Mobile Surveillance and the Protection of Communications Secrets Act of Korea

April 1, 2009

TEL +82_2_701_7687 FAX +82_2_701_7112 www.jinbo.net
서울시 서대문구 충정로 3가 227-1 우리타워 3층
Woori-tower 3F, 227-1, Chungjeongno 3-ga, Seodaemun-gu, Seoul, Korea

Mobile Surveillance and the Protection of Communications Secrets Act of Korea

Yeo-Kyung Chang, Jisung Kim
Korean Progressive Network, 'JINBONET'

Table of Contents

※ This report is produced as a part of a multi-national research project funded by the Open Network Initiative (ONI).

I. Political Backgrounds

Civil government and democracy were restored after a long period of military dictatorship by the 80's democracy movement in Korea. In 1997, political power was peacefully transferred to the opposing party by the presidential and the general election. Some anti-human-rights practices such as the censorship on films and records were reformed and the National Human Rights Commission (NHRC) was established. However, the basic administrative systems for surveillance and control on citizens like the resident registration system were maintained. The law enforcement agencies have been using the information and communication technologies (ICT) to surveil and suppress popular opposition toward the neo-liberal globalization and the corresponding market liberalization policies by the new government after the 1997 economic crisis and there have been growing concerns about a police state based on electronic surveillance technologies and practices.

An conservative authoritarian administration came into power by the presidential election in 2007. As the result of the 2008 general election, the government party took an overwhelming majority of the National Assembly. In April, 2008, the Korean Government hastily decided to lift a ban on the U.S. Beef imports right after it negotiated with the U.S. Government on the issue. As a reaction to the government decision, citizens attended candlelight vigils almost every night. At its peak in May, 2008, millions of people participated in the vigils. The government reacted to the civil action by violently repressing it with physical reinforcement, arresting more than fourteen thousand citizens and prosecuting them on criminal charges. The government and the government party are also pushing for amendments of human rights related laws to extend the government's power to watch over citizens such as expanding the surveillance authority of law enforcement agencies to mobile communication and the Internet.

While the legal protection measures against unlawful interceptions are in every aspects inadequate, there have been many unlawful interception incidents conducted by private entities causing controversies.

II. Developments in Mobile Communication Technologies and The Service Market

1. Mobile communication technologies

In 1984, the Korea Mobile Telecommunications Services Co. (renamed to SK Telecom) launched the first commercial mobile telephony service. It serviced through the 800MHz band using one of the first generation mobile telephony technologies, the AMPS cellular system which was also adopted in the North America. In 1996, SK Telecom launched the commercial CDMA based second generation digital mobile telephony service. In 2000, CDMA2000 1x (2.5G) service, in 2002, CDMA2000 1x EV-DO (3G), in 2006, WCDMA (3G) service by the SK Telecom (SKT) and the Korea Telecom Freetel (KTF), and in 2007, EV-DO Rev. A (3G) based service was introduced by LG Telecom (LGT) to the public in Korea.

Currently, both 2G and 3G technologies are used in services. Since SKT's T service and KTF's Show service were introduced in 2006 based on the WCDMA technologies, the number of 3G service subscribers is increasing

rapidly. In the case of KTF which invested in 3G service earlier than competitors, the number of 3G subscribers already exceeded that of 2G subscribers.

In addition to the advance of the mobile telecommunication technologies and public offerings of commercial services, there are other emerging mobile communication technologies and services that might compete with existing technologies and services such as WiBro. Commercial WiBro service was introduced in 2006 and provides broaderr bandwidth mobile data transmission. WiBro is better than WCDA and EV-DO family technologies in terms of data transmission speed but is behind the other two 3G technologies in mobility.

Table 1: Comparison between generations[1]

	1G	2G	3G	4G
Standard Technology	analog (AMPS, NMT)	TDMA, CDMA, GSM, PDC	WCDMA, CDMA2000, Mobile WiMax	WiMax evolution, 3GPP LTE, 3GPP2 UMB
Transmission Rate	~10kbps	9.6~64kbps	144~2Mbps	100M~1Gbps
Multiplexing	FDMA	TDMA, CDMA	CDMA, OFDM	OFDM
Market Introduction	1984	1995	2003~2006	After 2012
Major Services	voice	voice, SMS, low speed Internet	voice, high speed Internet, Video conferencing	high speed Internet, multimedia services
Multimedia Service[2]	unserviceable	6 hours 4 minutes	9 minutes 43 seconds	5.6 secons

WiBro service coverage is yet limited to Seoul and the nearby metropolitan area. In the long run, mobile. However, in the long run, as mobile high speed Internet services such as WiBro combines with Voice over IP (VoIP) services, it can cause competition with the mobile telephony services.

Table 2: Comparison between 4G technologies[3]

		LTE	UMB	WiBro+
Bandwidth		1.25-20MHz	1.25-20MHz	5-20MHz
Transmission Rate	Downlink	100Mbps	275Mbps	> 130Mbps (mobile) < 1Gbps (stationary)
	Uplink	50Mbps	75Mbps	>56Mbps
Method of Transmission	Downlink	OFDMA	OFDMA	OFDMA
	Uplink	SC-FDMA	SC-CDMA	OFDMA
Users per Cell		200 users	1000 users	-
Mobility		> 350Km/h	> 250Km/h	> 120Km/h
Cell Coverage		5/30/100Km	15Km	< 5Km 5~30Km 30~100Km
Duplexing		TDD/FDD	TDD/FDD	TDD/FDD
Latence		5ms (User Plane)	14.3ms	< 10ms

As the 3G services expands rapidly, the 4G services are heading toward increasing the data transmission rate.

1 2008·2009 Korea Mobile Yearbook. p.71
2 Time to download a 800MB movie file
3 2008·2009 Korea Mobile Yearbook. p.77

Such a technological development trend shows that the primary use of future services will move from voice to various multimedia services.

2. Market penetration and competition

According to the 2008 statistics by ITU, the population of Korea is about forty eight million. In 2007, the fixed telephone lines per 100 inhabitants is 46.44, the Internet users per 100 inhabitants is 76.80, and the broadband Internet subscribers per 100 inhabitants is 30.50. In 2008, the mobile cellular subscribers per 100 inhabitants is 94.24. As shown in the Table 3, while the number of fixed line telephone subscribers is stagnating, the number of mobile telephone subscribers is increasing, but the rate of increase is not so high. We can see the mobile telephone service market is getting closer to its saturation point..

Table 3: Korea Communication Commission, "Fixed-Mobile Communication Service Subscribers"

	2002.12	2003.12	2004.12	2005.12	2006.12	2007.12	2008.12
Fixed Line Telephone	23,490,130	22,877,019	22,870,615	22,920,151	23,119,170	23,130,253	22,131,737
Mobile Telephone	32,342,493	33,591,758	36,586,052	38,342,323	40,197,115	43,497,541	45,606,984
Paging	140,284	73,160	45,634	42,003	42,690	39,328	41,082
TRS	210,894	279,896	311,457	322,830	321,125	332,747	353,267
Wireless Data Communication	80,499	104,608	111,051	111,433	97,272	100,354	90,984
GM-PCS	0	0	0	0	0	4,412	3,897
Total	56,264,300	56,926,441	59,924,809	61,738,740	63,777,372	67,104,635	68,227,951

In the mobile telephony market, SKT takes about a half of the market. If looking at only the 3G services, KTF has approximately the same number of subscribers as that of SKT. With emergence of various bundled service such as telephone service bundled with IPTV or Internet connection, changes in the market share and structure are expected to happen, but the current market oligopoly by three operators, especially by SKT and KTF will not change in a short term. As the data transmission rate is getting higher with the introduction of 4G services and all the core communication networks moves from mix of circuit switching based networks and packet switching based networks to a unified IP based packet switching network with the next generation network, the current communication service market structure and competition developing around the mobile telephony services will face a significant pressure to change.

Table 4: Market Share[4]

	SKT	KTF	LG	전체
Subscriber Total	23,032	14,365	0	45,607
3G Subscribers	8,239	8,266		16,505
Market Share	50.50%	31.50%	18.00%	100%

4 from each operator's monthly report on its web site.

III. Case Analysis: Lawful and Unlawful Interceptions

1. Unlawful interceptions by the government

(a) Interception of phone calls in fixed-line telephony[5]

(1) Military regime period

The military regime paved a way to developing and deploying surveillance technologies. The Park Chung-hee administration which came to power by a military coup established a department specialized in wiretapping in the Korea Central Intelligence Agency (KCIA) which had twenty staffs and began wiretapping on fixed line telephones in 1961. In 1968, the department grew to be a group of sixty staffs and wiretapped about seven hundred thousand telephones. At the end of the Chun Doo-hwan administration, another military coup born, the fixed line telephone was popularized and the number of the fixed telephone lines reached ten millions. In that era, the Korea Telecom Authority was established and assisted wiretapping. Since 1988, the Roh Tae-woo administration which succeeded the Chun Doo-hwan administration put the Cheong Wa Dae, the office of the president, in the leading role of the nationwide information infrastructure developments and also invested resources in development of communication interception technologies.

In 1988 and 1989, there were controversies in the National Assembly during the annual parliamentary inspection of the administration over the so called 'Black Box' system which was suspected to be developed by the government for wiretapping. At that time, the opposition party argued that since the Chun Doo-hwan administration, “non-voice telecommunication transmission quality measuring systems” were deployed forty four places over the nation and the systems were the 'Black Boxes' used for wiretapping. Responding to the accusation, the National Assembly conducted an on-site inspection of the IMTC facility at the Kwang-hwa-mun Telecommunication Center on September 28, 1989, but the persons concerned denied the argument that the facility was a wiretapping device.

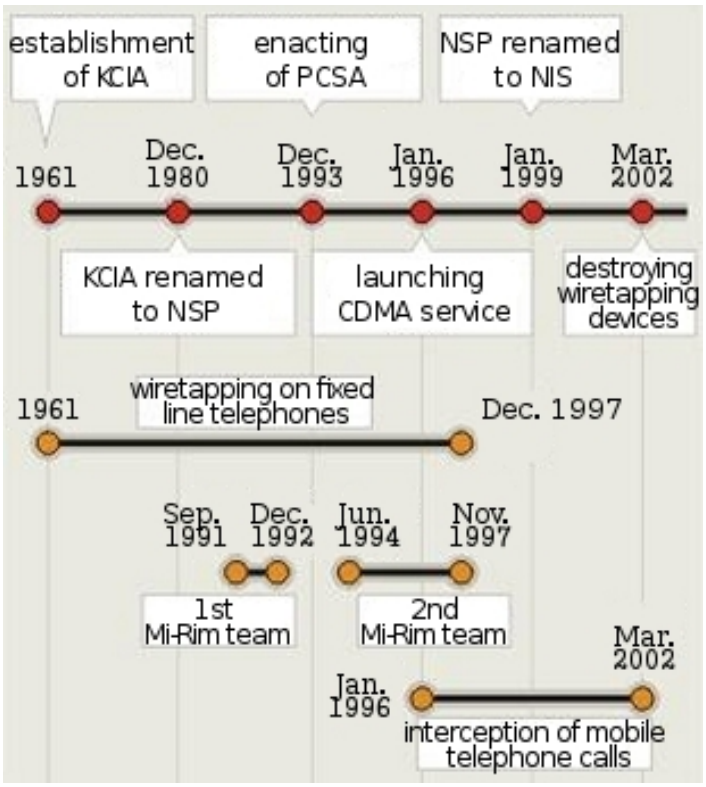

Figure 1: History of Interceptions

** source: Seoul newspaper 2005.12.15*

The surveillance system under those military regimes forced people to accept anticommunism and to internalize the surveillance. The military regimes pursued for routinizing surveillance by acquiring and

5 In the regard of this section, see Sung-Hak Ko. “Democratization of Korea and the Changes of Surveillance Power – Comparison between governments before and after democratization (한국의 민주화와 감시권력의 변화 - 민주화 이전 정부와 이후 정부의 비교)”, PhD Dissertation, Soong-Sil Univ., 2005.12.

developing new technologies in the technology side and to utilize such technologies, systemically established the government agencies such as the KCIA which became the Agency for National Security Planning (NSP) in 1980, the Defense Security Command, the public prosecutors, the police, and so on, and the subordinate agencies such as the post office and the Korea Telecom Authority in the institutional side.

The military regimes did not ensure individual's basic rights and freedom of express and association, while exercised state power arbitrarily. They seized the power by military coups. To overcome the crisis of political legitimacy and retain their power, they expanded their authority in surveillance and used state terrorism.

(2) Since the civil government restored in 1992

Just before the the fourteenth presidential election in December, 1992, the Minister of Justice and other heads of major government agencies gathered at a restaurant in Busan and they shared the idea to instigate regionalism and slander the opposition party's candidate to help the government party's candidate to win the election. The opposition party's candidate eavesdropped the conversation and revealed it to the press which caused a nation-wide shock. Mr. Kim Young-sam, the government party's candidate won the election and as soon as he became the president, he started a legislative process to enact a law to provide a protection against eavesdropping. In December, 1993, the Protection of Communications Secrets Act was enacted and provided a legal basis for communication interception by national security agencies and law enforcement agencies.

However, on July 21, 2005, audio recordings made through unlawful interceptions by NSP were exposed to the public by news reports. It shocked the nation. Despite the enactment of the Protection of Communications Act, the Kim, Young-sam government kept wiretapping since 1994 just like the military regimes. Finally, the suspicion that the NSP (renamed to the National Intelligence Service (NIS) in January, 1999) might have maintained its unlawful interception unit and kept intercepting unlawfully for the political purpose was proven to be true.

The Mi-Rim team, the secret eavesdropping unit of NSP, got details about meeting of targets from the Scientific Security Department which was in charge of the fixed line telephone wiretapping, and then the team went to the meeting place beforehand, installed transmitters, and eavesdropped on the conversation. The prosecutor confiscated 274 audio tapes and 13 volumes of transcriptions from the house of Kong Woon-young, the former leader of the team. According to the confiscated materials, there are 273 politicians, 84 high ranking government officials, 75 people in the press, 57 businessmen, 27 people in the field of law, 26 scholars, and 104 people in other areas among the victims of the unlawful interception.

The Scientific Security Department of NSP connected two or three telephone lines of the targets to NSP's lines each time and conducted unlawful interceptions one or two times every week at the Kwang-Hwa-Mun, Hye-Hwa, Young-Dong, Shin-Chon, Shin-Sa, and Mok-Dong telephone offices without court permissions. Since the wiretapping scheme needed cooperation from the telephone offices, it could not be conducted in a wider scale for security reasons. The prosecutors reported that nevertheless wiretapping and eavesdropping on important figures were executed without exception. The staffs at the telephone offices were paid from one hundred thousand won to five hundred thousand won each month in reward for keeping the unlawful acts secret.

(b) Appearance of interception of mobile telecommunications

There are roughly three categories of technologies for interception of mobile communications. The technologies

of the first kind are copying the target mobile devices or implanting a small eavesdropping device in the target device. The second kind includes intercepting airwaves which deliver signals between the target devices and the base stations. The technologies of the third category intercept the communication data (voice or other data) on the wire part of the mobile communication network. Theoretically a mobile communication data should pass through wire networks except for the case when the two mobile devices to communicate to each other are in a single cell, in other words two mobile devices use the same base station for their communication.

In this report, the technologies of the second and the third category will be analyzed. For intercepting airwaves, with the first generation mobile phones, basically you need only a radio scanner that can capture radio signals in specific bands. With the second generation digital mobile phones based on CDMA technology, in addition to a radio scanner, you need to know the codes for scrambling and spreading the signals. The law enforcement agencies and the intelligence agencies had insisted that it is impossible to eavesdropping on mobile communication because of this feature of CDMA technology until the prosecutors reported in 2005 that eavesdropping on airwaves and wiretapping of the wire part of mobile communication had been widely executed.

(1) Interception of 1G analog mobile communications

Since January, 1996, the Kim Young-sam administration had purchased four sets of analog mobile phone interception device from an Italian company and used them until the analog mobile service had been stopped in December, 1999. These devices were unlawfully used several dozen times every one or two months and the target phone numbers were entered at the interception sites

The device was portable weighing from ten to fifteen kilograms and being the size of a briefcase. A device can intercept six calls at a time. To intercept communication, the device should be located in the same cell with the target mobile phone. With the device, only one necessary information was the phone number of the target phone.

Besides the NSP, multiple government agency such as the Supreme Public Prosecutor's Office (SPO), the National Police Agency, the Ministry of Defense illegally imported eavesdropping devices from private companies without government permission. On October 24, 2005, in a hearing by the Special Committee on Budget and Accounts, the Minister of Justice at that time disclosed that SPO had purchased and used eight analog mobile phone eavesdropping devices by Mar, 1995. Three of the eight devices were made in the U.S.

It is noteworthy that purchase of communication intercepting devices were increased rapidly between 1996 and 1999. There is no evidence that crimes suddenly happened more frequently during the period. The period can be characterized by the socio-economic events like a change of regime by the presidential election and economic unsuitability by the crash of financial system known as the IMF situation in Korea. In addition to such peculiarity of that time, the amendment of the Act of the Agency for National Security Planning in December, 1996 is assumed to be a factor to increase the demand for the communication interception devices. The amendment resurrected the investigation power of NSP into the crimes provided in Article 7 (appraising/inciting and etc.) and Article 10 (failure to notify) of the National Security Law which were vulnerable to political abuse and could violate human rights.

Table 5: The Ministry of Information and Communication's 2005 Report to the National Assembly

	1994 ~ 95	1996	1997	1998	1999	2000	2001	2002	2003	2004	2005 .7	Total
Downer Information and Communicati	–	10	10	5	10	8	10	8	8	14	10	93

on												
Korea Delcom	–	210	307	114	175	–	–	1	2	4	–	813
Others	1	–	–	–	–	–	–	6	2	–	2	11
Total	1	220	317	119	185	8	10	15	12	18	12	917

(2) Interception of 2G digital mobile communications

It was revealed that the administration of Kim Dae-jung who was the first presidential candidate who ever won the election as an opposition party candidate kept conducting unlawful interceptions. In 1998 and 1999, the Kim Dae-jung administration kept assuring the public that interception of phone calls made with the CDMA mobile phones was technologically impossible, while the administration developed CDMA mobile communication interception devices by itself. In January, 1996 when the 2G digital mobile service was launched, NIS developed two communication interception systems; R2 (developed in May, 1998) for intercepting communications on the wire relaying part of the mobile networks and CAS (developed in December, 1999) for intercepting communications over the airwaves. The Department Eight of NIS was in charge of the use of both systems and use them for interceptions.[6]

A CAS system should be located near the target phone and can be used for intercepting relatively small number of targets at a time, while an R2 system was able to deployed for far larger number of targets at a time at a relatively low cost. However, to use an R2 system, there was a risk that third party other than the targets and the agencies can notice that interceptions are going on because the system must be installed physically in a telephone office. Therefore, the R2 system is not the desirable system for the case when the interception should be kept secret from the target and others.

(3) Interception of 2G digital mobile communications on the wires

According to the investigation report from the Public Prosecutor's Office in 2005, R2 system was developed with the budget of 1.4 billion wons in total for its development. Around May, 1998. the first set of the system was developed and deployed for action and in September, 1999, another 5 sets were added.

An R2 system was installed in a telephone office where the Mobile Switching Center (MSC) and the Interconnection Gateway Switch (IGS) are located, connected to a line that was split from a trunk line in the wireless-to-wire relay networks, and intercepted phone calls pass through the relay networks. Many phone calls with different phone numbers happens on a relay network. It was possible to intercept all the phone calls with a single R2 system on a relay network. R2 system was named after the signaling protocol (R2 signaling) for the most of switches in a relay network at that time.

An R2 system could be connected to 600 different lines at its maximum and intercept 64 lines at a time. In other words, the input to the system was 600 lines and the output of it was 64 lines. Since six systems were deployed, it was possible to connect to 3600 lines. The system has two operation modes; In one mode, it intercepts only the phone calls with specific phone numbers that entered by operators and in the other mode, it can intercepts phone calls randomly. The NIS intercepted phone calls by 1800 major public figures including politicians, journalists, public officials, leaders of civil organizations and trade unions around the clock.

6 "국정원의 과거 불법감청 실태 발표문(요약)", Hankyoreh newspaper 2005.8.5; "임동원・신건씨 감청장비 개발에도 관여", Yonhap news 2005.12.2; "수사발표서 등장한 도청장비・용어", Yonhap news 2005.12.14; "중정・안기부 36년간 전화국 `관리'", Yonhap news 2005.12.14; "도청정보 이용한 김현철씨도 도청당해", 동아일보 2005.12.15.

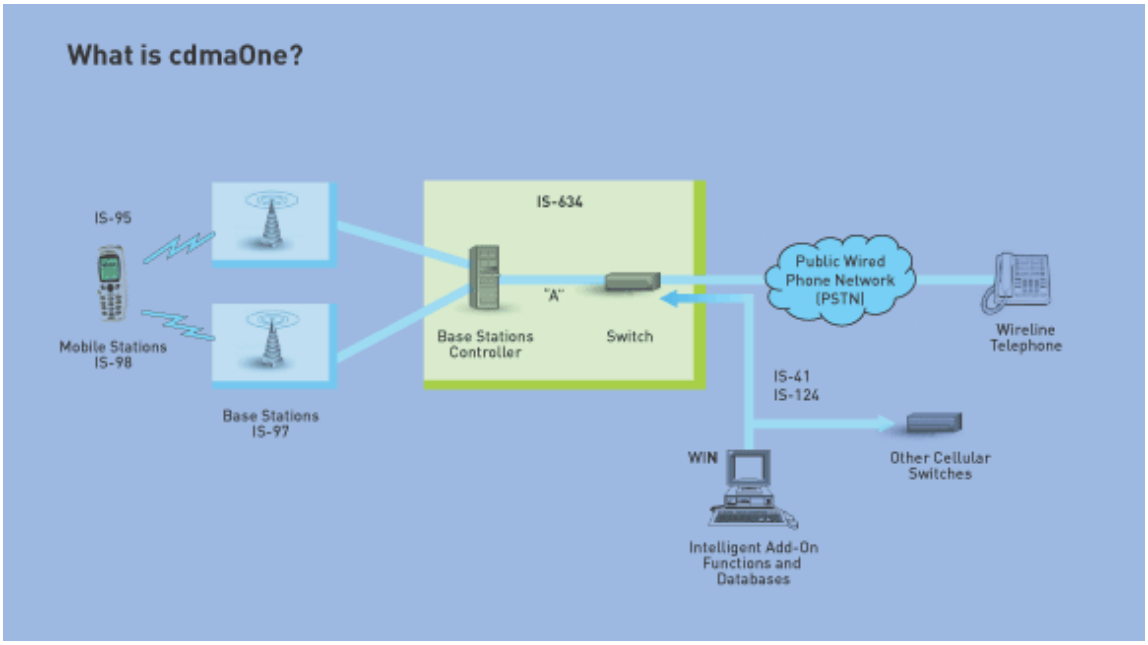

Figure 2: 2G CDMA (cdmaOne) Network Diagram (source: CDMA Development Group, "2G-cdmaOne")

A 2G digital CDMA network diagram depicted in Figure 2 will help us in understanding the methods of interceptions of communications relayed over the wires by the R2 system. The CAS system that will be explained later takes advantage of the security weakness in the wireless connection[7] between a mobile station (MS) and a base station (BS)[8]. Interceptions using the R2 system seemed to happen on the trunk line connecting the Switch[9] and the Public Wired Phone Network (PSTN[10]) in the diagram. Multiple BSs are connected to a Base Stations Controller (BSC), again multiple BSCs are connected to a Mobile Switching Center (MSC). If a mobile phone user makes a call to someone on a fixed-line telephone or a mobile phone, the call signal always have to be delivered to a MSC before the signal reaches the other party. Physical connections between MSCs and between a MSC and the PSTN are usually optical cables. R2 system was attached to an optical cable split from such cables.

(4) Interception of 2G digital mobile communications over the airwaves

According to the investigation report from the Public Prosecutor's Office in 2005, the NIS developed the CDMA Analysis System (CAS) with the development budget of 1.9 billion wons around December, 1999. the NIS built 20 sets of the system and deployed them for interception. NIS installed a system on a car and approached the target within 200 meters to intercept communications. To intercept the airwaves and unscramble the signal, they needed to know the frequency and ESN of the phone and the location of the BS. The system was in use from May, 2000 to April, 2001.

The CAS system is possible because the codes used for spreading signals and scrambling them in physical layer of the CDMA was obtainable through monitoring the airwaves.

As the Protection of Communications Secrets Act was amened in December, 2001, the procedure to have and

7 The standard for the wireless connection is IS-95 in 2G CDMA. The core technology of 2G CDMA deployed in Korea was developed by the Qualcomm, a U.S. Company and it is commercially branded under the name of cdmaOne.
8 Also called Base Transceiver Station (BTS)
9 When it is acting as a switch between mobile communication networks, it can be usually called a Mobile Switching Center (MSC). When its role is to relay wireless communication to PSTN, it is called a gateway.
10 PSTN stands for Public Switched Telephone Network.

use communication interception devices was also getting stricter and a controversy over the unlawful interceptions before the sixteenth presidential election flared up, NIS dissolved the the interception team and destroyed all the interception devices including R2 and CAS systems in March, 2002.

(c) Technical aspects of the 2G mobile communication interception by the airwaves

(1) Built-in physical layer security features of the CDMA technology: Spreading and scrambling

In wireless communications, multiple terminal devices such as mobile phones should share a specific band of radio spectrum and time to communicated with BS. To accomplish such sharing and avoid conflicts, there needed to a way to distinguish each terminal device that wants to communicated with the same BS. The problem of multiple terminals connecting to a base station is called the "multiple access" problem. To overcome the multiple access problem, different strategies (or technologies) are in use. For the 1G analogy mobile phones, the Frequency Division Multiple Access (FDMA) method has been used, for the 2G GSM services which was popularized in Europe, the Time Division Multiple Access (TDMA) method has been used, and for the 2G CDMA services which has been the primary type of the 2G services in Korea, the Code Division Multiple Access (CDMA) has been used. With FDMA, each user uses a different sub-band of the whole radio band, with TDMA, each user uses different time slots, and with CDMA, each user uses a different spreading code unique to the terminal. The current 3G mobile telephony technologies such as CDMA200 and Wideband CDMA (W-CDMA) are using CDMA multiple access methods. In this section, we will discuss the details of the CDMA technology, especially the IS-95 standard that has been used for the 2G CDMA services.

CDMA is based on spread spectrum technologies. A spread spectrum technology spread signals over a broader band than the original signals need. To achieve the spreading, a conversion from narrow band signals to broad band signals is needed. With CDMA, spreading codes are used for the conversion.

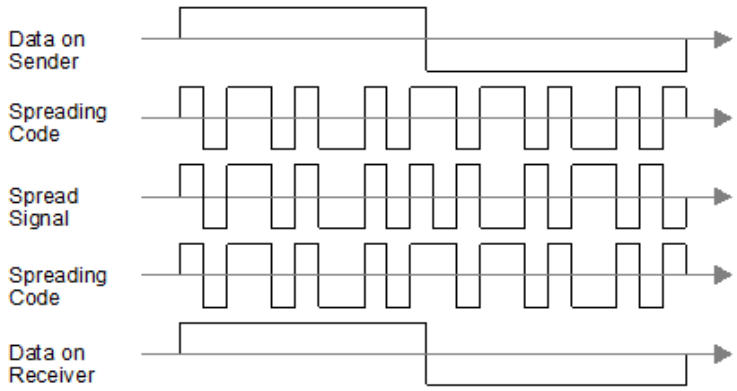

Figure 3: Spreading

In Figure 3, if the sender sends '1' and '0' in the process of communication between the terminal (MS) and the

BS, the signals transmitted over the airwaves are not the '1' and '0'. What you can get from the signals transmitted over the airwaves are the Spread Signal that is spread by the Spreading Code. Therefore, even if someone intercept the signals over the airwaves, he/she can not recover the original data, '1' and '0' without knowing the Spreading Code.

In addition to this spreading feature, IS-95 usually incorporate scrambling process in its signal processing before the actual air-wave transmission to improve the data security. Scrambling means converting a signal sequence into another sequence using a pseudo-random sequence that is very hard to guess. After scrambling, the signal sequence is much more like noises to someone who does not know the pseudo-random sequence used for scrambling. Therefore, if someone wants to intercept the wireless communications under IS-95, he/she should know the code for spreading and the code for scrambling at the same time.

These features were the bases for governments to claim intercepting the wireless communication in 2G digital CDMA telephony is impossible before the 2005 public prosecutor's investigation.

(2) Possibility of IS-95 wireless communication interception

Dae-Hyun Ryu and Sueng-Ju Jang reported in their 2003 paper, “An Enhanced Mechanism of Security Weakness in CDMA service”, that they succeeded in IS-95 wireless communication interception. They could successfully intercept the forward link communication which is signal transmission from a BS to a terminal.

In CDMA, the wireless communications between BSs and MSs are divided into the forward link and the reverse line depends on the originator of the transmission. If the transmission originated from a BS, it is a forward link and the data flows from the BS to an MS. If the transmission originated from an MS, it its a reverse link. These two links are also logically divided into different channels based on each channel's functions. Such logical division scheme does not only apply to IS-95 but also to 3G CDMA technologies with some differences such as types of channels. In IS-95, the forward link is divided into pilot, sync, paging and traffic channel. The reverse link is divided into access and traffic channel. Each channel has different functions, and different spreading code and scrambling sequence if the channel is subject to spreading and/or scrambling.

In the case of the traffic channel of the forward link, a signal sequence is first scrambled by a long code and then channelized by a Walsh code. The traffic channel of the reverse link is modulated by a Walsh code and then spread by a long code. The long codes for these purposes are the public long code and the private long code. The private long code is usually used for voice security.

The masks for generating the public long code and the private long code are structured as in Figure 4.

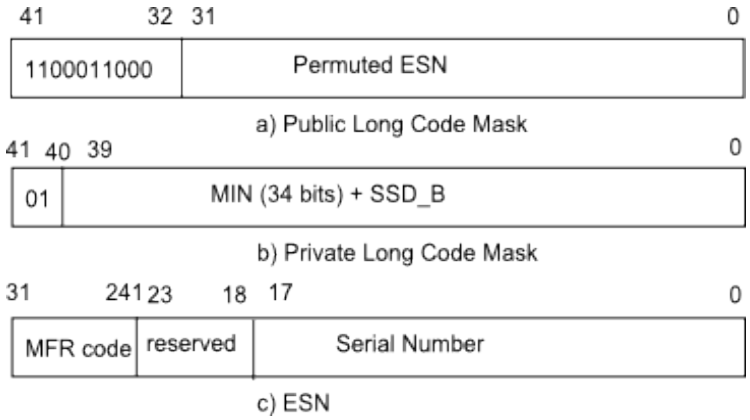

Figure 4: Long Code Mask Format in the Traffic Channel

In the paper, the authors can get the long code for the traffic channel by figuring out MIN and ESN transmitted over the access channel and the paging channel.

The paging channel is first spread by the Walsh function and then scrambled by the paging channel long code mask. The access channel is spread by the access channel long code mask. You can see two long code mask structure in Figure 5.

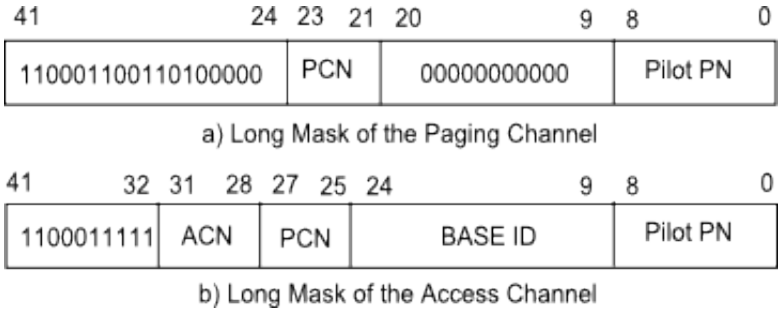

Figure 5: Long Mask for the Paging and the Access Channel

The authors can get the Pilot PN value by monitoring the pilot channel. The Paging Channel Number (PCN) is three bit value between '000' and '111', and generated by a hash function with known value. Therefore, PCN was easily obtainable. BASE ID of the access channel can be obtained by monitoring the sync channel. The Access Channel Number (ACN) was obtained from the paging channel.

The MIN and SSD_B part of the private long code is always the same with the same phone number. The ESN of the public long code is simply a recombination of ESN data.

The paper suggests that if you know the phone number and ESN, one can easily intercept voice traffic over the 2G CDMA wireless communication and even if you do not know the ESN and the phone number, you can still intercept voice traffic by monitoring the paging and the access channel.

(d) Network operators involvement in unlawful interception by the government

In the cases of unlawfully interceptions by the governments, the telecommunication providers cooperation was essential.

In addition to their cooperation in installation of illegal interception devices into their communication facilities and provision of split lines on requests from NSP, the telecommunication providers routinely assisted law enforcement agencies' unlawful interception requests, which was pointed out by the Board of Audit and Inspection (BAI). On May 12, 2000, BAI released a report, “Audit report on Operation Conditions of the Communication Restriction Measures.” In this report, BAI pointed out the unlawful interception by government agencies and cooperation of telecommunication providers as well. The staffs at the telephone offices accepted interception requests and assisted interception without checking court warrants, and did not record the interception activities in their maintenance logs. In some cases, the providers provided passwords and identification keys of the mobile phones, pagers and voice mails to the agencies instead of sending stored messages to the agencies. With such information, agencies could intercept

communications even after the authorized period of time by the courts.[11] The providers also cooperated with the agencies for emergency interceptions which were allowed for only 48 hours without checking the authorization documents or for interceptions extended over the authorized period of time. Even after the authorized period of time expired, some wiretapped lines remained for interceptions. Another problem was that even with the emergency interceptions any staff of the agencies who is not eligible performed the interceptions. Government officials who are eligible for the request of emergency interception are limited to over certain class officials in the public prosecutor's office, the police, NIS and the Ministry of Defense. But there were many cases that arbitrarily ordinary staffs of the public prosecutor's office, minor policemen or common soldiers were assigned to the interception tasks.

In August, 2003, it was revealed that the public prosecutors and the police unlawfully inquired call data of telecommunication service subscribers without proper legal procedures. According to Rep. Young-Se Kwon (Grand National Party HANARA) at that time, there were 1,966 cases of call detail inquiry without a chief public prosecutor's prior or ex post authorizations that were required by the Protection of Communications Secrets Act. Later, the Ministry of Information and Communication disclosed that chief public prosecutors authorization letters were sent to the telecommunication providers for 1,191 cases among the 1,966 cases after Rep. Kwon brought up the problem, and requested investigations for the rest cases, 704 cases of the police, 62 cases of the public prosecutors, 8 cases of the Ministry of Defense, 1 case of the Customs Office. The police and the Public Prosecutor's Office explained most of their cases caused by errors and mistakes. However, it aroused a public controversy that telecommunication providers accepted the call detail inquiry requests not following the legally required procedures.[12]

2. Lawful interceptions and information handover

In Korea, lawful interception and information handover take place as follows. First, investigative agencies such as public prosecutors, the police, NIS present court warrants to the service providers and request cooperation according to the Protection of Communications Secrets Act for the call content interceptions of fixed line telephones. However, since information such as SMS messages, e-mail messages and articles on closed group bulletin boards are not real time communication information and not protected by the Protection of Communications Secrets Act[13], such information is collected by seizure procedures which were pointed out problematic.

Handover of communication activity verification information such as identification of the other party, the date and time of calls, the location of a call and Internet activity log information such as IP addresses are also subject to the same procedure as for the fixed line telephone related procedures. But since certain call data such as name, telephone number, resident registration number, address, Internet ID, and etc. which can reveal the identity of a subscriber are not protected by the Protection of Communications Secrets Act, information and law enforcement agencies can get such information simply by written requests.

The following subsections will discuss details and show statistics of interception activities.[14]

---

11 From January 1, 1997 to June 30, 1999, 14 telecommunication service resellers handed 3,494 passwords over to law enforcement agencies with 2,388 requests. Even after BAI noticed it, unlawful activities continued. According to the May, 2005 MIC report, 4,050 passwords of mobile phone and voice mail accounts was provided to the agencies instead of submitting printouts of messages in the voice mail in-boxes or mobile phone message boxes.다.

12 Yonhap news 2003.8.3.

13 대판 2003. 8. 22, 2003도3344. But the cases related with this kind of information handover are included in the statistics from MIC and the Korean Communications Commission.

14 The interception and handover statistics is reconstructed from the materials published twice a year by MIC and the Korean Communications Commission which succeeded MIC according to “The Guide for Tasks Related with Electronic Communication Interception and Communication Information Handover (전기통신감청 및 통신자료제공 관련업무 처리

(a) Communication interception

According to Figure 6, on the surface, communication interception cases decreased because the written requests were declining. Especially mobile interceptions disappeared since 2005.

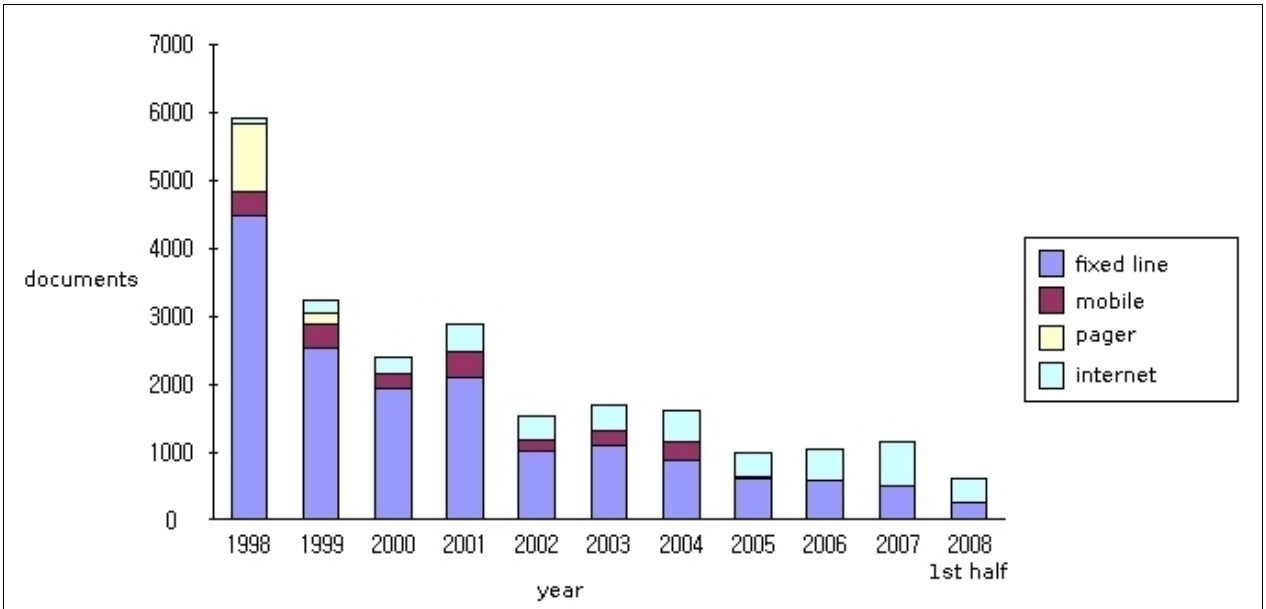

Figure 6: Number of Written Requests

However, if reanalyze interception activities not by the number of written requests but by telephone numbers or IDs, the number of telephone numbers and IDs per each document is increased. As a result, the number of interceptions increased overall. Particularly interceptions done by NIS took a large portion of all interception activities. In 2007, among 8,803 all cases 8,628 cases were done by NIS, and it is about 98% of all activities.

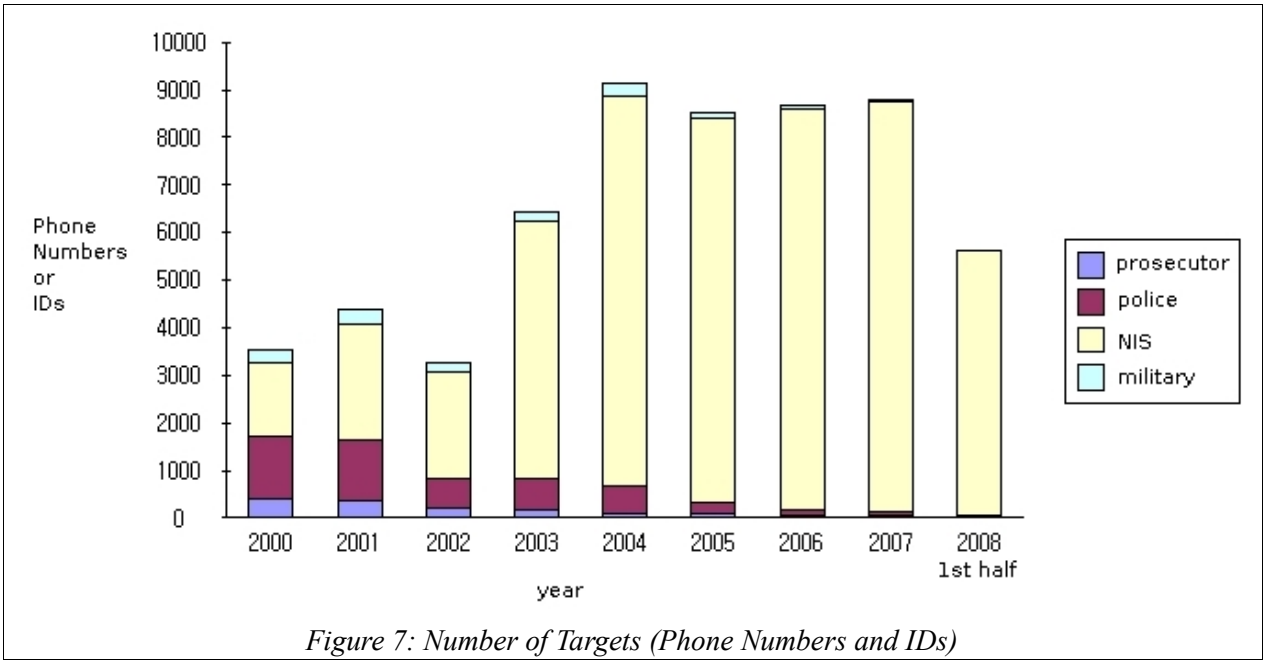

Figure 7: Number of Targets (Phone Numbers and IDs)

지침)" revised in June, 2000.

(b) Handover of communication activity verification information

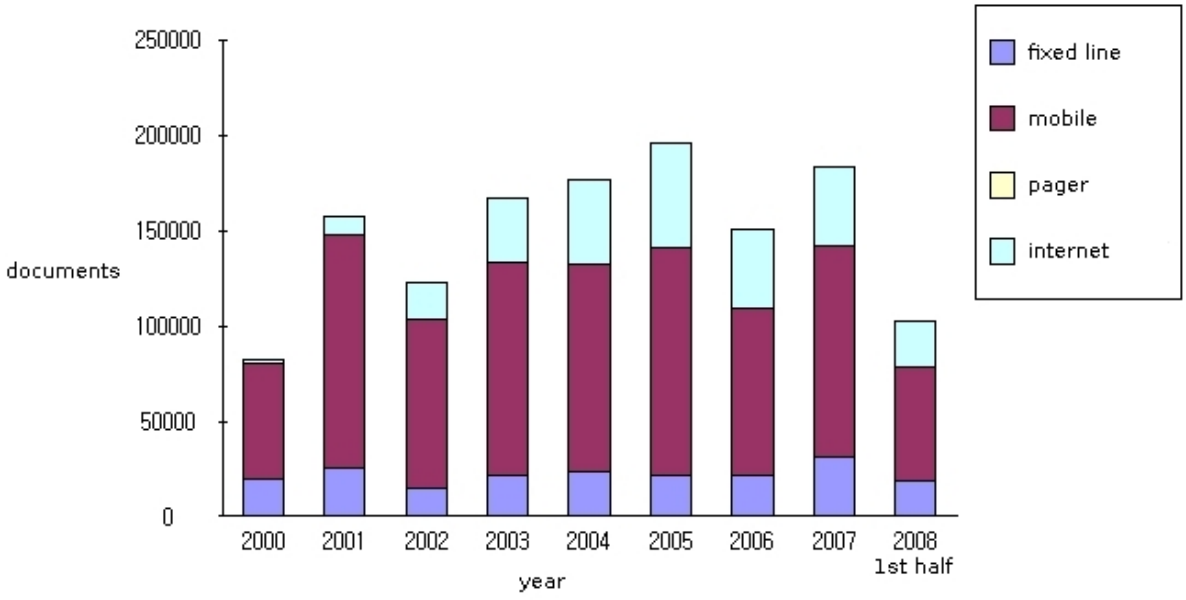

Figure 8: Number of Written Requests for Communication Activity Verification Information Handover

The number of communication activity verification information handover cases were temporarily declined in 2006. That was possibly because the amendment of he Protection of Communications Secrets Act on August 27, 2005 required a court warrant instead of a chief public prosecutor's authorization for the communication activity verification information request procedure. It is also noticeable that requests for communication activity verification information mobile phones are very frequent overall.

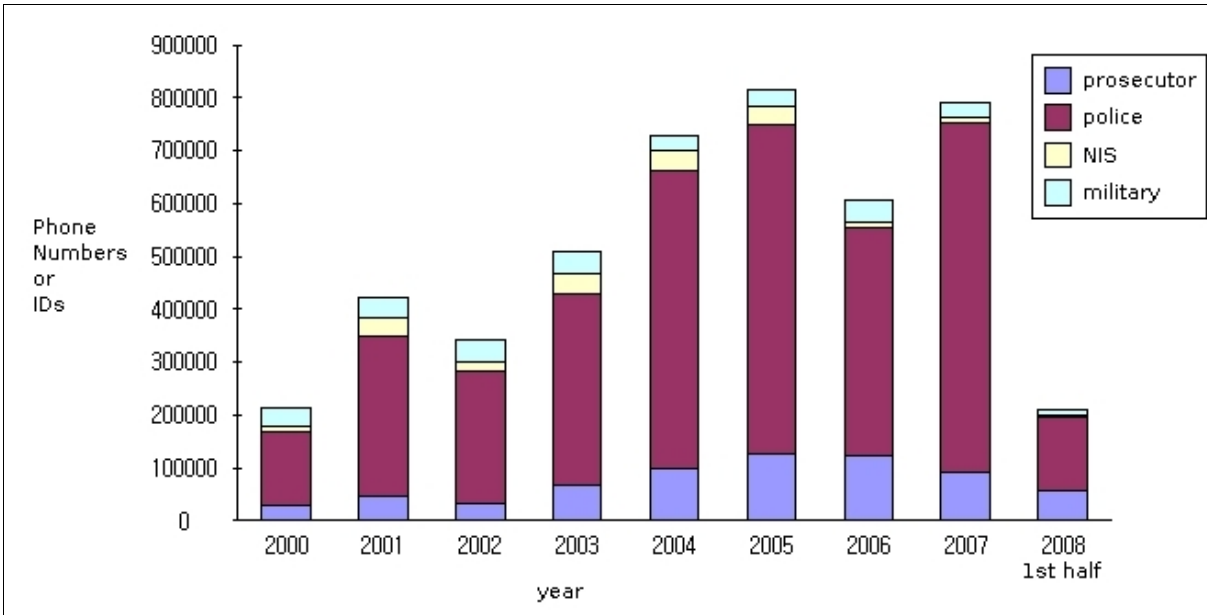

Figure 9: Number of Targets of Communication Activity Verification Information Requests

In addition to the amendment of the Protection of Communications Secrets Act by the National Assembly, in 2005, the administration revised the ordinance of the Protection of Communications Secrets Act imposed obligation to retain communication activity verification information. The retention period for information related with local and long distance phone calls is 6 months, for information related with mobile phone calls 12 months, and for information related with the Internet 3 months in the ordinance. The revision of the ordinance did not based on its parent act and

has been a subject for criticism because the provisions treats all subscribers as potential criminals.

(c) Handover of communication data

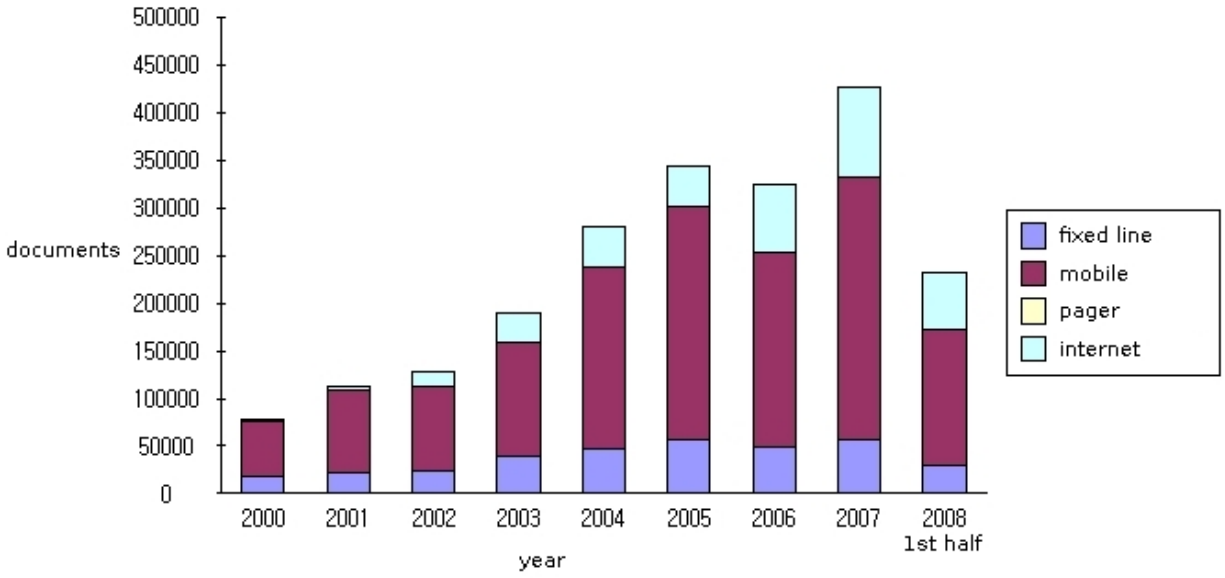

Figure 10: Number of Written Requests for Communication Data

The number of handover cases of communication data that include personal identification information such as names, phone numbers, resident registration number, addresses, Internet Ids and etc. rapidly increases in 2007, especially in the cases related with the Internet activities. If you take a look at the number of information items such as phone numbers and Ids, the total number passed over four millions. This increase seems to be a consequence of the nation wide mandatory real name policy that was applicable to 37 major Internet sites in July, 2007. The sites such as Yahoo Korea, Daum Communications, and DCInside began to collect real name information since the introduction of the real name policy.

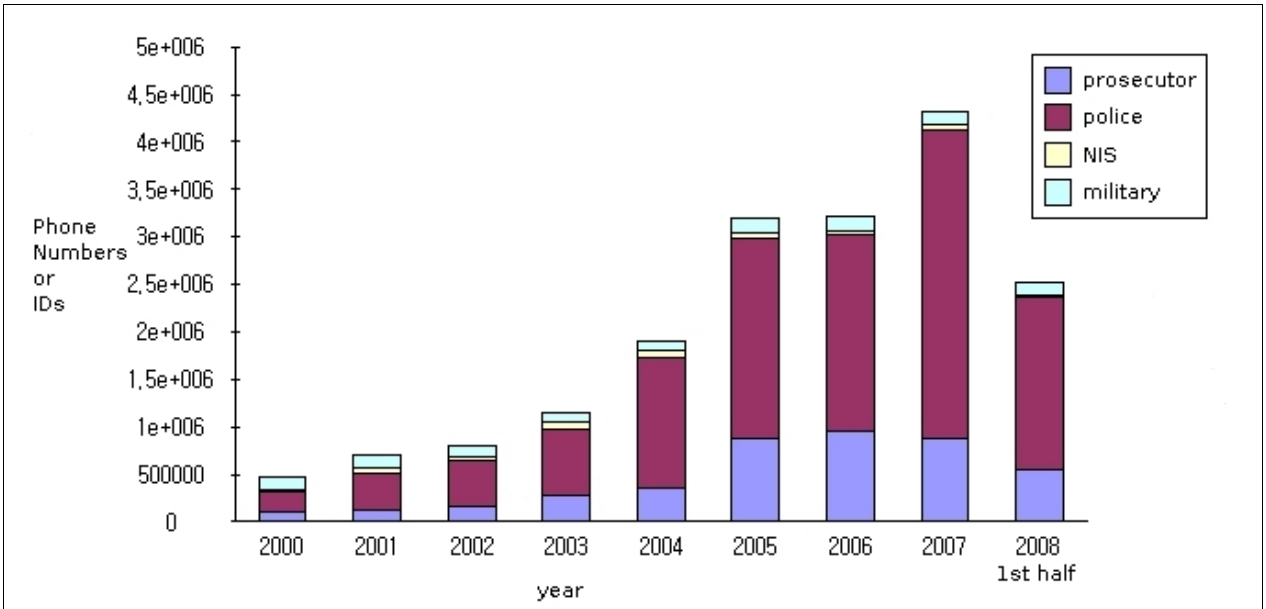

Figure 11: Number of Targets of Communication Data Handover

(d) Abuse of information handover procedures

Even when the communication interception or handover of communication activity verification information had been carried out according to appropriate procedures, there were cases that investigative agencies abused them, for example, inquiring call details of news reporters who frequently had reported stories of the agencies.

In October, 2003, the Central Investigation Division at the Supreme Public Prosecutor's Office frequently inquired call details of the news reporters' mobile phones whose news covers mainly the Supreme Public Prosecutor's Office, and the primary purpose of such inquiry was to find out who leaked investigation information of major criminal cases. It was known that the Supreme Public Prosecutor's Office tracked down the leakers by comparing incoming and outgoing calls of mobile phones of the prosecutors or the investigators and those of the news reporters who reported investigation information just after the Supreme Public Prosecutor's Office started the investigation of the secret fund of Hyundai Group.

In January, 2004, NIS inquired call details of the news reporters to verify possible security breaches in the National Security Council (NSC) and the Ministry of Foreign Affairs and Trade. It caused a public outrage especially because the inquiry was conducted not by the Investigation Department of NIS that was required to get a permission from a chief district public prosecutor to conduct such inquiry but by the Counter-terrorism Security Department of NIS that needed only the authorization from the NIS director. The Science, Technology, Communications & Information Committee of the National Assembly visited SKT, KTF, LGT in turn and conducted on-site investigation on handover of communication activity verification information. However, the companies refused to submit materials to the committee on the grounds that such submission violates the Telecommunication Business Act and the Protection of Communications Secrets Act, and the on-site investigation fell apart.

In January, 2009, the public prosecutors and the police call details inquired call details of the news reporters who reported the 'written request for dealing audit results' to the Ministry of Defense. They also inquired call details of two news reporters who reported the 'written request for dealing audit results' to the U.S. Forces Korea Base Relocation Office at the Defense Ministry in June, 2008.[15]

15 Yonhap news 2003.10.6; Hankyoreh newspaper 2004.1.30; Hankyoreh newspaper 2004.2.15; Hankyoreh newspaper

3. Unlawful interception by private entities

The government kept denying the possibility of interception while the information or law enforcement agencies continued to unlawfully intercept communications even though there are communications secrets protection measures under the Protection of Communications Secrets Act until August, 2005. Taking advantage of gaps in regulations, private entities also have actively pursued opportunities for unlawful interception for their own interests. As the number of mobile users increased, the number of unlawful interception cases also increased. Most common and increasing practices of unlawful interceptions were eavesdropping on conversations over phones, peeping at SMS messages and tracking the location of the users by copying the mobile phones.

Crimes related with illegal copies of mobile phones were recognized social problems since early 2000. In June, 2001, a ring of criminals who collected lost mobile phones and copied them to sell in and out of the country was arrested, and in November, 2002, offenders who bought mobile phones under the names of credit defaulters and sell them were rounded up. In February, 2003, a group of criminals who made one thousand "clone phones", subscribed to a paid mobile phone location tracking service, "Locate My Friend" service, using the phones, and used the service to track down female employees who ran away from decadent entertainment establishments were arrested. Similar incidents follow one after another.[16]

In July, 2004, it was revealed that SAMSUNG had traced locations of its employees who sought to form a trade union and families of employees who were victims of industrial accidents, using mobile phone location services for at least three months 20 to 40 times a day without letting them know they are traced. All the victims of the location tracking service were related directly or indirectly with establishment of the trade union and the place where the tracking service happened was the SAMSUNG SDI factories in Ulsan and Suwon, but the owner of the mobile phone used for tracking service died 11 months before. The victims submitted a letter of complaint to the Seoul Central District Prosecutors` Office arguing that SAMSUNG traced their location using illegally copied mobile phones. In February, 2005. the public prosecutors said that it was a fact that 'someone' copied the phones of the complainants, but they could not find who did that, and they decided to dismiss the case.[17]

According to the Central Radio Management Office (CRMO) of the Ministry of Information and Communication, the number of illegal copies of mobile phones that was picked up had been increasing from 858 in 2004 to 6,574 in January, 2006, which was about 7.7 times larger than the number in 2004 and was the largest ever number since CRMO had been given juridical authority in 2002 and began to crackdown on illegal clone phones. The number of clone phones which were used for crimes was 14 in 2003 and the number reached 91 in 2006. The 91 phones were picked up while trying to turn the lost phones to exact copies of the offenders' phones. The number of illegal interception devices is steadily growing at 2 cases in 2004, 45 in 2005, and 54 in 2006.[18]

As the problem got serious, the government took preventive measures like running a mobile phone simultaneous receiving protection program, prohibiting electronic serial number (ESN) provision by revising the Protection of Communications Secrets Act, introducing mobile phone authentication services, and tightening up the enforcement. In March, 2005, mobile phone authentication service was provided for new mobile phone free of charge, and fraud management system (FMS) was introduced. Introducing such measures against illegal copying, the government

2004.2.17; Yonhap news 2009.1.22.

16 See Kookmin Daily 2001.6.26; Yonhap news 2002.11.5; Hankyoreh newspaper 2003.9.25

17 See Hankyoreh newspaper 2004.7.11; Hankyoreh newspaper 2004.7.14; Hankyoreh newspaper 2004.7.22; Yonhap news 2005.2.16; Hankyoreh newspaper 2005.2.16

18 See Yonhap news 2006.1.16; inews24 2007.4.30

assured that mobile phone eavesdropping was not possible. Still, the public concerns over unlawful interception grew ever bigger because of the revelation of NSP's unlawful interception activities in July, 2005 by the public prosecutors. Finally, the government acknowledged that it was possible to intercept mobile communications in August, 2008 and announced a plan to improve mobile communication security. The plan included a new encryption scheme, authentication service for both call origination and arrival, and at the same time building up enforcement strength. Later, the Ministry of Information and Communication and the mobile telecommunication service providers agreed to launch paid encryption services that used the private long code to scramble the voice traffic and authentication services so that if the network authentication key did not match the mobile phone's authentication number, the communication link automatically shut down.[19]

In addition, the government established a reporting center for illegal copied mobile phones and a cash-reward system for reporting, which was called "phone-parazzi"[20]system since March, 2006. According to the statistics of June, 2006, 1,500 illegally copied phones were reported and eleven million two hundred thousand won was paid to 15 people who reported to the center. CRMO ran a street campaign under the banner saying "Do Not Illegally Copy Mobile Phones".[21]

Nevertheless, three employees of a courier company sneaked a look at the SMS message of a top actress by copying her mobile phone were caught. The entertainment company with whom she had a management contract which was about to expire is suspected to have copied her phone to monitor her activities. After this incident, the National Assembly is considering to revise the Telecommunication Basic Act that mandates the mobile telecommunication service providers to report to the Korea Communications Commission when they detect any mobile phone number which is suspected to be a copy. [22]

IV. The Protection of Communications Secrets Act

1. Enactment

The article 18 of the Constitution of Korea says "The privacy of correspondence of no citizen shall be infringed." After years of surveillance and eavesdropping against human rights under the military regimes, in December, 1993, the Protection of Communications Secrets Act was enacted. The purpose of the Protection of Communications Secrets Act is stated "This act aims to limit the subjects of any restriction on the secrets and the freedom of communications and conversation and to ensure such restrictions to follow strict legal procedures so to protect the secrets of communications and increase the freedom of communication".

The Protection of Communications Secrets Act does not allow anyone to censor mail, intercept electronic communications, handover communication activity verification information, or record or listen to private conversations between third parties unless he/she was authorized by the provisions in the Protection of Communications Secrets Act, the code of criminal procedure or the court-martial law. (Article 3) A public prosecutor, a policeman or a head of an information agency should limit censoring mail, intercepting communications or

19 See MIC press release 2005.2.16; Segye Ilbo 2005.8.16; Yonhap news 2006.10.19; Yonhap news 2007.1.23; KOOKINEWS 2007.1.15

20 The word is a mixture of word "phone" and word "paparazzi".

21 See Yonhap news 2006.3.16; Hankook Ilbo 2006.6.8; MIC press release 2006.6.12; inews24 2007.4.30

22 See Hankyoreh newspaper 2009.1.19; Yonhap news 2009.2.9

recording/listening to private conversation only to the cases where such investigation methods are necessary for criminal investigation or national security and meet the legal requirements provided in the act, and stop such communication restricting activities immediately if such activities are decided not to be necessary any longer even they got permissions or authorization according to the act so that infringement of the privacy of citizens remains at the minimum. (article 2 of the ordinance)

In the act, “communications” means mail and electric communications, “interception” means obtaining or recording the content by receiving or reading sounds, texts and speech, symbols, or images with the use of electronic or mechanical devices, and also means obstructing transmission or reception of electronic communications. (article 2) According to the definitions, the electric communications include telephones, facsimile and telegraphs. Mobile phones and personal mobile communication also belong to electric communications. Transmission of data or information over the computer networks is electric communication. Originally, there was no regulation on communication activity verification information such as call details or Internet activity logs in the act while the Telecommunications Business Act provides some regulatory ground for such information. However, As the importance of the verification information gained more public recognition, the Protection of Communications Secrets Act included the verification information as a subject of legal protection. In 2005, law enforcement agencies became required to obtain a court warrant before requesting handover of communication activity verification information by revision of the act.

The conditions for interception permission are that there is a good reason to suspect the crime is under planning, under execution, or executed, and it is difficult to deter the crime, arrest the offenders, or collect evidences with other methods. When the conditions are met, the court may issue warrants. (article 5) However, since the crimes subject to communication restrictions are defined too extensive to be more than 300 different crimes under 19 laws including crimes under the code of Criminal Procedures, the Military Criminal Law, the National Security Law and the Military Secret Protection Act. The extensiveness left a room for abuse since the enactment.

For cases related with national security, the conditions for permission are further eased. When a Korean is a target of communication restrictions, there has to be permission from a chief senior judge of a high court, while the target is a foreigner, only the permission from the president is required. (article 7)

For the purpose of ordinary crime investigation, the prosecutors can request a permission from the court with the limit on the duration of the interception activities to three months at most and request an extension up to three months. When there are emergent reasons, the interception activities can be executed without the court permission, but within 36 hours they should get the permission. This provision has been used by the investigation agencies to conduct interception without the court permission and stop the interception before it reaches the 36 hour deadline to apply for an ex post permission.

Another problem with the current provisions is that it is very likely to get an extension once the first court permission is issued. For example, in 1998, 14 members of a labor organization so called “Yeongnam Committee” were arrested on the account that violated the National Security Law. In this case, the court had given an extension permission even though the extension request included conversation recording, new interception targets and new phone numbers that were not included in the first court permission. Such practice sustained the intercepting communications related with the crimes provided in the National Security Law for years.

The Kim Young-sam administration enacted the Protection of Communications Secrets Act and restricted interceptions by information and law enforcement agencies to the cases where they are in accordance with the act. Nonetheless, the number of the interceptions and other communication restrictions was increased and there were many cases done for political gains.

2. Revisions

The Kim Dae-jung administration ended up to face suspicion about unlawful interception frequently. In December, 2001, the Protection of Communications Secrets Act was extensively revised. The number of crimes subject to communications restriction measures was reduced from 390 to 280, the restriction period for ordinary crimes was also reduce from three months to two months, the restriction period for crimes related with national security was reduced from six months to four months, the extension periods for those two types of crimes were set to be two months and four months respectively, the duration of emergent restrictions was reduced from 48 hours to 36 hours, the agencies should inform the targets of the restrictions, the handover of communication activity verification information was now included in he Protection of Communications Secrets Act, and the National Assembly was able to get reports on such communications restrictions two times a year. To deploy communications restriction devices, law enforcement agencies should report to the Ministry of Information and Communications, and NIS to the Intelligence Committee of the National Assembly.

After this revision, there have been several important revision. Table 6 summaries details of each revision.

Table 6: Major revision of the Protection of Communications Secrets Act

	Date	Contents	Background
Enactment	1993.12.27	–	• Eavesdropping affair during the 1992 presidential election
6th Rev.	2001.12.29	• Reduced and adjusted the scope of crimes • Restricted the scope of targets for request for permission to restrict communication • Reduced the period of communication restrictions • Strengthened the procedure of emergency communications restrictions • Introduced the obligation to notify targets • Provided the procedures of handover of communication activity verification information • Forced reporting communication restrictions devices	• The National Assembly had raised issues about unlawful interception and abuse of it since 1998. • Public suspicion on mobile communication interception from 1999
8th Rev.	2004.1.29	• Prohibited handover of mobile phones' ESN • Defined the unlawful interception detection business	• Illegal cloning of mobile phones • Flood of unlawful interception detection businesses
9th Rev.	2005.1.27	• Included Internet activity logs, call originator location,and information and communication devices' network access location in communication activity verification information	• Lack of provisions for Internet activity logs, IP addresses, and etc.
11th Rev.	2005.5.26	• Strengthened the procedure for handover of communication activity verification information (court warrant) • Introduced mandatory retention of communication activity verification information • Introduced notification of communication activity verification information handover to the targets	• The rapid growth in request for communication activity verification information and abuse of them

However, on the one hand, the efforts to improve the control of law over the interceptions and other communication restrictions were intensified. On the other, the scope of the interception got ever wider because the revision added new areas of communications such as Internet activity logs and IP addresses to be subjected to lawful interceptions and other measures. It was clear that regulation over information and law enforcement agencies' interception practice failed as proven in the NSP' “X-file” case. Obviously, the problem can not be solved by simply by the law, the Protection of Communications Secrets Act. To solve the problem, we should search for answers to how

we can gain democratic control over the secret power of information and law enforcement agencies.

3. Dispute over future revision since 2007

(a) Legal issues

NIS kept insisting that it faced serious restriction on its investigation because it could not conduct mobile communications interception after the interception devices were destroyed. As a response to the NIS complaint, the Legislation and Judiciary Committee of the National Assembly revised the Protection of Communications Secrets Act in 2007. Human rights activists vigorously led a campaign against the revision. Some members of the National Assembly who opposed the bill proposed a counter-revision in the general meeting, and the bill were not passed. The revision was automatically discarded as the term of the 17th National Assembly expired after the 2008 general election.

Nonetheless, in early 2008, the new administration expressed its strong intention to push for the revision again. On October 30th, 2008, Rep. Lee Han-Sung (the Grand National Party HANARA) proposed a revision bill that has the same content as the previous one.

The revision adds crimes related with technology leaking to the crimes subject to communication restrictions (Paragraph (1) of Article 5), introduces mandatory installation of devices for restrictions with penalty of less than a billion won in fines as a mean to force the fulfillment (Article 15-2, Subparagraph 7 of Paragraph (1) of Article 17, ADDENDA Article 4 & Article 15-3), adds GPS location information to the communication activity verification information (Clause (h) of Subparagraph 11 of Article 2), and imposes a fine of 30 million won on failure to retain communication activity verification information (Subparagraph 2 of Paragraph (2) of Article 20)

The most serious problem of the revision is that it forces telecommunication service operators which are simply mediators to retain communication related data. Such retention obligation will worsen the situation where telecommunication service operators already has been collecting personal information indiscreetly and personal information leakage incidents by telecommunication service operators continue to occur. Also, it treats all citizens as potential criminals and restricts privacy in communications. The National Human Rights Commission (NHRC) released a written opinion saying "*While there is a need for a policy measure to force operators to delete all unnecessary personal information they already hold, It rather mandates data retention for specific period. This is against protection of personal information. The need for verifying communications records for the purpose of criminal investigation is recognized. However, the data retention of all citizens' communication activities for the maximum period of one year for crimes which are not under execution nor planning is against the purpose of the act and raises the possibility of violating human rights*" on January 16th, 2008. Particularly Internet activity logs depending on the settings of servers can expose not only the user identity and the location of access but also the content. However, the revision does not articulate on such risks. For example, the law enforcement agencies can force the operators to retain Internet activity logs that record file upload and download activities on account of needs for investigating copyright infringements by revising the ordinance. That means any communication information can be accumulated and, if that happens, there will not be any privacy over communication networks.

The revision forces the network operators to have devices necessary for lawful interceptions in their facilities. This obligation also threatens privacy in communications. First, there will be a constant danger that anyone can abuse the interception devices maintained by the operators to intercept communications. In that regard, NHRC properly

pointed out the perception that interception will be a routine procedure for any communications rather than an exception because of the implementation of such system will undermine privacy of citizens. Secondly, communication media that will be subject to interceptions will include not only mobile voice communications but also virtually any type of communications including Voice over IP, video telephony, Internet messengers, Internet chatting, and so forth. This should not be considered as a simple expansion of interception activities over various technologies. The effects of a certain technology on privacy should be examined separately. However, the revision reduces the problem of human rights to a simple technological choices of selecting interception devices. It defies the purposes of the Protection of Communications Secrets Act. Last, considering existing subordinate relation of network operators to the government it is very unlikely that the operators will reject requests for unlawful interceptions or report such attempts to the public or judiciary authorities. As seen in the BAI report, the network operators is likely to become accomplices in unlawful interception activities.

Furthermore, he Protection of Communications Secrets Act already has many problems even without the suggested revision. Still the scope of interception is too broad, and there are instances of emergency interceptions abuse. Also, the authority of law enforcement agencies has been recognized exceptionally broadly, and the agencies arbitrarily use their authority for the purpose of political gains.

The revision is also criticized on the account that it lacks proper legislative procedures. The administration chose not to propose the bill by itself. Instead, a member of the National Assembly proposed the bill to the National Assembly so that the bill does not have to be a subject of a public hearing. It deprives citizens of an opportunity to debate on and inspect the bill.

(b) Technological issues

The revision bill proposed by Rep. Lee Han-Sung does not articulate technological details at all. The bill leaves technological detail to be set by the ordinance. The bill provides that the standards, methods and procedures of the devices, facilities, technologies and functions necessary to enforce communication restriction measures are regulated by the ordinance. (Paragraph (3) of Article 15-2) It also provides that in maintaining devices and etc. necessary to enforce communication restriction measures, unauthorized person's access, management of access logs and etc. should follow the protection measures described by the ordinance. (Paragraph (5) of Article 15-2)

The bill does not provide enough information for further technological analysis. However, according to government official's comments in various debates and news reports, the government is considering something similar to the lawful interception standards of other countries such as the standards by the European Telecommunications Standards Institute (ETSI).

In this section, the standard architecture of ETSI lawful interception model and concerns expressed in an ETSI report[23] over the model will be introduced.

(1) ETSI lawful interception model

The key idea of the model is separation of data collecting function from a Law Enforcement Agency (LEA). The

23 ETSI (2006). “Lawful Interception (LI); Concepts of Interception in a Generic Network Architecture” (ESTI TR 101 943 v 2.2.1).

data can be grouped into categories, Intercept Related Information (IRI) and Content of Communication (CC). Data collecting function is done by network operators (NWO) who provide telecommunication services to the public, service providers (SvP) and access providers (AP). LEA builds Law Enforcement Monitoring Facility (LEMF) that receives the collected data by network operators and others. In this model, an important architectural challenge is to define the connection and the delivery protocols between the communication networks where the data collection occurs and LEMF. To achieve such interconnection, the ETSI model defines handover interfaces that controls interception procedures and mediates data delivery, and also it defines the functions necessary for interceptions.

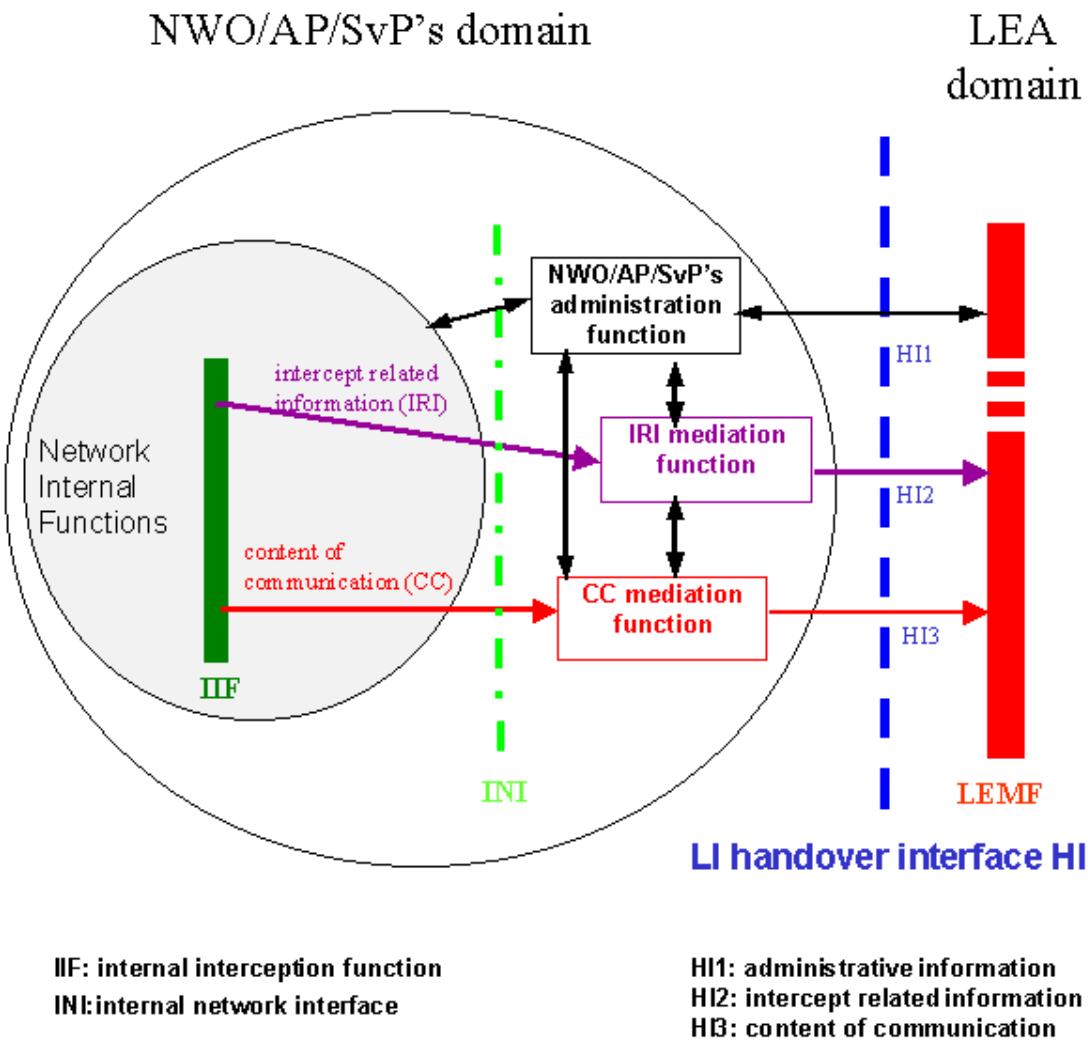

Figure 12: ETSI, "Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic". ETSI TS 101 671 V3.4.1. p.20.

Figure 12 shows that it is necessary for communication services provides to implement mediation function and administration function in their network facilities to enable interconnection between communication networks and LEMF. Depending on the providers, types of networks and types of services, the functionalities provided by each device. However, LEA can not accommodates its network to such differences. Instead, LEA controls devices, and collect and pass data using standardized mediation and administration functions. Administration function controls the interception process by passing information such as target identification, duration, types of data, delivery destination of collected data and so on through the H1 handover interface. Mediation function delivers IRI (target identification, failed calls, subscriber's service profile, location information and etc.) through the H2 handover interface and CC through H3 handover interface to LEMF. The handover interfaces also defines standard data formats and delivery technologies for transmission.

(2) Concerns over the ETSI lawful interception model

The primary obligation of telecommunication operators is to effectively provide telecommunication services at low price. However, additional obligation mandated by lawful interception such as ETSI interception model might increase the cost of telecommunication services and decrease the performance of telecommunication networks. The extent of disturbance and inefficiency can vary depending on the formats of interception reports, encryption methods for delivery or requirements of transmission technologies.

As the service operators equip themselves with such interception functions, intercepted data and interception activity logs that will be accumulated in the facilities of operators or LEMF can be leaked and the interception facilities can be used by unauthorized personnels. One can come up with measures that can limit the logical access to physical facilities such as devices or buildings where the devices are installed by setting up strict authentication and authorization procedures. However, it is also need to be considered that technologies circumventing such protective measures also develop accordingly. With all the caution and developments of protective measures, abuse by insiders is hard to prevent entirely.

V. Conclusions

First, in terms of political consequences, considering the past interception practices by the government, it is obvious that the purpose of unlawful interception activities was political one rather than criminal investigation and major practitioners of interceptions were secret information agencies like NSP. The Protection of Communications Secrets Act provides that lawful interceptions are allowed only for “cases where it it hard to stop execution of crimes, arrest offenders or collect evidences with other methods.” (Article 5) However, as illustrated in the 2005 unlawful interception cases of NSP, information agencies thought that they have a privilege to conduct interceptions as an initial way to do their business rather than as a last resort. Information monopoly by information agencies and desire of power groups to use such information for their own political gains aggravated unlawful interception practices and consequently it undermined privacy and other basic rights of citizens.

Second, the network operators and other service providers inevitably assisted unlawful interception activities. Even though they knew such activities were illegal, they feared disadvantage might be inflicted upon themselves when they refused to cooperate with the government. Considering unequal power relation between the operators and the government, it is highly unlikely that the operators will refuse unlawful interception requests. On the contrary, the operators might be force to be accomplices in unlawful interceptions.

Third, there is a tendency that the number of interception cases increases as the number of users increases partly because penetration of communication technologies is growing. Between late 1970's and early 1980's when information and communication technologies were not widely used, the number of fixed line telephone subscribers was merely about seven hundred sixty thousand. Therefore, the common methods used by the military governments to surveil individuals and groups opposing them were shadowing and physical watches. Wiretapping and eavesdropping on telephone lines were targeted only very limited number of people. However, after 1979, as rapid and huge investment in information and communication infrastructure to reduce a backlog application for telephone services, the number of fixed line subscribers exceeded 10 million in 1987. Since then, mobile phones and the Internet reached the vast majority of Koreans. Corresponding to such developments, the number of cases that use communication interception or communication records in criminal investigations and the scope of communication interception is

broadened. Controversial incidents of unlawful acquisition of communication data and abuse of such data repeated, and in some cases, the government agencies imported or developed interception technologies.

Fourth, the Protection of Communications Secrets Act was enacted to prevent unlawful interceptions, and it improved the situation surrounding unlawful interceptions to certain degree, even though there were dispute over the act. However, it is still inadequate to deal with secret and unlawful interception activities deeply rooted in political powers by information agencies as shown in the NSP X-File case.

Finally, unlawful interception activities by private entities is on the rise. Even though information agencies and law enforcement agencies keep conducting unlawful interceptions even under the restrictions provided by the Protection of Communications Secrets Act, the government denied technological possibility of mobile communication interceptions by August, 2005. Such attitude of the government left regulatory loop holes in the act and private entities took advantage of loop holes and actively engaged in unlawful interception activities.

Generally speaking, a wide use of information and technologies expands the scope and capability of surveillance power. As information and communication technology use in a society advances, ways of surveillance m more inhumane and electronic data surveillance methods, and an integrated surveillance encompassing fixed line telephones, mobile phones, the Internet and every means of communications becomes possible. In other sense, it means that more subtle and invisible ways to collect broader types of information are possible. Since people depend more on communications to do their daily businesses as they use more information and communication technologies, the surveillance power is growing ever more even it is not visible. Aggravation of the surveillance power without any check and balance increases the risk of human rights violation, social discrimination and abuse of the state power. Therefore, we need to raise social consciousness of the necessity to protect human rights in information age. At the same time, we keep working on improving the legal system including the Protection of Communications Secrets Act, removing blind spots in regulations and increasing transparency even with lawful interception practices.