IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 2 Issue 7, July 2015.
www.ijiset.com
ISSN 2348 – 7968

Wearable Devices' Security Risk Analysis and its Countermeasures : Korean cases

Hyun-Ju LEE[1], Woo-Young KIM[2] and Ji-Yeon YOO[3*]

[1 2] Department of Information and Security Management, Sangmyung University, Seoul, 110-743, Korea
[3] Corresponding author, Department of Information and Security Management, Sangmyung University, Seoul, 110-743, Korea

Abstract
Wearable devices are discussed as a new paradigm providing convenient life and will also change not only life behavior but also social structure. But, for the security risks of the wearable devices that will threaten such changes are only limited to the discussions in the security perspectives such as personal information, network security, etc. Therefore, this paper analyzes and derives the enhancements of the system in Korea to control security risks according to the characteristics of wearable devices (Scenarization, portability, awareness, and recording).
Keywords: *Wearable Devices, Security Risk, Scenarization, Portability, Awareness, Recording*

1. Introduction

Recently, with the release of Google Glasses, Samsung VR, iWatch, etc., wearable devices are emerging globally. Until now, watch type wearable devices are the mainstream devices, but various types of wearable devices such as glasses, headphone type smart equipment, etc. are expected to be out in the market. As the development and prevalence of wearable devices are becoming active, the corresponding security threat and issues are also emerging rapidly.
In case of smart glasses, all of the views seen by the user wearing the equipment are recorded, and since there is no indication or trace of the recording during the recording, in the point that the user may not be even aware of the recording, there is a big possibility of privacy invasion and personal information leakage [12].
And this can be a problem not only for others but also for user oneself. When one wears wearable device all the time, it will record all of the user's daily life, thus analyzing usual living pattern, and if the equipment is lost or stolen, it may lead to user's privacy problem [8].
In addition, wearable device user's authentication problem is also becoming an issue. Equipment user authentication requires careful management to prevent sharing with others, and until now, there is no authentication technology that can realize complete confidentiality and integrity. If in such a situation, if the equipment is hacked or if authentication is shared, a lot of data stored in the equipment will be leaked. In the same context as authentication, the problem of unsafe network environment also exists. Wearable devices can be connected to user via wireless network as smart phones, and if open network or unreliable access environment are used, security problem may occur [4].
As Google Glasses, a representative wearable device, is out in the market, personal information protection issue is becoming a big social issue. Especially, Google has been receiving legal remedy with the existing Street View service for violating Act on the Protection of Personal Information, as Google Glasses that can collect wide range of data are released, the concerns for privacy invasion and personal information leaking possibility are increasing [5].
Google's policy and personal information protection policies of Europe, etc. already have been continuously making conflicts, and as various problems surrounding wearable devices are pointed out, there is already a sign of rearranging the relevant laws in overseas. Wearable devices are not out in the market yet in Korea, but when they are released in the market, the issues brought up in overseas have high possibility of being brought up also in Korea.
Therefore, this paper intends to discuss the relationship between wearable devices' security issues and the laws in Korea. Centered on the most representative wearable device, Google Glasses, it will look at the relevant overseas trends and briefly look at the problem of conflict with laws in Korea and the possibility of application of the laws. This is expected to be used in the supplementation and enhancement of the laws at the time of the release of wearable devices.

2. Definition and Concept of Wearable Device

There is no clear definition of wearable device yet. Except that it is 'wearable' device as it is called, the concept and definition of wearable device are actively discussed until now from before the release of the equipment.
T. Starne (1996) defined wearable device as an effort to transfer part of our daily lives to computers[14], and Bradley Rhodes, et. al. (1997) said that it means equipment that can recognize the user's personal

ISSN 2348 – 7968

environment all the time from back of the user and equipment that can be more closely connected to the user [2]. Steve Mann (1998) said that wearable device exists in the user's personal space, always accessible, and has invariability for mutual interaction [15].

As such, the concept emphasizing the communication between equipment and user based on the potential related to the technical development formed the mainstream before the release of the wearable devices. Especially, the recognition for improved human capability supplementing the insufficiencies of the users and satisfying the requirements was emphasized. But, as the technical development for wearable device becomes active and the actual equipment is out in the market, discussions became more diversified, and the concept of wearable device defined with basis on potential moved to the utilization of various functions that help convenient daily lives of the users.

Korea Creative Content Agency (2012) defined wearable device as equipment that can continuously collect the detail information of the ambient environment and personal body changes in real time [9], and Khurram Nasir Gore, et. al. (2014) mentioned that it can provide the information by itself without the user making certain actions to use the equipment in daily life and that the user is not aware of what operations are done by the user[7]. Research Group of the Office of the Privacy Commissioner of Canada (2014) said that the wearable device 'learns' what the user is experiencing at anytime and anywhere through certain mutual interaction between the user and the equipment [11].

By putting together actual discussions from the advent of equipment until recently, you can see that wearable device mainly has the characteristics of 'Scenarization' providing the information required for the user with the screens captured through various smart functions, 'portability' wearing like a part of the body without repulsion and move freely, 'awareness' making self decisions without order by user by effectively analyzing the user's pattern, and 'recording' helping the expansion of the incomplete memory without the user stopping any work to use the equipment.

3. Security Threat according to Wearable Devices' Characteristics

3.1 Security Threat by Scenarization

Table 1: Regulation related to scenarization in Korea

Classification	Law Provisions	Contents
Act on the Protection of Personal Information	Article 25 Paragraph 5 (Restriction of Installation and Operation of Video Information Processing Equipment)	The video information processing equipment operator cannot manipulate the video information processing equipment without authorization for purposes other than the purpose of installation or view other places, and sound recording function may not be used.
CCTV Personal Video Information Protection Guideline	Article 6 Paragraph 3 & 4 (Operation and Management of Video Information Processing Equipment)	③ Person handling personal video information needs to take necessary action such as masking when there is a concern for invasion of other people's privacy by the angle of the camera of the video information processing equipment. ④ Person handling personal video information may not use sound recording function in any case when the video information processing equipment is installed and operated.
Copyright Law	Article 104-6 (Prohibition of Copyrighted Video Recording)	No one shall record or publicly transmit the copyrighted video products that are protected by copyright in the movie theater, etc. where it is being played without the consent of the owner of the copyright.

CCTV having public purposes have legal/systematic installation regulations. But, wearable computers are used for various purposes not only for the convenience of the business but also for entertainment, medical, health care, etc.[4]. That is, wearable devices are used for personal usages, so there is no legal regulation, and there is no specified purpose, so the purpose can be said to be decided according to the usage. This means that if one uses Google Glasses with the purpose to record one's own daily life, there is no obligation to use it only for that one purpose, so it can be used freely or other usages such as filming others, etc. Also, wearable devices are always working, and it is difficult for others except the user to know what actions are taken by the user with the wearable device. Also, Google Glasses, which is a wearable device, not likely smart phone camera, user does not need to take certain actions to stop a while to focus to take the picture, so illegal actions such as taking pictures without

ISSN 2348 – 7968

permission became much easier [7]. This can be said to mean that the possibility of taking pictures of other people's faces and actions in streets and public places without the consent of other people with Google Glasses which can be manipulated without authorization regardless of the intention of the user.

With concerns for this, Google prohibited wearing Google Glasses in the bars and several restaurants in the West Coast where the headquarter is located, and announced the developer policy to the Google Glasses application developers the policy not to use camera or microphone by using mutual reference and recognition of other people when personal information can be invaded and disable turning off the display when camera is used. But, the guideline of Google headquarter for prohibiting the wearing of the equipment has no compulsion, and only with the developer policy, it did not include the limit for developer in the design stage or technical manipulation by the user, so the expectation that the guideline will be followed can be said to be not realistic. As an example, 'Wink' photographing function of Google Glasses is installed as default in Google Glasses due to the popularity of the application called Winky. As such, the reason not being able to restrict the matters against the Google's developer policy is that there is no technology that is completely prohibited [11].

Also, in case of Google Glasses, user can freely file/record as he or she moves, and it is difficult to identify whether the camera function is ON, so there is a possibility of having the problem related to copyright by recording non-open concert or movie, etc.

3.2 Security Threat by Portability

Table 2: Regulation related to portability in Korea

Classification	Law Provisions	Contents
Act on the Protection of Personal Information	Article 2 (Definition)	"Video information processing equipment" means the equipment specified by the Presidential decree among the equipment continuously installed in certain space taking videos of person or object or sending the video through wired or wireless network.
Act on the Protection of Personal Information	Enforcement Ordinance Article 3 (Scope of Video Information Processing Equipment)	① Closed circuit television: equipment falling into any one of the following categories A. Equipment taking videos through the installed camera continuously installed in certain space, or sending the filmed video information to certain place through the transmission route such as wired or wireless closed circuit, etc. B. Equipment that can film/record the video information filmed or sent as in A. ② Network camera: equipment which the installer or manager of the equipment can process such as collect or store the video information taken by the equipment continuously installed in certain space at any time through wired or wireless internet
Privacy Act for Location Information ("Law on Protection and Usage of Location Information")	Article 5 Paragraph 1 (Prohibition of Collecting, etc. of Location Information)	No one shall collect, use, or provide the location information of an individual or object with portability without the consent of the corresponding individual or owner of the object.

In Act on the Protection of Personal Information, the boundary of video information processing equipment is closed circuit television and network camera, and the common points of the two equipment is 'continuously installed in certain space'. To protect the privacy of the owner of the information in the filmed video, CCTV is installed and operated in 'fixed' space and in 'public location' with clear public purposes. CCTV is installed and with purpose of safety of people or compliance of the law, so the boundary of the installation space is set to place with frequent crimes, deserted place, place with frequent traffic accident, highways, etc., and it is fixed and used at one location. Of course, CCTV is not defined and receives legal restrictions just with 'fixed' property. CCTV inside transportations such as taxi or bus, like wearable device, move freely according to the location of

ISSN 2348 – 7968

the transportation, thus there was a controversy on whether CCTV in vehicles correspond to the video information processing equipment in 「Act on the Protection of Personal Information」.

But, in case of CCTV inside vehicle is installed in certain space, which is inside vehicle, continuously filming the corresponding space, and for transportation such as taxi or bus, which is not a private vehicle, many and unspecified people are not restricted for riding, so it is decided that there is a sufficient basis to see it as an open space, and it is regulated as video information processing equipment installed in public space according to Act on the Protection of Personal information[6]. But, wearable device can move freely according to the location of the user, so it is difficult to apply the corresponding law, and also, there is no limitation of time and space, so owner of the information can be exposed to security risk by the camera at anytime and anywhere. Also, user oneself is also exposed to the security risk.

Google Street View service, which is introduced as a part of Google Map from May 2007, tells the location desired by the user and various routes such as distance from the current location to the corresponding location and the direction, etc., so if the user information is stored, one's moving path or frequently visited location can be easily obtained, and user privacy may be invaded. If companies abuse the corresponding information for the purpose of marketing, it is the part that can easily become a problem [10].

Such Google Glasses app services send the information to Google server through internet, and Google server sends the information through Glass Sink, so all app usage records of the user are stored. This means that Google possesses all activity records using Google Glasses, so there is a big possibility of becoming an element of personal information intrusion.

Also in case of CCTV, it can be regulated with relevant law, but there are a lot of insufficiencies to legally regulate wearable devices. In Aug. 2010 in Korea, with the suspicion of illegal personal information collection by Google's Street View vehicles, there was investigation on the server and prosecution by police [13], and this is the part that can become a problem not only in vehicle's Street View service but also in Google Glasses Street View service. When Google Glasses are out in the market, the log record related to the user's moving route shall not be basically collected or used, but in such situation, it can be collected without the awareness of the user, so it may violate Privacy Act for Location Information.

3.3 Security Threat by Awareness

Table 3: Regulation related to awareness in Korea

Classification	Law Provisions	Contents
Act on the Protection of Personal Information	Article 25 Paragraph (Restriction of Installation and Operation of Video Information Processing Equipment)	Person who install and operate video information processing equipment (hereinafter, "video information processing equipment operator") shall take necessary action such as installing signboard as set in the Presidential decree so that the information owner can easily recognize
Act on the Protection of Personal Information	Article 4 Paragraph 2 (Rights of Information Owner)	The information owner has the following rights related to one's own personal information processing - Right to select and decide whether to agree on the personal information processing and the boundary of the consent
Standard Personal Information Protection Guideline	Article 50 (Personal Video Information Protection by Person other than Information Owner)	Video information processing equipment operator, when one takes action such as viewing in Article 48 paragraph 2, shall take protective actions so that personal video information of a person other than the information owner cannot be identified when person other than the information owner can be clearly identified or if there is a concern for privacy invasion of the person other than the information owner.
CCTV Personal Video Information Protection Guideline	Article 6 Paragraph 3 (Operation and Management of Video Information Processing Equipment)	Person handling personal video information needs to take necessary action such as masking when there is a concern for invasion of other people's privacy by the angle of the camera of the video information processing equipment.

Any information owner of the personal video information collected through CCTV has the right for protection as the information owner whoever he or she is. But, it is not possible to obtain 'consent' from various information owners in many CCTV, so signboard shall be attached near the CCTV so that people can be aware that the zone is currently filmed by CCTV. Also, according to Standard Personal Information Protection Guideline Article 50, protective action is taken to disable identification of a

ISSN 2348 – 7968

person in the process of viewing CCTV video information, if it is possible to identify person other than the information owner or if there is a concern for privacy invasion.

But in case of wearable device, because of 'awareness' that can identify individual, there may be severe invasion of portrait right of the information owner or self decision right of personal information. One of the known most representative wearable device, Google Glasses has 'Name Tag' function to find the matching profile in the internet and tell the other's information when the user takes a photo of other people with the camera attached to the glasses. This can verify the personal profile of others without obtaining the consent of other people, so there is a very big concern for privacy invasion of the information owner [12]. If there is no separate device to tell the photographic in the equipment itself, the opposite to CCTV, individual cannot even be aware that his or her photo is being taken, and even if the information owner does not want, the photographing can occur without knowing.

Not only the user's privacy issue but also concerns for privacy invasion and portrait right invasion were brought up for Google's Street View service with the exposure of other people's faces and vehicle plate, etc., and to solve such privacy problems, Google developed the technology for automatically blurring important components of the image such as Face-blurring and now in service. Google Street View's face-blurring technology disables the face recognition of the pedestrians so that the user identity cannot be easily obtained to provide strong privacy, and if one directly requests deletion to Google, it is deleted upon personal identification, but it still remains as a big problem in a point that blurring is not at a level to completely disable identification of a person or vehicle and a point that original data is still stored by Google [10].

3.4 Security Threat by Recording

Table 4: Regulation related to recording in Korea

Classification	Law Provisions	Contents
CCTV Personal Video Information Protection Guideline	Article 6 Paragraph 1 (Operation and Management of Video Information Processing Equipment)	① Person handling personal video information shall prepare and document 「Video information processing equipment operation and management guideline」 including the following items - Recording time, storage period of the recording, storage · management · destruction method and storage location
Standard Personal Information Protection Guideline	Article 45 Paragraph 1, 2, and 3 (Storage and Destruction)	① Video information processing equipment operator shall destruct the collected personal video information without delay when the storage period specified in the video information processing equipment operation and management guideline is over. ② If the video information processing equipment operator cannot set the minimum period to achieve the purpose of the possession due to one's own circumstances, the storage period shall be within 30 days from the collection of the personal video information. ③ The method of the destruction of the personal video information shall be one of the following methods. 1. Fragmentation or incineration of the printings (pictures, etc.) with personal video information 2. Permanent deletion of electromagnetic file form personal video information with technical method disabling recovery

CCTV has documented recording time and storage period of recording as in the guideline, keeps the destruction procedure and permanently deletes according to Standard Personal Information Protection Guideline.

But, wearable device has the privacy problem since not only all information of others and but also user equipment usage records are also remaining. According to Standard Personal Information Protection Guideline, personal video information shall be permanently deleted with technical method disabling recovery, but in case of Google Glasses,

ISSN 2348 – 7968

original data is stored by Google, so the equipment user directly deleting the information cannot be seen as a complete deletion, and the individual video recording of the person owning Google Glasses cannot be controlled by the government.
On the surface, it is easy to think that the wearable device owner obtains and manages all of one's own and other's information, but in reality, you can say that the company manufacturing and managing the device collects and stores all data.

4. Overseas Trend and Relevant Law Enhancement Movements

We need to be sensitive to the security risks by the Scenarization of wearable devices. Currently, most of the countries recognize wearable devices as 'video information processing equipment' and are adding the contents related to 'wearable device' in CCTV related laws.
Among them, Britain is the quickest in responding to the security issues of wearable device, and with such response, it is showing the movement to make provisions for 'wearable device' in Data Protection Act. British Information Protection Committee (ICO) sees that it is most important whether other can be aware when the wearable device user is taking a picture, and said that it shall be applied as the same as CCTV related regulation in the current Data Protection Act. In Britain's Data Protection Act, CCTV has the responsibility for protection according to the location, and the personal or commercial usage is restricted, so when one installs CCTV in front of one's house, it is personal purpose and cannot be protected by law. Also, to install CCTV, code assigned by ICO shall be complied with, and brief checklist for CCTV system user is also included. The committee emphasized that wearable device also cannot receive the legal protection in case of taking pictures with certain purpose [3].
'Serious Invasions of Privacy in the Digital Era' report announced by Law Reformation Committee of Australia states a part on "wearable device". Wearable device is defined as equipment containing video and audio recording function like Google Glasses, and wearable device with audio recording function generally belongs to 'listening device', but it mentions that all regulations are not limited to wearable devices with possible video filming. Also, according to Surveillance Device Laws, it is not right to prohibit the general use of such equipment, use of wearable device "not surveying" is legitimate, and the decision of the legitimacy of the usage of the equipment depends on the situation of that time, and it even provided a detail guideline that it is different according to whether the corresponding person was aware that it was a wearable device [1].
Canada Personal Information Committee (OPC) is studying the supplementation of the current Act on the Protection of Personal Information for the commercialization of the wearable device. Especially, it newly installed the category 'video camera wearing on body' in the revision of Closed Circuit CCTV Guideline, and forced to provide adequate information to the person recorded and maintain the security of the recorded video when it is used, and to consider to comply with Information Sharing Agreement when the video is shared with a 3rd party [11].

5. Conclusion

There is an intense competition with interests of large global companies such as Google, Apple, Samsung, etc. for wearable devices that is called the advancement of mobile equipment by introducing the next generation mobile technology. Currently, wearable device is at the early stage of commercialization, but beside the characteristics and advantages of the equipment, there is also security risk directly connected to the privacy issues. The privacy issues are not just limited to the wearable devices, but due to the unique characteristics, the risk is magnified more.
So, overseas regulations include not only CCTV but also wearable devices in the boundary of video information processing equipment. That is, CCTV and wearable device are considered as similar equipment, and wearable device is included in the boundary of CCTV to expand the definition and relevant law provisions in CCTV laws.
In case of Korea, people are sensitive to security problems such as personal information leakage and privacy invasion, etc. due to security incidents following one another. Therefore, when the wearable devices are introduced and if security problems occur, the consequences are difficult to estimate.
Therefore, it is necessary, as the current overseas trends, to be aware of the security risks and to search for the enhancements before the equipment is introduced.

References

[1] Australian Law Reform Commission. "Serious Invasions of Privacy in the Digital Era : Surveillance Devices", pp.190-200. 2014.
[2] Bradley R, Jeffrey L, Jennifer H, Dana K, Roz P, and Alex P "Augmented Reality Through Wearable Computing", The Media Laboratory Massachusetts Institute of Technology. 1997.
[3] Information Commissioner's Office. "Guide to data protection - CCTV". 2014.

ISSN 2348 – 7968

[4] John, L. "Security challenges for wearable computing a case study", Lulea University of Technology, Sweden Centre for Distance-spanning Technology, pp.4. 2007.
[5] Kang, G. S. "[Column]Wearable devices and security threats". 2014.
[6] Kang, S. H, and Kim, H. S. "Privacy Issues Analysis of the operating proliferation of Image information processing equipment", Internet&security focus, XIV No. 4, pp.45-65. 2013.
[7] Khurram G, Fred L, and Paul B. "Controlling Legal Risk if Google Glass and Wearable Tech". 2014.
[8] Kim., D. G. "Trends and Implications of wearable devices", Korea Information Society Development Institute, Vol. 25, No. 21, No XIV. 566, pp.23-24. 2013.
[9] Korea Creative Content Agency. "Human-device interaction technology", XIV No. 27, pp.36. 2012.
[10] Lee, S. J. "Face-blurring techniques of Google Street View Service". 2012.
[11] Office of the Privacy Commissioner of Canada. "Wearable Computing - Challenges and opportunities for privacy protection". 2014.
[12] Park, H. S. "Privacy issues and implications surrounding the wearable computer", KT Economic Management Institute. 2013.
[13] Seong, Y. G. " 韓 , 'Countdown' of Sanctions for unauthorized collection of personal information, Google Street View". 2014.
[14] Starne, T. "Human-powered wearable computing", IBM SYSTEMS JOURNAL, VOL 35, NOS 3&4. 1996.
[15] Steve, M. "WEARABLE COMPUTING as means for PERSONAL EMPOWERMENT", ICWC-98. 1998.