# SOMEBODY IS WATCHING YOU WHILE YOU ARE ONLINE: EXPERIENCES OF SOUTH KOREA

Heesob Nam (hurips@gmail.com)

## BACKGROUND

Deep packet inspection (DPI) is a technology which enables someone to know who you are and what you are doing online. This technology is not neutral in a sense that it has been developed and adopted by those who seek their own sake. One sake is gaining control on you and the other one is commercial profit. The state, normally the administrative body, favors DPI because it provides with unimaginably enormous information on individuals, which is essential to control them. The purpose of commercial interests to use the DPI technology is simple: to make more money. They can make more money by expelling competitors from the market or by taking opportunities to attract more customers.

For the past four or five years, we, South Koreans, have witnessed almost all stories that the DPI technology have been deployed both for the state and market surveillances. This article aims to share our experiences and lessons therefrom. The story explored here is not a success story. Instead it shows ongoing debate and its outcome being dependent upon the reaction of proponents of free and open Internet.

For the purpose of background about the Korean telecommunication industry, common carriers or Internet connection service providers which have their own backbone network are required to get an approval from regulatory authority. As of September 2012, the number of common carriers is one hundred nineteen (119). But the market is dominated by three major ISPs: Korea Telecom (KT), SK Telecom and LG U+, and hence they are main players in deploying the DPI technologies.

## STATE SURVEILLANCE: INTERNET WIRETAPPING

Wiretapping is extensively and strictly prohibited by laws. Under the meaning of the Communications Privacy Protection Act (CPPA), which was enacted in 1993, the wiretapping refers to any act to know or record contents of others' electronic communications by using electronic or mechanical devices.[1] And

[1] Interestingly, the CPPA defines an act to inhibit transmission or reception of others' electronic communications as the wiretapping. The legislative history fails to shed a light on the meaning of this phrase and there has been no court cases dealing with this.

the electronic communications are so broadly defined as to cover any transmission or receiving any kind of sound, text, sign, or video by way of wire, wireless, optical or any other electronic means. Anyone who commits wiretapping without consent and statutory due process may be sentenced to imprisonment up to ten years or suspension of qualification up to five years. Monetary penalty in place of the imprisonment is not allowed. Law enforcement authorities, like prosecutors, police office and information agencies, are no exception.

However, the strict prohibition of wiretapping does not guarantee the full protection of communication privacy. For the lawful wiretapping, the CPPA requires the law enforcement authorities to get a permission from the court (or an approval of the president in case where foreigners are involved) by specifying how to inspect, what to be inspected, how long and to what extent the inspection is to be made. Yet the law enforcement authorities have been easy to obtain the permission of inspection from the court.

For instance, in 2011, the National Intelligence Service (NIS) did wiretapping in 6,840 cases, when counting on the basis of how many telephone numbers were inspected. This amounts to 95.4% of the total inspection by the law enforcement authorities.[2] This figure only reflects the surveillance conducted by ISPs upon request of NIS, meaning that inspection by NIS alone is not counted (note that NIS possesses more than thirty inspection equipment as revealed in 2010 by the congressional investigation). According to Della, one of the most prominent privacy activists in South Korea, the investigation authorities are increasingly relying on the Internet wiretapping. In 2011, it was over 60% and the investigation authorities were looking into the suspect’s email and every web surfing. Inspection into the mobile communication goes beyond your imagination. When something suspected happens in a certain area, the law enforcement authorities inspect all of the mobile stations within the area. In a single year of 2010, around 39 million of mobile telephone numbers were inspected.

Whether the inspection permitted by the court, which is called “restrictive measures on communication” under the Act, includes packet inspection has not been known for a long time from the enactment of the CPPA in 1993. But in a criminal trial of 2009 it was uncovered that NIS had inspected every email messages, Internet browsing, and telephone conversations of the suspect. In another case, it turned out to be that NIS conducted a packet inspection for about six years from July 2003 to June 2009. The NIS was able to obtain the court permission in as many as 36 times to the same person on the same

[2] http://www.mediaus.co.kr/news/articleView.html?idxno=24942

suspicion, which was related to North Korea. Surprisingly enough the court permitted the inspection of Internet line installed at the suspect's house, two email accounts of the suspect, and the Internet connection line to the suspect's place of work. This means that NIS can capture all of the packets flowing through the lines and watch in remote and real-time everything that is being displayed on the suspect's computer screen.

This case sparked heated controversy over the legality of the packet inspection. In 2010, members of the National Assembly hosted an open discussion, demonstrating how the packet inspection worked. The participants of the discussion could see every email message and even the password a user typed for an instant messaging program were captured and displayed on the screen of DPI system. Some legislators introduced bills to limit the lawful packet inspection. One proposal was to permit the packet inspection only when an authorized observer is attended.

But the legislative efforts did not come to fruition. So in March 29, 2011, human rights advocates brought the case to the Constitutional Court arguing that the packet inspection is unconstitutional because the judicial permission allowing the packet inspection is tantamount to the prohibited "general" warrant.[3] Here their argument was not to limit the scope of permissible DPI. Nor the improved judicial vigilance over the government's DPI. Their argument was simple and clear: permission of DPI *per se* is unconstitutional.

According to our constitution, a judicial warrant should be limited in scope, i.e., the person to be inspected should be specified. However, DPI of a certain Internet line allows inspection into communication of others who share the line, which is common in Internet connection. Further, the inspection should be limited to certain communications which are relevant to suspected crimes. Yet the relevance to crimes cannot be determined until when investigators look into the whole communications and decides certain communication is relevant. Therefore, the warrant allowing DPI is tantamount to unconstitutional "general" warrant, and judicial check and balance cannot work in DPI.

## Commercialization of DPI - Phorm and Target Marketing

Commercialization of DPI technology is another threat to privacy. Notable example was target marketing, which was invoked in 2009 by KT's "QOOK

[3] This case involves an individual who is a high school teacher and works for the Korean Teachers & Educational Workers' Union. The suspicion on him was notorious "praise or inspiration" for the North Korea.

SmartWeb."[4] KT designed this system on the basis of Phorm's Webwise system,[5] and made public the fact that KT already conducted a trial service targeting around its one thousands customers living in Seoul.

Many CSOs and experts expressed their concerns on the potential infringement of users' privacy right because the KT's target marketing was to inspect and analyze search words and online behaviors of users. While KT, Phorm, and their advocates argued that there was no threat to privacy because the service was targeting only those who consented, CSOs successfully revealed that the target marketing violated the CPPA, which prohibited any act to know and record somebody else's electronic communication.

### COMMERCIALIZATION OF DPI – FOR ISP'S SAKE: SMART TV

ISPs such as Internet access providers use DPI technology for their own sake. They are eager to keep their avenue as much as possible even by stifling legitimate competition.

On February 10, 2012, KT blocked an Internet connection made through Samsung's smart TV. According to KT, its blocking was legitimate because the smart TV was very likely to cause excessive traffic (the smart TV were said to cause traffic 5 to 15 times larger than IPTV). But this was not sensible because KT did not block LG Electronics' smart TV.[6] KT argued that it tried to negotiate with Samsung about the fee for the use of KT's network but Samsung didn't come to the negotiation table. During 2010 and 2011, Samsung sold around 750,000 smart TV in Korea and, for the smart TV service, had 77 servers placed in the US and leased lines from AT&T.

So KT can block the smart TV traffic by simply capture packets having destination address directing to the servers and dropping them at its four central routers located in Seoul.[7] The very next day, Samsung went to the court and asked a preliminary injunction to prohibit KT from blocking. And Korean government, i.e., the Korea Communications Commission (KCC) intervened between them. In addition, the public opinion was going against KT.

Therefore, on February 14, 2012, KT finally lifted its sanction on the

[4] "QOOK" is a brand of KT's Internet connection service.

[5] For the details of the Webwise, visit http://www.cl.cam.ac.uk/~rnc1/080518-phorm.pdf

[6] In third quarter 2011, the market share of LG smart TV was 14.4% while Samsung smart TV shares 22.5%.

[7] The routers were GSR12316 and blocked IP address was 210.118.88.200.

Samsung’s smart TV, and the KCC decided on May 4 that the KT’s blocking violated the Telecommunication Business Act because KT blocked only Samsung’s smart TV traffic not the traffic by the LG’s smart TV users, and the blocking was made without sufficient prior notice to its subscribers.

## COMMERCIALIZATION OF DPI – FOR ISP’S SAKE: mVoIP

Debate on mobile voice over IP (mVoIP) in 2012 showed how DPI used for the sake of ISPs undermines the principles of network neutrality. KakaoTalk service, which was launched in 2010 and had, as of January 2013, its subscribers of approximately 70 millions (domestically 35 millions), is a software application for mobile devices allowing users to send and receive messages including texts, photos and videos. Last year, KakaoTalk started to provide free calls over IP. But major ISPs, SK Telecom, KT and LG U+, all of which have provided telephone and VoIP services as well, did not wait a minute. The very next day when KakaoTalk launched the free call service, they throttled the KakaoTalk’s mVoIP traffic.

According to KakoaTalk’s survey, the loss rate of the first day when they launched the mVoIP service was more or less one percent, meaning little difficulty in voice-over-IP conversation with the service. However, from the second day, the loss rate high-rocketed to 20 percent in case of SK Telecom, and 54 percent in case of LG U+, leading to too poor quality to talk on KakaoTalk. This data was comparable with loss rate with Japanese ISPs (0.6 to 0.7 percent) and American ISPs (1.5 to 1.9 percent).

Unlike the smart TV case, the regulatory authority (KCC) just stood and watched, saying that it should be solved according to market’s self-regulating mechanism. But to the eyes of advocates of network neutrality, arbitrary blocking of mVoIP traffic by the major ISPs is anti-competitive and violates the Telecommunication Business Act by the same token found in the Samsung’s smart TV case.

Taking this opportunity, several CSOs, experts and activists launched Users’ Forum for Network Neutrality (called nnForum) and have taken diverse actions. For instance, nnForum asked the National Board of Audit and Inspection to investigate KCC for its negligence and dereliction of duties, and brought SK Telecom and KT to the KCC and Fair Trade Commission pointing out that they misused their market power at the expense of consumers’ benefits. They were successful in making the principle network neutrality one of the controversial issues during the campaign of the presidential election of December 2012.

## COMMERCIALIZATION OF DPI – FOR ISP'S SAKE: P2P DELIVERY

Next case also involves KT. From June 2012, KT planned to block P2P grid delivery traffic and made a contract with Sandvine for trial service. Reportedly KT paid three billions KRW to Sandvine for the trail service and would introduce the Sandvine's equipment by paying around eighty billions KRW in late 2012.

It is unknown how KT can block the P2P traffic. I just heard from the KT's information centre that they do not look into the subscribers' packets. Instead they simply make unseen to P2P service providers the information about subscribers who installed client programs for the P2P grid delivery. The P2P grid delivery is implemented by a specific program distributed by the web hard service providers or online file storage service providers. And what I heard from KT's worker who is in charge of P2P traffic management is that the specific technology to implement the P2P grid delivery traffic management is trade secret and they just look into the addresses contained in the IP header, not the port number.

Unlike common practices on the restrictions on P2P traffic,[8] the KT case has little to do with congestion management or copyright protection. KT views that any individuals who installed the client program are not *individual* subscribers: they are *business* subscribers and have to pay more fees for using KT's network for the commercial purpose.

As of now KT did not seem to implement its plan. One possible reason may be the KCC's work on draft of the standard for the reasonable management and use of communication network, which aims to set out details of "the guideline for the network neutrality and Internet traffic management of 2011." For KT, it would be better for their reputation to wait until the standard is enacted because the draft seems to legitimize their blocking of mVoIP and P2P grid delivery traffic. Actually, the draft standard enumerates restriction of mVoIP as one of the permissible traffic managements. Civil society members criticized this draft as lacking of transparency in drafting process, failing to listen diverse stake holders including end users, and making the congestion control the universal key of ISPs.

***

[8] According to BEREC (A view of traffic management and other practices resulting in restrictions to the open Internet in Europ, 29 May 2012), the most frequently reported restrictions are the blocking and/or throttling of peer-to-peer (P2P) traffic on both fixed and mobile networks, mostly for the purpose of congestion management.