GLOBAL INFORMATION SOCIETY WATCH 2014

Communications surveillance in the digital age

This report was originally published as part of a larger compilation, which can be downloaded from GISWatch.org

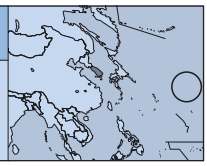
Association for Progressive Communications (APC)
and Humanist Institute for Cooperation with Developing Countries (Hivos)

ISBN: 978-92-95102-16-3

APC-201408-CIPP-R-EN-DIGITAL-207

KOREA, REPUBLIC OF

Communications surveillance in South Korea



Jinbonet
Chang, Yeo-Kyung
http://act.jinbo.net/drupal/english

Introduction

The Korean Railway Worker's Union (KRWU) went on strike on 9 December 2013 opposing the privatisation of the railroad. The Korean government's response was hard-line, and the police imposed widespread surveillance on the striking workers and their families.

Firstly, the police acquired all the mobile communication records of union members and their families, including schoolchildren, and tracked the real-time location of their mobile phones – the mobile service providers had offered to provide this information at 10-minute intervals for several months. The police also asked popular websites, such as game sites and internet shopping malls, to provide the real-time access IP addresses of the workers and their families. The mobile service providers also handed over the identities of about 300 to 400 people who talked on the phone with the strikers to the police, who used this information to interview the subscribers about details of their relationship with the strikers. Railway workers and human rights NGOs, including Jinbonet, filed a petition to the Constitutional Court against the real-time location tracking on May 2014.

Policy and political background

The NGOs argued that the lack of adequate legal requirements for police to access communication metadata in an investigation is unconstitutional. The authorities conduct surveillance on workers exercising their right to strike as if they were criminals – they have been maintaining a DNA database of criminals, which includes striking workers, since 2010.[1] Communications surveillance in particular, which has insufficient legal control given the rapid development of the internet and mobile technologies, has significantly extended the power of the police and the intelligence agency beyond the law.

Communications surveillance in South Korea is regulated by the Protection of Communications Secrets Act (PCSA). The previous military dictatorship in South Korea had conducted communications surveillance for a long time without any legal regulation. The PCSA, passed in 1993 in the aftermath of a wiretapping controversy among presidential candidates, allows the intelligence agency and investigation agencies to intercept the content of communications in real time with prior court approval. The content of communications such as stored email or SMS messages is provided to agencies with a prior warrant for search and seizure under the Criminal Procedure Act. However real-time wiretapping on foreign groups and nationals can be conducted merely with the approval of the president. The intelligence agency and the investigation agencies can wiretap in real time by making use of intermediaries, including telecommunication service providers, or by using their own technologies. They can also wiretap without any permission for 36 hours if it is considered an emergency.

Since 2002 the PCSA has begun to regulate communication metadata: the record of the date and the time of communications, the IP address, the internet logs, the location of the base station or the communication device, etc. Although court permission has been required to collect communication metadata since 2005, when it is "necessary to conduct any investigation," the permission is given without any specific restrictions. According to the Telecommunications Business Act, personal information to identify the subscriber or user such as name, residential registration number (which is the national ID number in South Korea), address, etc. is separately provided to the agencies without any permission from external supervisory agencies such as the courts.

Ex-post notification[2] has been implemented regarding undercover communications surveillance: users have been notified of wiretapping since 2001, of the handing over of communication metadata to agencies since 2005, and of the search and seizure of stored communications content since 2009.[3] The personal information of the subscriber or the user is not included in this notification. The government

1 act.jinbo.net/drupal/node/7631

2 Police notify persons of the fact that they became a target of wiretapping within 30 days after the decision is made.

3 However, in the last two cases the violator was not punished.

TABLE 1.

Base-station data provided to investigators

	Base-station data	All communications metadata
Second half of 2009	15,440,864	15,778,887
2010	38,706,986	39,391,220
2011	36,800,375	37,304,882
2012	24,831,080	25,402,617
2013	15,245,487	16,114,668

SOURCE: Government of the Republic of Korea (Korea Communications Commission, the Ministry of Future Creation and Science)

then releases statistics about the number of these cases twice a year.

Besides the above, telecommunications service providers, including intermediaries, should keep communication metadata depending on the service they offer:

- Twelve months for mobile service providers
- Six months for landline service providers
- Three months for internet service providers.

Communications surveillance: Cases and civil society reaction

Although the PCSA was an attempt to legally regulate communications surveillance, the rapid development of the internet and mobile technologies, and the prompt adoption of them by the agencies, makes it overwhelming. A popular example is real-time location tracking of telecommunication devices.

Real-time location tracking

When the PCSA created the framework for the regulation of communication metadata in 2002, it referred to *historical* communication records. Without any external request, telecommunications service providers have kept the historical communication metadata related to billing, and they were to some extent expected to and asked to by their customers. However, agencies then started to require the "future" location information of their targets. The telecommunications service providers accepted the request, not only because collecting real-time location information and providing this was technically possible, but also because the related regulatory clause was not clearly defined on that matter.

For example, in the case of a mobile phone location, the telecommunications service provider informs a police officer of the location of the base station capturing the signal from the specified mobile phone by text message every 10 minutes. In the case of IP addresses, the internet service provider informs the police officer when the specified ID logs in.[4] Because telecommunications service providers in South Korea confirm their subscribers' or users' identities before activating mobile phone or internet services including online games, this kind of location information helps the agencies to accurately track the subject.

Real-time tracking was illustrated when a woman worker had been staging a sit-in protest at the top of a 35-metre-high crane for more than 150 days to oppose a huge lay-off of workers. "Buses of hope" had been organised to support her struggle, carrying thousands of supporters to the place of protest. To arrest those who organised the buses, the police and the prosecutors traced the real-time location of the mobile phones of the activists and their families for months. Human rights NGOs challenged this in the Constitutional Court in 2012, filing a second petition against tracing the mobile phones and internet IDs of the leaders of the KRWU and their families in 2014. Both Constitutional Court reviews are still underway.

The use of data from base stations

Another constitutional controversy surrounding communication metadata concerns the use of data from mobile base stations. The PCSA does not clearly define whether or not agencies should specify the technical scope of the request when they require a telecommunications service provider to hand over communication metadata. Consequentially, agencies are offered mobile phone numbers captured by base stations around the areas where assemblies and demonstrations take place to identify people who participate in these protests. In the case of

4 Some online game companies have subsidiaries to deal with these requests as they receive too many from the police. newsmaker.khan.co.kr/khnm.html?mode=view&code=115&artid=201112061719361&pt=nv

TABLE 2.

Requests for telecommunications interception

Year	Prosecution	Police	NIS	Military investigative unit or others	Total	NIS requests as % of total
2010	4	227	8,391	48	8,670	96.8%
2011	3	263	6,840	61	7,167	95.4%
2012	0	139	5,928	20	6,087	97.4%
2013	1	96	5,927	8	6,032	98.3%

SOURCE: Government of the Republic of Korea

highly populated areas, the agency could be provided with over 10,000 mobile phone numbers from just one base station.

In 2012, a phone number of a journalist who covered an opposition party event was included in the base-station data offered to investigators. Jinbonet and the victim submitted a constitutional petition and the review is now underway.

Table 1 shows statistics on the amount of base-station data offered to investigators, compared to all the metadata handed over to authorities.

Internet packet inspection

Because the Korean intelligence agency, the National Intelligence Service (NIS), not only has the right to collect secret information but also the power to investigate, it now conducts the largest number of telecommunications interceptions among the agencies, according to official government statistics. The statistics are aggregated using the data from telecommunications service providers who have offered data to the agencies. However, the statistics on interception conducted by the NIS using its own equipment have never been open to public scrutiny and are cloaked in secrecy.[5]

Table 2 shows the overall statistics for telecommunications interceptions in South Korea compared to NIS requests.

It was first known that the NIS had been monitoring the internet network and intercepting content by using deep packet inspection (DPI) in 2009. Monitoring the internet network in this way infringes basic human rights such as the right to privacy and freedom of expression and communication, as it allows the agency to monitor not only emails but all other interests of an internet user, including relationships and the financial life of a subject. Human rights NGOs, including Jinbonet, revealed the presence of internet packet inspection by the NIS at a media conference, held together with its victims. They also submitted a petition to the Constitutional Court when the NIS again conducted internet packet inspection in 2011 while investigating a person suspected of being in violation of the country's national security laws.

The NIS insists that it is impossible to investigate foreign-based emails such as Gmail without packet inspection, while it can investigate domestic internet usage by approaching service providers. The constitutional review is now underway.

Provision of personal information

It is a massive infringement of human rights that internet service providers (ISPs) provide personal information of subscribers or users such as name, ID, resident registration number, address, etc. to the agencies, without any restriction. This provision has faced severe criticisms, with allegations that it is abused by authorities who deliberately target internet users who criticise the government. The fact that there have been 9,574,659 cases of personal information provided in 2013 means that the personal information of 26,232 people was provided every day, and that the details of around 19% of the total national population have already been provided in South Korea. Table 3 shows statistics on the provision of personal information.

Conclusions

The reason why stored communication metadata is offered to law enforcement agencies is because the data is needed as evidence in investigations, and these requests by authorities are allowed. However, when a crime has not yet happened, the "reserved" location data of someone is not necessary

5 In 2005, the fact that the intelligence agency had monitored CDMA mobile phones was revealed by the government. The agency had officially denied all queries from NGOs, media and the national assembly for a long time. The intelligence agency had developed tapping equipment that could be attached to the wirelines of mobile communication service providers as well as the equipment for intercepting radio frequencies. See Jinbonet. (2009). *Mobile Surveillance and the Protection of Communications Secrets Act of Korea.* act.jinbo.net/drupal/node/6306

TABLE 3.

Provision of personal information by ISPs

Year	Prosecution	Police	NIS	Military investigative unit or others	Total
2010	1,323,176	5,419,365	76,018	326,233	7,144,792
2011	1,295,968	3,958,055	102,979	491,989	5,848,991
2012	2,241,812	5,115,131	110,923	411,722	7,879,588
2013	2,858,991	6,230,617	113,305	371,746	9,574,659

SOURCE: Government of the Republic of Korea

information which telecommunications service providers have to generate or keep in order to provide it to the authorities. The data is processed only to make it convenient for the agencies to electronically trace their subjects in real time. This practice goes against data protection norms which require that collecting and using any personal information should be the minimum necessary.

The data protection norms, including the country's Data Protection Act, grant many exceptions to the intelligence and investigation agencies. The data generated under these exceptions might also be used for the financial benefit of the service providers. Considering that the purpose of the constitution and international human rights law is to protect private life, personal information, and the privacy and freedom of communication from any governmental surveillance, the present legal system in South Korea, such as PCSA and the Data Protection Act, means that the government is infringing on these human rights.

Action steps

There is a serious communication surveillance crisis, not only in South Korea but throughout the whole world. As a UN resolution[6] pointed out in November 2013, it is necessary to improve domestic laws related to the protection of privacy, communication privacy and personal information in the digital age. It is essential to establish an independent body that supervises communications surveillance conducted by the intelligence agency and the investigation agencies. Neither the Personal Information Protection Commission and the National Assembly in South Korea have performed this supervisory role well enough.

Additionally, an international norm to regulate secret surveillance by intelligence agencies is needed in each country. As Edward Snowden revealed, as long as intelligence agencies across the world collect information by cooperating with or competing with each other, no citizen of any nation can be guaranteed privacy.

To achieve this, lawmakers in South Korea have to recognise the seriousness of communications surveillance and improve domestic laws. They also need to cooperate internationally to build proper international norms on the issue. Human rights NGOs will continue taking vigorous action to demand that these steps are implemented.[7]

6 UN General Assembly Resolution A/C.3/68/L.45/Rev.1 on "The right to privacy in the digital age", 20 November 2013. www.un.org/ga/search/view_doc.asp?symbol=A/C.3/68/L.45/Rev.1

7 Joint Statement by NGOs in the Republic of Korea on Intelligence Agencies' Internet Surveillance, 21 August 2013. act.jinbo.net/drupal/node/7636