유비쿼터스 환경의 개인정보 보호를 위한 법률, 제도적 방안

최상호° 이은옥 정미란
동국대학교 교육대학원
whprince° , sprite0g , miranjung@hanmail.net

Protection of private information in Ubiquitous

Sangho Choi° Eunok Lee, Miran Jung
Graduate School of Education of Dongguk Univ.

요 약

유비쿼터스 컴퓨팅환경의 대두로 개인정보 보호에 관한 관심이 더욱 높아졌다. 지금의 사람 대 사람에서의 정보보호뿐만 아니라 그 범위는 사람 과 기계, 기계와 기계, 사물과 사물 간으로 넓어지고 있다. 유비쿼터스 환경하에서의 개인정보침해 사례를 살펴보고, 그에 따른 기술적 대응 방안과 법적 대응 방안을 알아본다. 한계를 보일 수 있는 개인정보보호기술은 개인정보보호정책으로 보안하기 위하여 시급한 법제화가 필요하다.

1. 개 요

개인정보는 인터넷에서 이루어지는 시장 경제의 활성화를 위해 반드시 필요한 것으로, 기업의 입장에서 보면 이러한 개인정보를 통해 온라인의 특성을 활용한 마케팅과 판매활동을 적극적으로 수행할 수 있다. 그러나 개별적인 인터넷 사용자들의 입장에서 볼 때 이들은 자신의 개인정보를 제공함으로써 발생할 수 있는 위험에 대해 매우 우려하는 것 또한 사실이다. 그런 면에서 개인정보 보호기술은 개별적인 사용자 혹은 기술 관리자가 어떠한 경우에 정보를 공개할 것인지에 대한 통제 능력을 부여한다는 점에서 매우 효율적인 프라이버시 보호 솔루션을 제공한다고 할 수 있다.

다시 말하면, 기존의 유·무선 컴퓨팅 환경에서의 정보보호 서비스는 사람 대 사람에서 발생하는 데이터의 secrecy, integrity 및 authentication, 그리고 non-repudiation 가 중요한 정보보호 이슈였다면, 유비쿼터스 컴퓨팅 환경에서는 사람과 기계, 기계와 기계, 사물과 사물 간으로 그 대상이 확장된다. 그러므로 기존의 정보보호 서비스 외에, 각 개체들이 상호 작용함으로써 제기되는 새로운 보안 문제들이 발생할 수 있다. 본격적인 유비쿼터스 시대가 도래하기 이전에 유비쿼터스 환경에 적합한 정보보호 기술에 관한 연구는 무엇보다도 중요하게 다루어져야 할 부분이다.

2. 유비쿼터스 환경 하에서의 개인정보침해사례

많은 사람들이 유비쿼터스 환경으로 인한 삶의 순기능에 대해 이야기하지만 이와 동시에 이로 인해 발생할 수 있 RFID의 확산으로 인한 과다한 개인정보의 수집, 이용과 관련된 이슈가 언론을 통해 논의되는 등 사회 일각에서 유비쿼터스의 역기능, 특히 개인정보 침해를 우려하는 의견이 제기되고 있는 현상은 바람직한 현상으로 생각되며 안전하고 편안한 유비쿼터스 환경을 갖추는 과정에서 개인정보 보호에 대한 공론화는 반드시 필요하다고 할 수 있다. 유비쿼터스 시대에 개인화된 서비스를 제공 받기 위해 자신의 개인정보를 일정부분 공개하는 것은 불가피한 선택으로 다가오고 있다. 이 과정에서 많은 개인정보의 유출, 변조, 오 남용이 급증할 것으로 보인다. 편리함과 개인정보 노출은 이런 Trade-off가 있다. 이 장에서는 유비쿼터스 환경에서 일어나는 혹은 예상되어지는 개인정보의 침해사례를 살펴보고자 한다.

기업의 입장에서 보면 CRM을 위해 보다 정확한 고객의 정보의 확보는 기업의 핵심역량이 되어 가고 있으며 이를 위해 경품, 이벤트, 무료 서비스를 통해 개인정보를 확보하고자 한다. 이로 인해 자신의 주민번호를 익명의 사업자에게 제공하는 가치에 비해 벨 소리 다운로드가 더 가치 있는 것으로 판단해 이벤트에 응모하는 등 개인정보 보호라는 취지에서 보면 이해하기 힘든 상황이 지금도 곳곳에서 벌어지고 있다. 이는 자신의 정보제공으로 인한 대가는 즉시 맛볼 수 있는 반면 그로 인한 피해는 먼 훗날 발생하기 때문에 생기는 착시현상 때문으로 볼 수 있다. 이 경우는 개인이 이벤트에 응모를 했다 하더라도 과도한 정보수집이 되거나 제공 받은 목적 달성 후 개인정보를 파기하지 않고 분석을 통해 다양한 용도로 재활용될 가능

는 역기능에 대해서도 주의를 기울일 필요가 있다. 최근 최근 여러 분야에서 사용되고 있는 RFID의 경우를 한번 살펴보면 실제로 재고관리나 SCM등에서 폭넓게 활용되고 있지만, reader를 사용하면 간단히 그 정보를 인출하는 것이 가능하므로 태그소유자의 개인정보를 입수하는 것이 가능하다. 또한 특정 태그의 정보를 추적함으로써, 태그 소유자의 거주지를 규명한다든지 추적하는 것이 가능하다(Location Privacy). 이 때문에 소매점이 소비자를 추적한다든지, 상품의 유통 정보가 누설되기도 한다. 이 경우 부적절한 모니터링과 분석을 통해 개인의 사생활이 노출되고 개인에 대한 통제행위가 발생할 가능성도 있다. 또한 태그의 취급과 손상에 따른 공방, 수집된 정보의 계열사 이전, 리더기의 변조나 태그절회를 가장한 변조에 의한 정보 수집 등도 예상될 수 있다. [1]
LBS의 경우 영화 " 에너미 오브 스테이트" 를 통해 개인정보의 유출이 사회적으로 떠들썩한 적이 있었다. 이 영화는 국가권력에 의해 위치 정보를 포함한 개인의 모든 정보가 오 남용되는데 대한 문제의 심각성을 다루고 있다. 얼마 전 삼성SDI가 전 현직직원의 휴대전화를 복제해 LBS에 가입하고 직원들을 감시한 예도 대표적인 침해사례라고 할 수 있다. 현재 우리나라에서는 2005년 1월부터 ' 위치 정보의 이용 및 보호 등에 관한 법률' 이 제정, 공표되어 LBS에서 개인의 정보를 다루는데 신중히 접근하도록 하고 있다.
현행의 개인정보 침해가 주로 개인의 신상 및 신용정보 등을 통해 침해사례가 집중적으로 나타난다면, 유비쿼터스 환경에서는 이들의 개인화 경향성에 집중되어 보다 심각한 사회적 파장이 예상된다. 개인에 대한 지배 및 통제를 통한 사회적 문제로 진행될 가능성이 커, 사회적 불안요인 및 계층간 또는 특정 집단 간의 갈등요인으로 발전할 가능성도 상존하고 있다고 보여진다.

3. 개인정보보호기술의 개발과 그 한계

1) RFID태그의 무효화(kill)방법
고객의 프라이버시 보호를 위한 가장 단순한 방법은 상품이 고객에게 인도되기 전에 RFID 태그를 무효화(kill)하는 것이다. 무효화된 태그는 다시는 re-activated 되어 사용될 수 없다. 예를 들면, 어떤 슈퍼마켓에서는 선반에 있는 제품감시 및 재고품 관리를 쉽게 하기 위해 RFID 태그를 사용한다. 고객의 프라이버시를 보호하기 위해, 카운터 점원은 구매된 상품의 태그를 무효화(kill) 할 것이다. 구매되지 않는 상품은 능동 RFID 태그를 가지고 있다. 그러면, 무엇 때문에 무효화(kill)하는 방법은 부적합한 것인가? 그 답은 여러 환경이 있을 수 있으며, 이러한 환경에서 " kill" 과 같은 단순한 방법은 개인 프라이버시 시행을 위해 동작하지 않을 수 있고, 바람직하지 않다. 예를 들면, 고객은 자기가 물건을 소유하고 있는 동안에 동작하는 RFID 태그를 원할 수도 있다. 가정에서 사용하는 예로, 식료품 패키지로부터 요리 방법을 읽어 들일 수 있는 레인지는 능동적으로 동작태그에 의존한다. 유사한 방법으로 RFID 태그를 위해 새롭고 고기능의 고객성이 높다.
태그응용의 다른 예로는 힘들이지 않고서 물리적 접근 제어, 소유물의 도난 방지, 무선 현금 카드 등을 생각할 수 있다.

2) The Active Jamming Approach
RF 신호의 액티브 jamming은 태그 통신을 차폐시키는 다른 형태의 물리적인 방법이다. 고객은 부근에 있는 RFID reader의 동작을 방해하거나 차단시키기 위해 능동적으로 무선 신호를 방송하는 장치를 가지고 다닐 수도 있다. 그러나 고출력으로 방송한다면, 이 방법은 불법이 되며, 조잡한 방법에 지나지 않는다. 또 주위의 모든 RFID 시스템을 교란시킬 것이며, 프라이버시에 관심이 없는 합법적인 시스템도 방해할 것이다.

3) RFID 태그와 Reader의 교신에 암호화 및 인증을 이용하는 방법
RFID 태그와 reader의 교신은 간단히 도청되기 때문에 그 통신에 암호화를 적용한다든지, RFID 태그가 소유자나 특정 reader만 통신이 가능하도록 인증을 이용하는 방법이다. Reader의 능력은 제한되어 있지 않기 때문에, RFID 태그에 써넣을 내용을 암호화하여 써넣은 것이 가능하다. 이것에 의해 RFID태그의 정보가 인출되어도 그 내용을 이해하는 것은 어렵다. 가격은 RFID 태그 당 50원 정도가 바람직스럽기 때문에, RFID 태그에는 한정된 계산 능력밖에 탑재할 수 없다. 이 때문에, RFID 태그가 복잡한 암호화를 처리한다는 것은 현실적으로 어렵다. 이와 같은 이유에서, RFID 태그가 reader를 인증하는 방법을 적용해도, 인증에 필요한 정보를 암호화하여 전송하는 것이 불가능하기 때문에, 도청되어 가장 등의 공격을 받을 가능성이 있다. 따라서 RFID 태그가 특정 reader를 인증하는 것은 곤란하기 때문에, 공격자가 RFID 태그 정보를 인출하는 것을 방지하는 것은 곤란하다.

4. 개인정보보호정책의 나아갈 방향

유비쿼터스 환경에서의 개인정보보호는 기술적인 방책 못지않게 정책적인 면도 중요하다고 할 수 있다. 기술적인 면의 외부적인 제약요인과 내재적 한계는 정책 및 법제도적 뒷받침을 통해 보완되어야 한다. 그러나 아직까지 관련 논의가 활성화되지 못하고 있으며 정책적 뒷받침도 마련되지 않은 상태이다. 우리나라의 경우, 보다 앞서 법제화 작업이 진행중인 유럽이나 미국의 개인보호정책을 본보기 삼아 다음과 같은 내용을 정책적으로 만들어 가야겠다.[5]

1. 익명권의 보장
유비쿼터스 환경에서 익명화 기술에 관한 이야기들이 나오고 있는데 이를 널리 적용하기 위해서는 익명권을

의존형 응용이 나타날 것이다. 일반 고객을 위한 RFID 표현도 표현의 자유로 인정한 미국과는 달리 그 범위가 모호한 상태이다. 또한 현행 정보통신망법도 익명화 기술이 개발되고 활용될 수 있는 법적 조건을 확보하지 못하고 있다. 이러한 규정을 확실히 검토해야 할 필요성이 높다고 하겠다.

덧붙여서 서비스 이용 시 중간매개자가 보유하고 있는 이용자의 신원정보에 대한 국가 등 제 3자로부터의 공개요구에 대해 중간매개자가 이를 거부할 수 있는 법적 보장도 시급하다고 하겠다. 현행법이 이전보다 통신비밀의 보장을 강화하고 있기는 하나, 그 동안의 경험과 관행에 비추어보면 유비쿼터스 환경의 이용자 익명성 보호에는 충분치 못한 것이 사실이기 때문이다.

2. 정보시스템의 기술적 표준화와 인증제의 활용 필요

현행 정보통신망법 제 8조(정보통신망의 표준화 및 인증) 는 정보통신부장관은 정보통신망의 이용촉진을 위하여 " 정보통신망에 관한 표준" 을 정하고 이를 고시하며, 그 사용을 정보통신서비스제공자 또는 정보통신망과 관련된 제품을 제조 또는 공급하는 자에게 " 권고할 수 있다" 고 규정하고(제1항), 그 효율적인 시행을 위한 인증제도를 마련해 놓고 있다(제2항). 그런데 표준화의 대상, 방법, 절차를 위임 받은 정보통신부령에는 이에 관한 아무런 규정이 없는 상태이다. 유비쿼터스 환경하의 개인정보보호를 위해 프라이버시보호기술의 시장형성을 촉진시킬 표준 및 인증제도를 적극 이용해야 하겠다.

3. 정부기금에 의한 PETs 연구 및 개발 촉진

정보통신망법 제 6조(기술개발의 추진 등)에 의하면, 정보통신부장관은 정보통신망과 관련된 기술의 개발을 추진하기 위하여 관련 연구기관으로 하여금 연구개발, 기술지도 등의 사업을 하게 할 수 있다고 규정하고, 그러한 사업을 실시하는 연구기관에 대하여는 그 사업에 소요되는 비용의 전부 또는 일부를 지원할 수 있다고 규정하고 있다.

이 규정에 따라 정보통신부장관은 PETs의 개발 및 보급을 위한 사업에 역점을 두고, 정책을 시행함에 있어서 우선 순위를 두어야 할 것이다.

4. 개인정보보호지침상의 기술적 대책의 강화를 통한 보안시장의 활성화

정보통신망법 제 28조는 "정보통신 서비스 제공자 등은 이용자의 개인정보를 취급함에 있어서 개인정보가 분실,도난, 누출,변조 또는 훼손되지 아니하도록 안전성 확보에 필요한 기술적, 관리적 조치를 강구하여야 한다 ." 고 규정하고 있다. 그러나 이러한 기술적 보호조치 의무는 법률상 아무런 강제장치가 없는 단순한 권고사항에 불과하다. 보안시장을 활성화하기 위해서는 이러한 보호조치 의무를 강화하고 실효적인 것이 되도록 하여야 할 것이다. 또한 개인정보보호등급제나 개인정보마크제의 도입을 통해 이를 실현하는 방안도 검토할 필요가 있다.

법적으로 보장하여야 한다. 그러나, 우리나라는 익명

5. 이용자 프로파일에 대한 명확한 법적 기준의 설정

현재 인터넷상에서는 쿠키 등을 통해 광범위한 개인정보를 수집, 처리하고 있다. 유비쿼터스 환경에서도 서비스를 제공 제공자가 이용자의 광범위한 개인정보 수집이 예상된다.

독일 멀티미디어법(TDDSG) 제4조 제4항은 " 이용자 프로파일은 가명이 사용되는 조건 하에서 허용된다. 가명으로 검색할 수 있는 프로파일은 그 가명의 주체에 관한 자료와 결합되어서는 아니 된다." 고 하여 인터넷에서 profiling 기술의 개발을 사실상 통제하고 있다. 유비쿼터스 환경에서도 개인정보 수집의 한계 등에 대하여 명확하고 구체적인 법적 기준이 설정되어야 할 것이다. 그밖에 스파이웨어 등 다른 도구를 통한 정보수집에 대한 법적 대응방안도 강구되어야 할 것이다.

5. 결론

우리 사회의 빠른 정보화시대로의 변화로 인해 사용자들은 점차 의식하지 못한 채 자의, 타의에 의해 개인 정보를 침해 당하고 있다. 유비쿼터스 환경의 도입으로 개인에 대한 일거수일투족을 모니터하고 기록하는 기형적인 모형으로 변화가 가속화 될 것이다. 이에 대해 개인정보보호기술의 개발과 적용의 확대는 유용한 대안일 수 있다. 그러나 개인정보보호기술이 가지고 있는 외부적 및 내재적 제약요인 때문에 기술 자체만으로는 유비쿼터스 환경에서 익명성과 개인정보를 보호하는 데에는 역부족이다. 법과 기술이 함께 개인정보보호체계를 구축해야 할 것이다. 그러기 위해서는 결국 사회의 모든 구성원들이 개인정보보호의 중요성을 인식하고 시급한 문제로 받아들이는 문제의식이 우선되어야 할 것이다.

Reference

[1] 김태중 김인호 연구원, " 유비쿼터스 환경하에서의 개인정보 관리체계에 관한 연구" , 정보보호뉴스 2005년 3월호 13페이지

[2] Junichiro Saito and Kouichi Sakurai, "Privacy Protection Using Re-encryption in RFID Tags," Technical Report of IEICE ISEC2003-81, Nov. 2003.

[3] A.Juels, "Privacy and Authentication in Low-Cost RFID Tags," 2003. http://www.resasecurity.com.

[4] A.Juels, R. Rivest, and M. Szydlo, "The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy," 2003, http://www.rsasecurity.com.

[5]Buckley v. American Constitutional Law Found., 525 U.S. 182 (1999)

[6]Michael Froomkin, Anonymity and Its Enmities, 1995 J. ONLINE L. art. 4 (1995)