacks that could lead to the interception and impersonation of MOIBA's servers. According to SSL Labs' widely used metric, Smart Sheriff's deployment of SSL receives an "F" grade.[16] The transport encryption offered is clearly inadequate.[17]

After our disclosure, MOIBA released an update to Smart Sheriff (v1.7.6) that includes communication over HTTPS. However this version does not properly validate the credentials received and appears to accept a self-signed certificate, which minimizes the update's effectiveness.

Lack of Effective Access Controls

The primary mechanism for authentication across the Smart Sheriff service is a device identifier that is derived using reversible obfuscation rather than industry-standard encryption. If an attacker is able to guess, enumerate, or intercept the device identifier of a phone with Smart Sheriff installed, the attacker can impersonate the application and undertake a range of attacks.[18]

For example, using only the device identifier, an attacker can impersonate a user and request the parents' phone number, children's names, and their dates of birth. Moreover, an attacker can use the Smart Sheriff API to request a parent's administration code (itself an insecure four-character string) and use it to take control of the account.

Inconsistent and Insufficient Authentication

Neither the Smart Sheriff Web-based parental administration interface nor its API consistently check that requests for sensitive information are valid. The result is a wide range of potential attacks. An attacker who knows only the phone number of a target

[15] TSL refers to Transport Layer Security protocol, and SSL refers to Secure Sockets Layer protocol, which provide for the authentication of servers and clients and the transmission of encrypted communications between the authenticated parties. See, for example, https://technet.microsoft.com/en-us/library/Cc784450(v=WS.10).aspx.

[16] SSL Report, https://www.ssllabs.com/ssltest/analyze.html?d=api.moiba.or.kr&hideResults=on

[17] See issue 6.2: "SSL Misconfiguration on MOIBA Resources" in the technical appendix.

[18] See issue 3.1: "Identification to Smart Sheriff API Is Based on Predictable Identifiers" in the technical appendix.

can request the name, age, and usage statistics of a user via the API.[19] Similarly, an attacker can falsify reports that a particular user has violated parental controls.

In some cases, Smart Sheriff servers blindly accept queries that it believes are sent by the browser without checking whether the requester owns the account, or if the user whose data are being accessed is even logged in via the Web interface. This vulnerability enables an attacker who possesses a Smart Sheriff user's phone number to retrieve sensitive information, modify accounts, and even disable devices. An unauthenticated attacker can even create a new account, whether or not an original account already exists, creating a further vector of compromise.[20]

While our audit examined only a limited number of queries, it is clear that an attacker who has enumerated users' phone numbers could potentially change the PINs of parental accounts, remotely disable devices, and even disclose personal information for all Smart Sheriff users.

Lack of Infrastructure Security

High-Volume Queries Not Restricted

We attempted to identify local phone numbers registered with Smart Sheriff to measure the applications' popularity. This test involved queries that made thousands of requests to MOIBA within a short period of time. At no point were these queries restricted, which means that brute-force attempts on passwords and numbers would be feasible against the application, even if protections for account access were put into place.[21]

Unpatched and Outdated

The software providing the Smart Sheriff back-end services is out of date, and contains known vulnerabilities. Most of the software observed on the remote server is at least two years old. These outdated and depreciated services make it highly likely that the Smart Sheriff infrastructure will experience compromise or error. Software packages should be kept current and patch levels should be no more than days or weeks behind new updates, at the very most. The Web services also appear to be misconfigured,

[19] For details see issue 3.8: "Smart Sheriff Application Interface Leaks Account Information without Authentication" in the technical appendix.

[20] See issue 3.10: "Smart Sheriff Web Interface Allows Account Access and Discloses Personal Information Through Unauthenticated Web Interface API Queries" in the technical appendix.

[21] See issue 3.4: "Smart Sheriff Does Not Appear to Monitor or Rate Limit Sensitive API Requests" in the technical appendix.

leaving default documents, internal administrative information, and test code openly accessible, which can also be used to compromise infrastructure.[22]

Potential for Mass Compromise

Combinations of the identified vulnerabilities could lead to mass compromise of accounts or service disruption. An attacker with the resources to run a high volume of queries against Smart Sheriff could potentially identify all of Smart Sheriff's users, and then use the vulnerabilities we identified to systematically disrupt all subscribers' devices or the service itself.

Legal and Policy Implications

Smart Sheriff raises a number of legal and policy questions not only because of its security vulnerabilities but also because authorities have positioned it as a primary means for compliance with Korean telecommunications regulations. South Korean law establishes high standards for the protection of personal information and users' digital security but the technical design of Smart Sheriff fails to properly meet these standards. Even though the application's functionality is far more expansive — and invasive — than that required by the April 2015 mandate, the KCC and others have promoted the application specifically in connection with that mandate. These issues are particularly significant in light of the intended use of the application by minors and their guardians.

Insufficient Data Protection and Information Security Measures under Korean Law

South Korean data privacy and security laws place a number of requirements on MOIBA as the provider of Smart Sheriff.[23] The *Personal Information Protection Act* (PIPA) and its Enforcement Decree apply to entities such as MOIBA that manage personal information.[24] PIPA mandates that personal information managers "take technical, administrative and physical measures" to protect personal information "from loss, theft, leakage, alteration or damage."[25] Among the measures enumerated in the Enforcement Decree for ensuring the safety of personal information are requirements to control access to such data; adopt encryption technology to store and transmit the data;

[22] See issue 6.3: "Resources Out of Date, Potentially Vulnerable" in the technical appendix.

[23] See the legal and policy appendix (B) for a complete discussion of the relevant law.

[24] Personal information includes any information by which an individual can be identified (e.g., that individual's name or registration number), either alone or in combination with other information. PIPA art. 2(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(10465) [in Korean].

[25] PIPA art. 29.

retain login records to respond to data-breach incidents; and install and upgrade security programs.[26]

Our security audit, however, found Smart Sheriff did not meet the specific measures required by the PIPA Enforcement Decree. For example, MOIBA did not provide adequate access controls and failed to properly encrypt personal information, its servers also did not monitor and limit access requests made to the API, and made use of outdated software on its infrastructure. Any or all of these vulnerabilities could lead to the “loss, theft, leakage, alteration or damage” of personal information that PIPA was enacted to prevent.

Additionally, if MOIBA is considered an “information and communications service provider” under Korean law,[27] it must also follow the technical and administrative protective measures for handling personal information as laid out in the *Act on Promotion of Information and Communications Network Utilization and Information Protection, Etc.* (ICNA).[28] Similar to PIPA, the ICNA requires a service provider to, among other things, prevent unauthorized access to personal information, and to use “encryption technology and other methods for safe storage and transmission of personal information.”[29]

The ICNA’s Enforcement Decree and the KCC guidelines released pursuant to that decree provide significant detail on the appropriate application of encryption technology. The decree requires “one-way encrypted storage of passwords”; encrypted storage of account numbers and other information designated by the KCC; and secure servers for “transmitting users’ personal information and certification information.”[30]

As we identified, Smart Sheriff did not properly incorporate these measures. Moreover, the KCC guidelines — which apply to “service providers or similar”— note that “secure server[s] must have one of the following features: a. installation of SSL (Secure Socket Layer) certificate on the web server to encrypt information being transmitted; [or] b.

[26] 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).

[27] See discussion in legal and policy appendix, n. 81 and accompanying text.

[28] ICNA art. 28(1), 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).

[29] ICNA art. 28(1).

[30] Enforcement Decree of ICNA, art. 15(4), 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).

installation of an encryption application program on the web server to encrypt information being transmitted."[31] However, Smart Sheriff servers employed neither SSL/TLS nor local encryption; rather, the application transmitted all personally identifying information in cleartext to the network.

Insufficient Information Security Measures under MOIBA's Own Terms of Service

The South Korean regulations described here are at face value reflected in the terms of service and privacy policy provided by MOIBA to users of the Smart Sheriff application. Yet just as the application falls short of regulatory standards, so does it fail to fulfill MOIBA's own contractual terms. In particular, MOIBA asserts that it has "put in place technical measures to prevent leakage, loss, theft, or falsification of personal information in processing Member's information."[32] These measures purportedly include password protection for personal information, updated antivirus protections, encrypted communications, and an intrusion-blocking system.[33] However, our analysis shows that Smart Sheriff did not incorporate some of these data protection measures demonstrated by lack of encryption for data in transit and the presence of outdated software on MOIBA's server infrastructure.

Functionality Exceeds Actual Requirements of the Law

Smart Sheriff was developed, with the KCC's substantial support, throughout the time that the South Korean government has worked to establish greater control over digital media consumption by minors. The government's efforts culminated in the April 2015 mandate on provision of blocking means and parental notification, and Smart Sheriff was highlighted prominently as a solution for compliance with that mandate.[34]

As the primary association of telecommunication providers in the country, MOIBA is powerfully positioned to publicize Smart Sheriff to vendors who must comply with the official mandate. Yet there is a divergence between Smart Sheriff's functionality and the regulation's actual requirements.

The April 2015 mandate proposed by the KCC requires only a means for blocking harmful media products, accompanied by notice to a parent by the telecommunications business operator when that means becomes inoperative. Yet Smart Sheriff is designed

[31] Guidelines on Technical and Managerial Protective Measures for Personal Information, art. 6, http://www.law.go.kr/admRulLsInfoP.do?admRulSeq=2100000019404 (available only in Korean).

[32] "Treatment of Personal Information," art. 5(1), https://ss.moiba.or.kr/popup/popupPers.do (available in Korean only, see an English translation in the legal and policy appendix).

[33] Ibid.

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

to do much more. The KCC itself distinguished among the features offered by Smart Sheriff 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.[35]

Thus, the application provides not only a “means for blocking harmful information,” but also “functions for querying or blocking … or limiting the number of access hours,” enabling direct parental control of a child’s smartphone usage.

Through the promotion of Smart Sheriff by the KCC and others, the April 2015 mandate has acquired the de facto effect of a parental monitoring and control mandate. This evolution of the mandate seems to implicate privacy concerns and excessive restrictions on juveniles that the National Assembly specifically tried to avoid when amending the law. It also raises questions regarding public expectations surrounding the mandate, and legislative intent. Indeed, Smart Sheriff’s actual blocking functionality was curtailed by MOIBA in May 2015, with MOIBA citing privacy implications — leaving in place only the parental control functionality that is outside the plain terms of the regulation.

International Human Rights Law Concerning Children and Privacy

The privacy implications of government-mandated smartphone applications for minors merit further scrutiny under international human rights law, particularly the International Covenant on Civil and Political Rights (ICCPR)[36] (accession by South Korea in 1990)[37] and the Convention on the Rights of the Child (CRC)[38] (ratified by South Korea in 1991).[39] ICCPR article 17 provides that “no one shall be subjected to arbitrary or

[35] Korea Communications Commission, 2013 Annual Report, p. 109, available at http://eng.kcc.go.kr/user.do?mode=view&page=E02020000&dc=E02020000&boardId=1053&cp=1&boardSeq=38653.

[36] United Nations International Covenant on Civil and Political Rights, http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx.

[37] https://treaties.un.org/pages/viewdetails.aspx?chapter=4&src=treaty&mtdsg_no=iv-4&lang=en

[38] UN Convention on the Rights of the Child, http://www.ohchr.org/en/professionalinterest/pages/crc.aspx.

[39] https://treaties.un.org/pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-11&chapter=4&lang=en

unlawful interference with his privacy, family, home or correspondence,"[40] and that "everyone has the right to the protection of the law against such interference."[41] CRC article 16 provides that this right to privacy applies specifically to children.[42] The April 2015 mandate and its overbroad fulfillment through Smart Sheriff may undermine minors' right to privacy because it has resulted in the collection of an extensive amount of data, including minors' personal information and smartphone usage patterns, and permits that data to be shared not only with parents but also with entities such as the child's school.[43]

Indeed, the United Nations Human Rights Committee has, in preparation for its upcoming review of South Korea, requested from the government more "information on current legislation and practices governing the monitoring, surveillance and interception, analysis, use and storage of private communications (including Internet, telephone, e-mail and fax communications) and private data," including an explanation of how a similar application for control of students' mobile phones is compatible with ICCPR article 17.[44]

These privacy concerns are compounded by the significant security vulnerabilities of the application that could allow malicious actors to wholly compromise the personal data and accounts of minors and their parents. To protect the right to privacy, the KCC or other government entities should have carefully evaluated the digital security risks presented by the government's mandate and promotion of Smart Sheriff services (and other such applications). It is unknown whether the government undertook such an evaluation before relying on the service. However, it is probable that a technical security audit of Smart Sheriff would have identified many of the problems we uncovered in our investigation.

Finally, the mandate and its implementation raise questions regarding the role of the government in parental oversight of children. CRC article 5 requires states to "respect the responsibilities, rights and duties of parents … to provide, in a manner consistent with the evolving capacities of the child, appropriate direction and guidance in the

[40] ICCPR art. 17(1).

[41] ICCPR art. 17(2).

[42] CRC art. 16.

[43] An extensive report by UNICEF and the Young and Well Cooperative Research Centre in 2014 found that children's right to privacy can be affected by parental monitoring, and that some children surveyed felt "that privacy often means having a space of their own beyond the adult gaze." See Third, Amanda, et al., *Children's Rights in the Digital Age: A Download from Children Around the World* (Melbourne: Young and Well Cooperative Research Centre, 2014), 47, http://www.unicef.org/publications/files/Childrens_Rights_in_the_Digital_Age_A_Download_from_Children_Around_the_World_FINAL.pdf.

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

exercise by the child of the rights recognized in the present Convention"[45] — including freedom of expression and the right to privacy. By requiring telecommunications business operators to provide blocking means on minors' mobile devices by default, and promoting insecure options for doing so, the state has instead compelled parents to moderate their children's experience of digital media, and exposed children to security risks of which parents are not informed.[46]

Conclusion

Smart Sheriff exemplifies the risks inherent in government-mandated monitoring applications. The application's design suffers from serious security flaws and appears to have been insufficiently checked for vulnerabilities, yet users have little choice in adopting and continuing to use the software. Indeed, this technology was popularized throughout the country through government regulation, exposing potentially hundreds of thousands of users to digital security compromise. It has also opened the door to societal acceptance of parental-monitoring and content-blocking practices that raise concerns under international human rights law.

Acknowledgements

We are grateful to Kelly Kha Yeun Kim (OpenNet Korea) and Professor Kyung Sin "K.S." Park (Korea University, OpenNet Korea) for substantive input on the South Korean legal and policy environment and for translation assistance (for further information on OpenNet Korea see http://opennetkorea.org). Special thanks to Jakub Dalek, Jacqueline Larson, Irene Poetranto, and Adam Senft. The 2015 Citizen Lab Summer Institute where one of the security audits was conducted was sponsored by the Open Technology Fund and the University of Toronto's Connaught Fund.

[45] CRC art. 5.

[46] While Japan is the only country to have taken a similar step with regard to minors' digital usage, the government offered citizens a clear opt-out process that establishes boundaries more in keeping with international human rights principles. See Japan, Global Information Society Watch, http://www.giswatch.org/country-report/20/japan.