

유비쿼터스 도시 환경에서 프라이버시 보호 방안에 관한 소고 - 경쟁하는 개인정보가치 분석을 중심으로 -

A Study Privacy and Security in Ubiquitous City Environment (Focus on Computing Values Analysis of Personal Information)

정창덕*, 강장묵+

(Chang-Duk Jung, Jang-Mook Kang)

Abstract : As the concept of Ubiquitous City has become an important issue, we need to have a voice in the field of Privacy. The Ubiquitous Computing revolution, it is achieved a physical space and an intelligent union of cyber space in the space where an off-line space was integrated with on-line. It is combined with a life space naturally, and Ubiquitous creates a new integrated space. The space is the opportunity space that is limitless as soon as it is the unknown world that mankind was not able to experience yet. According to the recent papers and studies, Privacy or Personal Information sector is mentioned as a major problem for Ubiquitous Computing Society. Therefore, this paper checks Ubiquitous City, the present privacy concept and situation of currently proceeding Ubiquitous computing environment. Also, The main purpose of this paper is to analyze the concepts privacy, personal information. Thus this paper treated the analysis of case, technological or social issue, problem and solution, competing values of privacy and so on.

Keywords: Ubiquitous City, Ubiquitous Computing, Privacy, Personal Information, Competing value model of privacy

I. 서론

디지털 기기에 융합화(convergence)되어 실생활에 침투하는 유비쿼터스 컴퓨팅 기술은 정보화의 순기능을 극대화시켜 인간의 삶을 윤택하게 할 것으로 기대되고 있다. 그러나 가상 공간(cyber space)으로부터 물리 공간(physical space)으로의 융합과 침투 과정에서 이미 수많은 유비쿼터스화의 역기능이 제기되고 있다.

유비쿼터스화가 단순한 기술적인 진보에 그치지 않고 커뮤니케이션 환경의 변화, 지식의 생성과 흐름의 변화, 유비쿼터스 공간이라는 이전에 경험하지 못한 새로운 공간의 창조 등 사회의 패러다임과 인식의 변화를 요구하고 있기 때문에 유비쿼터스화의 역기능이 가지는 위험성은 크다. 따라서 본 소고에서는 프라이버시 보호 영역이 확정적이지 못함에 따른 문제점을 지적하고, 보호 방안의 강구를 통하여 유비쿼터스 도시에서 발생하게 될 프라이버시 위협 요인과 해결방안을 제시하는데 도움을 주고자 한다.

II. 프라이버시 기술적·윤리적 환경 변화

1. 엔트로피 법칙에 따른 무질서의 증가

물리학에서 엔트로피란, 더 이상 일로 바꿀 수 없는 에너지의 양을 측정하는 수단을 말한다. 엔트로피가 증가되었다는 것은 이용 가능한 에너지의 양이 줄어들었다는 것을 뜻한다. 결국 기술의 발전이란 새로운 에너지를 찾아내는 것이 아니라, 일정하게 존재하는 에너지를 점점 더 바꿀 수 없는 상태의 에너지로 바꾸는 것이다. 이는 기술의 발전이 에너지

를 얻기 위한 비용을 증대시키고 있다는 것을 말한다.

여기서 논점은 유비쿼터스화는 과연 고(高)엔트로피 문화, 사회, 환경으로 모든 인간의 일상생활을 변화시키는 패러다임인가란 점이다. 만약 그렇다면, 정보화의 역기능이란 가상 공간에서 유용한 에너지가 줄어들고 일정량의 에너지가 무용한 에너지로 전환되는 오염의 부산물이라고 정의할 수 있다. 특히 유비쿼터스 컴퓨팅 시대에는 과거와 비교할 수 없을 만큼 빠른 속도로 엔트로피가 증가될 것으로 예상되며, 이로 인해 야기될 수 있는 프라이버시 위협과 기술적 해결방안 역시 엔트로피 증가를 가속화시킬 수 있다는 위험에 노출되어 있다.

2. 무질서의 증대에 대한 외부비용의 증대

이 외부비용이란, 특정한 제품, 공정, 계획, 서비스에 의해 파생된 2차 효과의 결과로 발생하는 예상치 못한 비용을 뜻한다. 만약 기술에서 얻는 이익(정보화의 순기능)이 외부 비용(정보화의 역기능)보다 작게 된다면 기술사용 이전으로 회귀하는 것이 바람직하나 기술사용 이전으로 회귀하는 문제 역시 사회 전체의 패러다임을 바꾸는 변화이기 때문에 기술이 도입된 이후 기술사용 이전으로 돌아가는 문제는 불가능하다.

유비쿼터스 컴퓨팅 기술의 외부비용은 지수 함수적으로 증가한다. 이는 오늘날의 기술이 인간의 삶을 규정하고 생활 방식을 결정지을 만큼 침투력과 영향력이 절대적으로 증대되었기 때문이다. 특히 정보화의 빠른 발전으로 사회가 복잡해지고 사회적 오염이 증가하게 되었다.

3. 자유주의적 또는 개인주의적 프라이버시 이론

유비쿼터스 컴퓨팅 시대에 프라이버시에 대한 자기보호의 원리는 자유주의적 또는 개인주의적 프라이버시 이론에 기초한 주장들이다. 자유주의적 프라이버시를 다섯 가지의 목

*: 고려대학교

+: 세종대.학교

표로 명시한 리차드 세버슨의 ‘공정한 정보 실천 규약(code of fair information practices)’은 프라이버시를 윤리적인 원리로 나아가게 하기 위한 사회적 공리주의적 접근이다.^[1]

이 규약들을 자율적인 개인주의에 근거하여 스스로가 보호해야 하는 프라이버시로 발전시킨 사람은 가비슨(Ruth Gavision)과 밀(John Stuart Mill)이다. 가비슨은 비밀성, 익명성, 고독이라는 핵심원리에 입각하여 프라이버시를 어떤 개인에 대한 타인의 접근을 제한하는 것이라고 정의한다. 밀의 프라이버시 개념은 외적 간섭으로부터 자신의 신체와 마음을 자유롭게 지해하는 개인이 주권자가 되어 있는 상태를 뜻한다.^[2] 따라서 자유주의적 또는 인주의적 프라이버시 이론은 혼자 있을 수 있는 개인의 권리와 개인에게서 필요한 정보를 얻어야 하는 정부의 의무 사이에서 이익의 균형이 이루어져야 한다는 주장의 논리적 배경이 되어 왔다.^[3]

문제는 오늘날까지 프라이버시에 대한 자유주의적 또는 개인주의적 이론에 근거한 이익 균형의 원리가 법리적으로는 이익형량의 이론으로 폭 넓게 받아들여지고 있다는 사실이다. 그러나 이와 같은 해결방안은 복잡성이 증가하는 고엔트로피 사회인 유비쿼터스 도시 환경에서는 문제해결의 한계를 가진 방안이다.

4. 이익 형량의 한계

자유주의적 프라이버시 접근법은 침입과 간섭으로부터 저항하는 자유로서의 프라이버시와 자기 자신에 대하여 노출되는 프라이버시를 스스로 통제할 수 있는 자유로서의 프라이버시를 의미한다.

하지만 첫째 유비쿼터스 컴퓨팅 환경에서 개인은 개인정보의 자기통제 능력을 상실할 것이므로 프라이버시의 침입과 간섭으로부터 저항할 수 있는 자유를 스스로의 적극적인 통제를 통하여 해결할 수 없다.

둘째, 가상공간에서 이동하는 전자화 된 개인정보에 대한 협소한 보호 영역으로는 광범위하게 위협받게 될 유비쿼터스 컴퓨팅 공간의 프라이버시 침해 문제를 해결할 수 없다는 한계를 가지게 된다. 더욱 놀라운 점은 개인이 국가와 기업이 제공하는 공적인 혜택을 얻고자 개인이 원하지 않는 감시를 자발적인 참여로서 도울 수 밖에 없는 구조가 형성되었다는 점이다.

이익형량은 프라이버시 속에 내재되어 있는 상반된 두 가지 가치에 대한 해결방안은 제시할 수 있지만, 세 가지 이상의 다양한 가치를 내재한 경우에는 규범조화적인 해결방안을 제시해줄 수 없는 한계를 가지고 있다.

III. 프라이버시 및 개인정보의 이해

1. 개인정보의 의미

개인정보란 생존하는 개인에 대한 정보로서 개인을 식별할 수 있는 것이다. 특정 개인을 알 수 없다하더라도 다른 정보와 쉽게 결합하여 특정 개인을 식별할 수 있는 모든 것을 개인정보라고 볼 수 있다.^[4]

2. 개인정보와 프라이버시의 차이점

개인정보는 크게 공적인 것과 사적인 것으로 나누어진다.

공적인 것은 성명, 직장 등과 같은 사회적 관계를 형성하는데 필요한 정보이다. 사적인 것은 개인의 습관과 취미활동 등을 뜻한다. 일반적으로 사적인 정보를 개인정보와 구분된 프라이버시의 내용이라 할 수 있다

3. 정보주체와 개인정보의 가치

유비쿼터스 컴퓨팅 환경에서 개인정보를 보다 세분화시킴으로 보호의 영역을 확정하고자 개인정보에 내재된 정보 관리자와 주체 간의 가치를 세 가지로 분류하면 공적 가치, 사적 가치, 상업적 가치로 나눌 수 있다.

이와 같은 세 가지 가치는 세 영역의 정보관리주체가 추구하는 이해관계에 따라 충돌하기도 한다.

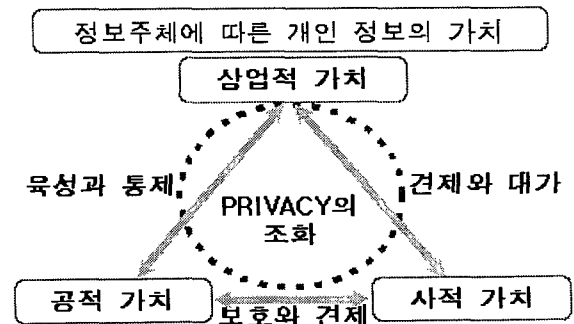


그림 1. 프라이버시의 조화.

Fig. 1. Harmony Of Privacy.

IV. 프라이버시 경쟁가치

1. 프라이버시의 내적 가치

프라이버시에 대한 개념을 정리하면 이익(interest)로 보는 견해와 권리(right)로 보는 견해 그리고 이익과 권리로 보는 견해로 크게 나누어진다. 즉 프라이버시 보호는 프라이버시와 충돌하는 다양한 가치들 간의 균형점을 찾는 과정으로 이루어진다.

2. 보다 세분화된 프라이버시의 경쟁가치(Computing Value in Privacy)

기술의 변화로 프라이버시의 개념이 변화하고 결국 프라이버시가 가지고 있는 내재적인 경쟁가치들이 어떤 관계를 가지고 변화하고 있는지를 살펴보면 다음과 같다. 유비쿼터스 컴퓨팅 환경에서의 프라이버시의 가치는 공적 가치, 사적 가치, 상업적 가치, 법 및 규범적 가치, 기술적 가치로 분류되며 각 가치는 경쟁, 충돌, 보완, 협력하는 관계를 가진다.

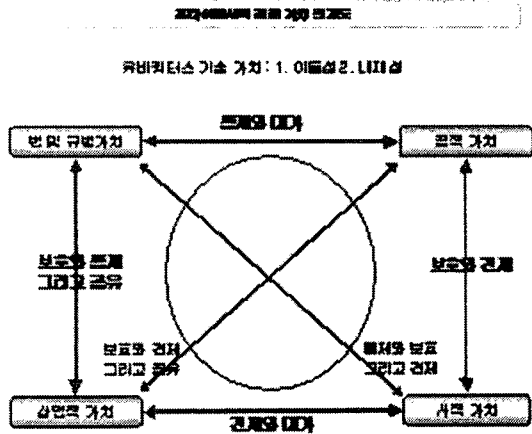


그림 2. 프라이버시의 경쟁가치 관계
Fig. 1. Relation of Computing Value In Privacy

유비쿼터스 기술로 대표되는 이동성(mobility)과 내재성(pervasive)⁵⁾이라는 기술적 특성은 다양한 가치들에 혜택과 비용(기술의 편리함과 프라이버시 위협), 한계(기술적 제한)와 규제(code에 의한 통제)를 주고있다.

V. U-CITY의 서비스와 프라이버시 경쟁가치

1. U-CITY에서 구현될 공통 서비스

유비쿼터스 도시(U-CITY : Ubiquitous City)에 적용될 공통서비스란 모든 도시에 일반적으로 적용 가능한 서비스를 뜻하며 주로 도시 기반 시설을 관리하거나 도시의 안전을 담당하는 것들이다. 즉 공통서비스로는 도시 시민의 안전과 밀접하게 연관되어 있는 지하시설물관리, 방법 및 치안서비스, 도시 시스템의 교통 효율성과 연관된 교통관리 서비스, 모든 시설에서 배출되는 오염원을 관리하는 환경 관리 서비스 그리고 도로, 터널, 다중 복합 시설 등 도시기반 시설의 안전과 이용 효율성과 관련된 시설관리 서비스가 있다.⁶⁾

본 소고에서는 기존의 서비스에 도시의 사회복지 측면을 강화함으로써 세대 간 또는 도시 구성원 간의 차이를 줄이는 서비스를 추가하였다. 이는 기존의 도시가 독거노인, 당뇨병 환자, 복지기관, 공원 및 놀이터 등에 대한 관리를 하고 있다는 사실과 지자체가 담당하는 중요한 업무 중에 하나인 사회복지 서비스를 유비쿼터스화함으로써 경쟁력을 높여야 한다는 이유 때문이다.

2. U-CITY에서 구현될 세부 예상 서비스

유비쿼터스 도시에서 우선적으로 도입될 것으로 예상되는 서비스는 크게 사회복지, 교통, 지상 시설물, 지하시설물, 환경으로 구분되어진다. 도시의 공통 서비스에 대한 유비쿼터스화는 장래 도시 시민의 자발적인 선택에 의한 유비쿼터스 아파트, 자동차, 가전기기 등과 연계되어 기업이 개발한 유비쿼터스 서비스의 시너지를 극대화시킬 수 있을 것이다.

3. 유비쿼터스 도시와 민감한 프라이버시

프라이버시는 개인정보 활용에서의 민감도(Degree of sensi-

tiveness)에 따라 민감한 정보와 비민감정보로 구분한다. 미국의 경우 연방통신법(Telecommunication Act of 1996)에서 인종, 성적 습관, 사상, 신조, 병력, 전과, 세무정보, 보험 및 금융거래, 어린이 인터넷 활용 정보, 통화 및 통신내용, 사회안전번호(SSN : Social Security Number) 등 개인이 고유하게 소유한 정보를 민감한 정보로 규정하고 있다. 그러나 이름, 전화번호, 주소와 같이 등재 및 공개된 전화가입자 목록 정보는 비민감정보로 규정하고 있다.⁷⁾

4. 유비쿼터스 도시의 예상 서비스중 민감한 프라이버시 위협 요인

유비쿼터스 도시에서는 사회복지와 교통에 대한 서비스가 민감한 프라이버시 관련 정보의 생성과 관리 등에 따른 위협에 노출될 가능성이 크다. 따라서 각 서비스 시나리오별로 노출되는 위협요인에 대하여 분석하면 다음과 같다.

첫째 사회복지서비스 분야 중 사회복지, 안전, 방범치안 서비스 시나리오와 위협요인은 다음과 같다.

공원관리는 센서와 RFID 같은 장치를 복합적으로 적용하여, 공원의 유지와 활용에 있어 사용자의 편의를 도모하는 서비스가 예상되며, 공원시설물관리, 동식물정보제공, 식물관리, 동물관리, 미아 찾기, 시설물예약, 시설물현황, 공원안전과 같은 상생 서비스를 포함한다.

독거노인 건강관리는 신체와 가정환경에 각종 센서와 RFID 장치, 그리고 통신 환경을 복합적으로 적용하여, 독거노인의 건강 및 질병상태 확인, 응급상황 감지 및 대처, 의약품 및 음식물 관리, 가정환경 자동조절 등의 기능을 통해 건강을 관리하는 서비스를 말한다.

둘째 교통 분야 중 교통관리, 전자지불관리, 운행안전관리 서비스 시나리오와 위협요인은 다음과 같다.

교통관리 분야 중 교통신호 관리 서비스, 실시간 라우팅 서비스, 지능형 지도단속 서비스, 주행도로상태 관리 서비스, 대중교통정보 서비스 등의 서비스에 대한 시나리오를 구현해 볼 수 있다.

교통신호 관리 서비스란 USN 기반으로 교통정보를 수집하여 이를 신호 등을 통하여 제어할 수 있는 서비스를 뜻한다. 여기서 중요한 프라이버시 위협으로는 차량에 부착한 Tag ID가 차량 소유자 등 단순한 교통신호 관리 서비스만이 아닌 범죄수사 등에 이용될 수 있다는 것이다. 프라이버시는 '공정한 정보 실천 규약(code of fair information practices)'의 "셋째, 한 가지 목적을 위해 수집·정리된 정보가 그 밖의 다른 목적으로 다시 사용될 때는 반드시 본인의 동의를 얻어야 한다." 를 준수하여야 한다. 따라서 차량의 종류와 차량 소유자의 신원을 확인할 수 없는 정도의 정보만을 가진 태그로 제한하고 철저한 보안 요구 사항을 만족하여야 할 것이다.

USN 기반 지능형 지도단속서비스는 속도위반 차량 단속, 버스전용차선 위반단속, 차로위반단속, 신호위반 단속, 과적 차량 단속으로 구성이 된다. 이들 서비스는 교통단속이라는 유사점이 있으나, 각기 구현되는 기술의 난이도가 확연히 구분될 수 있다.

USN 기반 대중교통관리서비스는 버스의 출발, 도착 정보 제공, 운행관리, 승하차 승객관리 등으로 구성된다. USN 센

서를 가지고 있는 지하철, 택시 관리서비스 등으로 U-city 통합 운영센터에서 관리 운영될 수 있다.

USN기반 주행도로 상태관리서비스는 USN기반의 차량 운행과 관련된 도로 상태를 파악하고 정보를 전달하여 차량 안전운행환경을 구축하도록 한다.

5. 민감한 프라이버시 서비스의 관리적 기술적 대응방안

- 관리적 방안 : OECD 가이드라인, EU 지침 등이 웹 어플리케이션 등을 통해 개인정보에 대한 기술적 보안을 강구하는 방향으로 틀이 개발되어있다. 하지만 세계적으로는 웹 보안의 중요성을 공유한 개인과 기업의 자발적인 참여로 오픈 프로젝트가 진행되고 있다. OWASP(Open Web Application Security Project) Top 10^[9]을 통해 긍정적인 영향을 주고 있는 단체에서 소개한 웹보안의 중요 10가지 점검항목을 살펴보면 다음과 같다.

- 첫째, Unvalidated Input - 입력값 검증 부재
- 둘째, Broken Access Control - 접근통제의 취약
- 셋째, Broken Authentcation & Session Management - 인증 및 세션 관리의 취약
- 넷째, Cross Site Scripting(XSS) Flows - 크로스 사이트 스크립팅의 취약
- 다섯째, Buffer Overflows
- 여섯째, Injection Flows - 삽입의 취약
- 일곱째, Improper Error Handling - 부적절한 에러 처리
- 여덟째, Insecure Storage - 정보 저장 방식의 취약
- 아홉째, Denial of Service
- 열 번째, Insecure Configuration Management - 부적절한 환경설정

- 기술적 방안 : 유비쿼터스 도시의 프라이버시를 보호하기 위한 익명성 보장 기술로는 영지식 프로토콜을 이용한 기술이 있다. 이에 대한 실질적인 도구들 중에서 실질적인 프라이버시를 강화할 수 있는 도구들만을 소개하면 다음과 같다.

- 첫째, Privacy Statement Creation Tools
 - P3P Privacy Statements for Web sites : IBM AlphaWorks, Internet Explorer V6
 - Zero Knowledge Systems(ZKS) : Privacy Rights Markup Language(PRML)
- 둘째, Web Site Scanning Technology
 - Zero Knowledge Systems(ZKS) : ZKS P3P analyzer WatchFire, IDcide 등의 제품 Server logs, web forms, cookies, web beacons 등
- 셋째, Client Privacy Software
 - McAfee's PrivacyService, ZKS's Freedom Suite
- 넷째, Anonymous Web Site Browsing
- 다섯째, Privacy Certification
- 여섯째, Comparison and Missing Pieces

위와 같은 기술들이 유비쿼터스 도시의 구체적인 서비스에 어떻게 적용하게 될 런지에 대한 연구는 첫째, 현존하는 동시대의 동커뮤니티에 속한 사람들이 느끼는 민감도를 반영한 프라이버시 민감도 조사의 통계결과를 사용할 수 있다. 둘째, 델파이 분석 등 전문가 중심의 심층면접 기법을 통하여 이익형량 할 수 없는 성격의 본질적인 개인정보 및 프라

이버시 보호 영역을 설정하는 연구를 진행할 수 있다.

이 부분은 사무국에서 처리하는 부분이다. 머리말 지정은 “보기”메뉴에서 “쪽설정”메뉴에 있는 “윤곽”에서 짝/홀수쪽 다르게 지정을 하고, 글씨체는 “서식” 메뉴에 있는 “글꼴”에서 영문은 Arial체로 하고 국문은 돋움체, 크기는 9pt로 설정한다. 그리고 홀수 페이지 머리말에서는 쪽페이지 번호 위치를 “서식”메뉴의 “탭”명령에서 탭위치를 17cm 오른쪽 지정을 한다. 그리고 짝수 페이지에서는 쪽페이지 번호를 좌측에 한 후, 같은 방법으로 탭위치를 17cm 오른쪽 지정한 후 내용을 작성한다.

VI. 비판

1. 지렛대 · 비용 편익적 분석

고급 정보 수집 능력의 보편화에 따른 글로벌 기업과 개인의 정보수집 능력의 강화가 과거 중앙집권적인 국가 중심의 고급정보 수집이라는 정보의 비대칭성을 기업과 국가로 고르게 분산시켰다. 이는 프라이버시 침해 위협의 주체가 다양해진 것을 의미하며 동시에 프라이버시 침해의 위험이 증가한 것이다.

그렇다면 도대체 왜 이런 현상이 나타났는가? 그 해답을 지식정보 사회의 디지털화가 개인에게 제공한 편의성에서 찾아보아야 할 것이다. 지식과 정보의 디지털화로 개인의 정보가 과거와는 비교할 수 없을 만큼 많이 축적되어 개인의 프라이버시 종말(end of privacy)이 예상되는 시대이지만 이와 동시에 개인에게 매우 높은 편의성을 제공해주고 있다. 이를 현대의 초파놉티콘으로 보고 있다. 즉 현대의 초파놉티콘이란 감시의 공간이기도 하지만 동시에 편리성을 가져다주는 사회적 공인의 공간이기도 하다.

국가 · 기업 · 개인이라는 정보를 관리하고자 하는 주체들은 비용 편익적인 분석을 통해 자신의 논리를 강조하고 당장에 올 편리함으로 장래 다가올 불확실한 위험을 가리려할 뿐 근본적인 해결책을 주장하는 것은 아니다. 더욱 큰 문제점은 비용 편익적 분석은 가치지향적인 분석이 아니라는 점이다. 프라이버시는 단순한 편리함을 얻고 조금 희생해도 되는 비용과 이익이라는 두 가지 가치로 분류될 수 있는 것이 아니다. 결국 경제적 효율성, 사회적 투명성, 개인의 안전이라는 명분 속에 가치가 배제된 한계를 드러내고 있는 것이다.

2. 국가, 기업, 개인별 역상관으로서 프라이버시

역상관(trade off)이란 “양립하지 못하는 상태” 또는 “일치되지 않는 관례”를 뜻한다. 프라이버시에서 이 같은 역상관이란 용어를 사용하는 이유는 유비쿼터스 컴퓨팅 기술을 적용하여 국민(공적), 고객(상업적), 개인(사적)에게 혜택을 주기 위해서는 개인의 프라이버시에 해당하는 정보를 수집 · 활용하여야 하므로 프라이버시 위협이 증대될 것이며, 프라이버시를 보장하기 위하여 개인정보를 수집 · 활용하지 못하게 하면 개인정보를 제공하는 당사자에게 특화된 서비스를 제공할 수 없는 이율배반적인 인과관계를 가지고 있기 때문이다.

이와 같은 역상관을 개인정보 관리 주체인 기업, 국가(행

정, 사법), 개인으로 나누어 볼 수 있다.

첫째 기업과 고객은 경우 고객은 끊임없이 개인정보의 보호를 요구하면서도 자신의 정보를 기업에게 제공해야만 효용이 높은 서비스를 제공받게 되는 역상관의 관계를 가지고 있다.

둘째 국가와 국민의 경우 국민은 태어나면서부터 출생신고에 따른 주민등록번호를 부여받고 주거지에 대한 주민등록을 하며 십자지문을 행정기관에 등록한다. 국민은 국가가 사법기관 등에 제공된 지문 등의 개인정보를 이용하여 범죄 등을 예방하는 안전한 사회를 만들어 줄 것을 기대하며 동시에 개인정보가 악용되거나 타인의 손에 넘어가는 것을 염려한다.

셋째 개인과 개인은 다른 개인의 프라이버시에 관한 정보를 상당부분 소유하게 될 것이며 1인 미디어 시대에 언제든 타인의 프라이버시에 해당하는 정보를 개인의 블로그, 미니홈피, 공유폴더에 올림으로 프라이버시를 위협할 수 있다.

3. 프라이버시 영향평가제도

일부 시민 단체에서 프라이버시 영향평가제도의 조기 도입을 주장하면서 소개되었다. 프라이버시의 보호 영역의 제시, 프라이버시 민감도를 측정함으로 양립할수 없는 프라이버시의 고유 영역 제시, 정보관리 주체별로 프라이버시의 경쟁가치 분석, 세부적인 기술 특성을 고려한 프라이버시 보호 방안 제시 등의 과학적인 연구 자료가 제시되지 않은 현 상태에서 프라이버시 영향평가제도는 실효성을 거두기 어려울 것이다.

VI. 결론

오늘날 프라이버시는 심각한 위협에 처하여 있다. 새로운 커뮤니케이션의 도구들은 상상하지 못했던 서비스를 제공하였고 프라이버시의 새로운 문제들을 불러일으켰다. 하지만 아직도 연구의 결과들은 OECD 및 EU에서 제시한 가이드라인이나 지침을 중심으로 살펴본 추상적인 규제, 프라이버시에 대한 개인 스스로가 자유주의적으로 프라이버시를 보호해야한다는 개념, 두 가지 상반된 가치가 충돌할 때 이익을 행량하여 적절한 균형점을 찾아야 한다는 이익행량의 원칙에 머물러있다.

본 소고에서는 현존하는 연구결과들이 가지고 있는 문제점에 대한 비판을 통해 프라이버시의 보호 영역과 세부 내용이 어떻게 변해나가야 할지에 대하여 유비쿼터스 도시 환경하에서 논증하였다.

연구 결과, 첫째 프라이버시 영역은 유비쿼터스화에 맞추어 개인정보에 국한된 영역에서 주관적이고 상대적인 요인이 보다 넓은 개념의 프라이버시 보호 영역을 설정하여야 한다.

둘째 프라이버시는 양립할 수 없는 절대권적인 보호 영역이 존재한다. 이러한 영역에 대한 이익행량이론이나 비용 편익 분석은 가치유무에 대한 윤리적 의미를 제시하지 못하는 한계를 보여준다. 다양한 이해관계를 조정할 수 있는 균형점을 찾기 위해서는 매트릭스 구조 또는 모델로서 제시할 수 있는 방안을 강구해야한다.

셋째 정량화되지 못한 OECD가이드라인과 EU지침 등의 추상적인 명제를 중심으로 세부적인 방안 수립의 방법론이 효율성을 잃어가고 있다. 보다 현실적인 대응방안을 제시하기 위해서는 프라이버시 민감도 분석, 프라이버시 지수화 개발 등을 통해 프라이버시 측량 도구 및 분석의 틀을 제시할 수 있어야 한다. 그리고 사용자를 중심으로 한 설문 조사, 전문가를 대상으로 한 델파이 조사로 문제에 대한 구체적인 항목들을 도출하는 연구가 수행되어야 한다.

넷째 프라이버시 속에 내제되어 있는 가치들의 이해관계가 대립하여 비용을 낭비하기 전에 정보관리주체별로 프라이버시에 대한 가치를 도출하고 산정할 수 있어야 한다.

다섯째 프라이버시는 다가오는 미래 사회에 가장 보장받기 힘든 문제가 될 것이다. 따라서 프라이버시는 개인의 자유주의적 또는 개인주의적 보호에서 국가, 기업, 시민단체 등의 개별적인 기술에 대한 대책으로 강구되어야 한다.

이와 같은 원칙을 준수하며 유비쿼터스 도시 구축에 따른 프라이버시 위협을 도출하여야 한다. 특히 다양하게 개발되는 서비스 환경에 미들웨어적인 차원에서의 표준화 플랫폼으로 설계 및 구현되는 경우가 아닌 경우에는 다양한 프라이버시 보호 기술이 가지는 서비스마다 구현할 수 있는 한계가 존재할 것이다. 따라서 유비쿼터스 도시 건설 단계에서 기반시설에 대한 보안 기술과 정책의 표준화와 가이드라인 제시가 요구된다.

참고문헌

- [1] 리차드 세버슨, 「정보윤리학의 기본원리」, 철학과 현실사, 2000. p.95.
- [2] Lyon, David, 「전자감시사회」(The Electronic Eye), 한국전자통신연구소, 1994, p. 276 재인용
- [3] 홍영두, “일상적 전자감시와 정보통신윤리-프라이버시, 정체성, 익명성-”, 시대철학, 16(2), 2005, p. 136.
- [4] 강장목, 「강교수의 UC특강, 유비쿼터스 컴퓨팅과 개인 정보」, 인터비전, 2006, p. 168.
- [5] Lyytinen, Kelly, and Youngjin Yoo, "Issues and Challenges in Ubiquitous Computing", Communications of the ACM 45(12), 2002.12.
- [6] 한국전산원, 한국형 u-City모델 제안, 2005., p. 36.
- [7] Telecommunication Act of 1996 SEC. 702. Privacy of Customer Information
- [8] <http://www.owasp.org>, <http://www.imperva.com>, <http://webappsec.org> 참조



정창덕(E-mail : jcd1234@paran.com)

1991 연세대학원 졸업
1996 미국 california cn university 박사
2001 KAIST박사(공학박사)
2006.3 현재 고려대학교 컴퓨터정보학과
교수

관심분야 : 유비쿼터스 센서, 데이터베

이스 보안, 그리드 컴퓨팅, U-city



강장목(E-mail : jcd1234@paran.com)

1999 고려대학교 대학원
(경영학 석사-인터넷 마케팅)
2005 고려대학교 대학원
(공학박사-유비쿼터스 컴퓨팅)
2006. 현재 세종대학교 컴퓨터공학과
교수

1996 ~ 1997 (주) 쌍용정보통신 컨설턴트팀 컨설턴트

2000 ~ 2005 (주) Super Technology 및 (주)세오 연구소장

2001 ~ 2005 서경대학교 컴퓨터공학과 겸임교수

관심분야 : 정보보안, 유비쿼터스 컴퓨팅, 개인정보 등