http://dx.doi.org/10.15813/kmr.2015.16.3.002

사물인터넷 환경에서 사용자 프라이버시 우려에 관한 연구: 운동추적기 사례를 중심으로*

Users' Privacy Concerns in the Internet of Things (IoT): The Case of Activity Trackers

배 진 석 (Jinseok Bae)

현대오토에버 (jbae@hyundai-autoever.com)

정 윤 혁 (Yoonhyuk Jung) **

울산과학기술원 경영학부 (yjung@unist.ac.kr)

조 우 제 (Wooje Cho)

서울시립대학교 경영대학 (wjcho1@uos.ac.kr)

ABSTRACT

최근 등장한 IoT(Internet of Things)는 개인과 기업에게 효율성 및 편의성을 제공해 줄 것으로 예상되는 기술로 주목받고 있으며, 이에 대한 관심과 투자가 점점 증가하고 있다. IoT의 정착은 빅데이터를 생성시키는 환경을 만듦으로써, 빅데이터분석을 통해 사회전반에 걸쳐 효율성을 증대시킬 뿐만 아니라 새로운 서비스 창출의 기반이 될 수 있다. 하지만 일각에서는 IoT 기술이 새로운 가치를 제공해 주는 이면에, 다양한 프라이버시 침해요소가 존재한다고 주장한다. 사용자가 IoT 서비스를 사용할 때 느낄 수 있는 프라이버시 침해에 대한 우려는 장기적으로 사용자의 수용을 저해할 수 있기 때문에, IoT 산업의 빠른 발전속도에 제동을 걸 수 있다. 따라서 본 연구에서는 IoT 환경에서 발생할 수 있는 사용자 프라이버시 침해를 세 가지 측면(기술적 위협, 서비스제공자의 위협, 정책에 대한 신뢰)에서 살펴보고 프라이버시 우려에 미치는 영향 수준을 비교해 보고자 한다.

Despite much interest and investment in the Internet of Things (IoT) which expand the Internet to a ubiquitous network including objects in the physical world, there is growing concerns of privacy protections. Because the risk of privacy invasion is higher in IoT environments than ever before, privacy need to be a key issue in the diffusion of IoT. Considering that the privacy concern is a critical barrier for user to adopt information technologies, it is important to investigate users' privacy concerns related to IoT applications. From the triad perspective (i.e., risk on technology, risk on service provider, and trust on legislation), this study aims to examine users' privacy concerns in the context of activity trackers.

Keywords: Internet of Things, IoT, Privacy, Activity tracker

* 본 논문은 2013년 한국연구재단의 사회과학지원사업(SSK)의 지원을 받아 수행된 연구임 (NRF-2013S1A3A2043357).

• 논문접수일: 2015년 4월 7일; 1차 수정: 2015년 6월 4일; 2차 수정: 2015년 7월 6일; 게재확정: 2015년 7월 23일

** 교신저자

I. 서 론

E-커머스(E-commerce)에 이어 M-커머스(M-Commerce)에 이르기까지 정보통신기술의 비약적인 발전은 새로운 환경변화를 이끄는 촉매가 되어 왔다. 최근 등장한 IoT(Internet of Things: 사물인터넷) 또한 새로운 환경을 가져 올 정보기술로써 산업계를 비롯한 소비자들에게 관심을 불러일으키고 있다. IoT는 우리가 주변에 있는 사물들이 센싱과 통신기능을 포함함으로서 서로 간에 네트워크가 연결되어 사람이 개입하지 않는(혹은 최소 개입) 상태에서 정보를 수집, 가공, 처리하는 시스템을 의미한다 (Atzori et al., 2010).[1] CISCO (2011)에 따르면 이미 인터넷에 연결된 사물들(Things)이 2008년에서 2009년 사이 기간 동안 전 세계 인구를 이미 초과하여 초연결시대가 도래했음을 알렸다. 가령, 전력회사 들은 웹에 연결된 스마트 계량기를 고객들의 시설에 배치함으로써 전기, 수자원 등을 효율적으로 운용하기 시작하였으며, 개인은 일상에서 생성되는 데이터(식사량, 혈압, 기분 등)을 웨어러블 디바이스를 통해 정량적으로 수치화함으로써 맞춤형 의료서비스의 기초 자료로 활용하고 있다. 최근에는 IoT 기술을 활용하여 재난발생대응 시스템 개발도 진행되고 있다 (Yang et al., 2013). 이처럼 IoT 환경에서는 네트워크에 연결된 사물이 방대한 양의 정보와 지식이 생산, 교환되기 때문에 인간이 과거에 경험하지 못했던 다양한 새로운 가치를 제공할 수 있다. 그러한 방대한 데이터에 기초한 기업의 전략수립과 새로운 서비스 창출은 데이터분석에 기초한 지식경영, 사회적 효율성 제고에 이바지할 수 있을 것으로 예상된다(심재문, 권오병, 강지욱, 2010).

하지만 IoT 기술이 가져다주는 효율성 및 편의성으로 관련 산업의 성장이 예고됨에도 불구하고, 일각에서는 사용자들의 프라이버시 침해와 관련된 문제를 우려하는 목소리가 적지 않다 (Medaglia & Serbanati, 2010). 모든 기기들이 인터넷으로 연결되는 IoT 환경에서는 그 만큼 외부의 해커들이 원격으로 해당기기를 조작하거나 정보를 빼낼 수 있는 위험이 존재하기 때문이다. 또한 IoT 기술에 대한 성급한 사업화로 수년전 구축된 네트워크와 웹, 그리고 물리적 보안 환경 하에서 IoT 상품 및 서비스가 출시되기도 하는데, 이때 하나의 기기가 외부로부터 침해를 당하면 다른 기기 또한 공격에 휩싸이며 순식간에 개인정보 유출과 관련된 사회적 이슈로 불거질 수 있다. 사용자 프라이버시 이슈는 IoT 디바이스를 통해 수집된 데이터의 저장 및 활용에 있어서 사용자의 민감한 개인정보가 노출되거나 본래의 목적과 다르게 사용할 때 발생할 수 있다 (Genaro & Caine, 2014). 셀프트래킹을 하기 위한 IoT 서비스의 경우 해당 디바이스에 저장되어 있는 위치정보, 신용정보, 생활습관 정보 등 개인의 프라이버시와 관련된 정보들이 IoT 서비스 계정에 자동으로 동기화되고, 백업이 되기 때문에 개인의 사생활을 심각하게 침해할 소지가 있다. IoT 서비스 사용자들은 IoT 계정에 저장된 사용자 개인 정보들을 기업이 어떻게 사용하는지 알 수 없기 때문에 불안감을 느끼고 있으며, 전문가들은 서비스 제공자들이 새로운 서비스 또는 상품 개발로 자신들의 비즈니스를 확장하기 위해 사용자의 개인정보를 무분별하게 사용할 경우 사용자들의 프라이버시가 심각하게 침해 될 수 있다고 주장하고 있다. 이러한 프라이버시 이슈들은 개인을 넘어 사회적인 문제를 낳을 수 있다는 점에서 우려할 만하다 (Margulis, 2003). 실제로 미국, 영국, 네덜란드에서는 시민단체를 중심으로 웨어러블 디바이스의 개인정보유출과 프라이버시 침해를 우려하여 웨어러블 디바이스 출시 반대 운동이 추진되고 있다. 프라이버시 이슈로 인한 불안감은 사용자들이 IoT

1) 본 연구는 포괄적으로 IoT를 정의하여 wearable computing을 IoT환경의 기반기술이자, 초기 IoT서비스로 간주하여 IoT의 영역에 포함시킨다 (한국정보화진흥원, 2014; Thierer, 2014).

의 확산을 더디게 할 수 있다.

정보시스템 분야에서 정보프라이버시에 대한 우려는 오늘날의 기술기반 환경에서 기술수용과 관련한 가장 중요한 요인 중의 하나이다(Stone & Stone, 1990). 사용자의 정보프라이버시에 관련한 이전의 연구들에 따르면, 프라이버시 우려는 소비자의 기술 수용에 있어서 주요한 억제요인으로 분류 된다 (Goodhue & Straub, 1991). 역사적으로 인터넷상에서 인간의 활동이 증대될수록, 정보프라이버시 침해의 위험 역시 증가하고 있으며 (Hann, et al., 2002), 온라인 거래에 있어서 프라이버시 침해 문제에 대한 소비자의 우려는 전자상거래의 성장을 저해하는 중요한 요인으로 언급되어 왔다 (Mahotra, et al., 1999; Mineta, 2000). 마찬가지로, IoT 또한 산업 활성화를 위해 프라이버시 문제 해결이 선행되어야 할 것으로 전망된다.

IoT 서비스 산업이 더욱 활성화되기 위해서는 IoT 환경에서 발생할 수 있는 정보프라이버시에 대한 이해가 필요함에도 불구하고, 현재 IoT 서비스 환경에서의 사용자의 프라이버시 침해와 관련된 연구의 대부분은 개념적 논의에 그치거나, 공학적 관점에서 프라이버시를 보호하기 위한 기술 설계에 관련된 연구에 집중되어 있는 실정이다. IoT 기술의 초기 서비스라고 할 수 있는 위치기반서비스 맥락에서 프라이버시 위험을 다룬 연구들이 수행되었지만(예, Xu & T대, 2004; Xu et al., 2011), 본격적인 IoT서비스의 시작이라고 할 수 있는 웨어러블 컴퓨팅 디바이스의 프라이버시 이슈에 대한 경험적(empirically) 연구는 드문 실정이다. IoT 서비스 활용에 있어서 소비자들이 어떠한 프라이버시 침해에 대한 우려를 가지고 있으며, 이러한 프라이버시 침해 우려에 영향을 미치는 요인들의 수준을 파악하는 것은 앞으로 IoT서비스 산업의 성장에 있어 의의가 있다. 이에 본 연구에서는 최근 인기를 얻고 있는 웨어러블 디바이스인 액티비티 트래커 (Activity tracker)[2]에 대해 세 가지 관점(기술적 위협, 서비스 제공자의 위협, 정부에 대한 신뢰)에서 사용자들의 프라이버시 우려 수준을 탐색하고자 한다.

2. 기존문헌 연구

2.1 정보프라이버시에 대한 논의

프라이버시의 의미는 시대가 직면하고 있는 상황에 따라 진화하고 있다. 고전적 의미의 프라이버시(Privacy)는 "외부의 간섭이나 침해로부터 벗어나 자유롭게 혼자 있을 수 있는 권리"로 정의 된다 (Warren et al., 1890). 즉, 통제되어야 하는 개인이나 조직의 권리를 말하며, 개인이나 조직은 정보를 소유하면서 허가 없이 사용해서는 안 되며, 조직에 속하는 개인 신상정보는 인사나, 고용, 작업, 서비스 등과 관련 없는 다른 개인이나 조직사이에서 부당하게 수집, 배포되거나 사용되어서는 안 된다 (Garfinkel & Rosenberg, 2006).

통신기술의 발전은 사용자와 기업가 정보를 쉽고 빠르게 유통시킬 수 있게 하였고, 이에 프라이버시의 범위 또한 확장되었다. 즉 정보의 확산속도가 빨라지고, 관련된 이해관계자들의 다양하고 민첩하게 행동하기 때문에, 사용자가 온라인상에서 자신의 프라이버시를 통제하는 것이 더욱 어려워지고 있다. 하지만 프라이버시는 사용자와 기업과의 관계에 있어서 보호해야 하는 중요한 문제이고, 기업은 프라이버시를 보호하고 안전하게 고객에게 서비스를 제공하는 것이 고객에게 신뢰를 제공하는 방법이다. 따라서 과거와 달리 고립적이고 배타적인 방식을 통해 프라이버시를 보호하는 것이 불가능하기 때문에, 자신에 관한 정보를 통제하는 권리로써 정보프라이버시(Information privacy)

2) 개인의 건강정보, 행동정보 등 라이프로그(LIfe log)를 정량화, 수치화 하기 위해 활용되는 웨어러블 형태의 대표적인 IoT 서비스 사례

가 제안되었다. 정보프라이버시는 자신의 개인정보에 대한 배타적 통제권을 가질 권리를 말하며, 다른 사람이나 기관에 공여된 자신의 개인정보가 유통되거나 활용될 때 관여할 수 있는 권리를 포함한다 (Regan, 1993). 이러한 정보프라이버시는 '개인정보에 대한 자기결정권'으로 정의되기도 한다 (Mayer-Schönberger, 1997). 따라서 사용자들은 어떠한 서비스를 사용할 때 자신의 정보가 어떠한 방식으로 수집되고, 활용, 공개되는 과정에 참여하며, 자신의 정보를 통제할 수 있어야 함을 말한다 (Culnan, et al., 2003; Westin, 1967).

오늘날에는 대다수의 소비자들이 정보프라이버시와 관련된 문제를 인지하고 있으며, 이러한 정보프라이버시 침해는 주요한 사회문제 중 하나로 부각되고 있다 (Hui et al., 2007). 정보프라이버시의 위험은 사용자가 개인정보를 기업에 제공하는데 있어서 잠재적으로 높은 손실이 발생할 수 있다고 인지하는 정도를 뜻한다 (Malhotra, et al., 2004). 특히 요즘의 정보들은 디지털 형태로 되어 있기 때문에 쉽게 복사할 수 있고, 전달, 통합이 가능하기 때문에 (Malhotra, et al., 2004), 기업은 개인을 쉽게 프로파일화 할 수 있다. 즉, 과거와 비교해서 개인이 위협에 쉽게 노출될 수 있는 환경이 만들어졌다. 따라서 개인은 자신의 정보에 대해 통제하고 관리 할 수 있어야 한다. 물론, 기업들은 사용자들의 개인정보를 활용하여 개인화, 맞춤화된 서비스를 제공하는 등, 사용자에게 이익을 제공할 수 있다 (Malhotra, et al., 2004). 예를 들면, 고객에 대한 정보, 맞춤화된 상품 및 서비스는 사용자의 거래시간을 단축시키고, 비용을 줄이면서 소비자의 만족을 향상시킬 수 있다. 따라서, 서비스 제공자가 사용자의 정보를 잘 활용한다면 이익을 향상시킬 수 있지만, 활용이 잘 이루어지지 않으면 사용자가 정보프라이버시의 위협에 노출 될 수 있다.

기존의 여러 실증연구의 결과에 따르면, 인터넷 환경에서 정보프라이버시 위험이 사용자가 정보를 제공하는데 부정적으로 작용하며 (Xu et al., 2009), 서비스 수용의도에도 부정적인 영향을 미치는 것을 볼 수 있다 (김병수, 2012; Fetherman, et al., 2003). IoT 서비스는 기술의 특성상 기기에 포함되어 있는 여러 가지 센서를 통해 실시간으로 사용자의 정보를 수집하여, 분석, 활용하는 것을 목적으로 한다. 더불어 위치정보를 포함한 사용자의 개인 정보들이 무선네트워크, 블루투스 등 무선으로 교환되기 때문에 프라이버시의 침해의 가능성에 대한 우려가 높아지고 있다. 물론 사용자가 IoT 서비스를 사용하여 이전에 없던 편리함과 유용함을 가질 수 있지만, 프라이버시 침해에 대한 우려와 불안감을 감수하면서 새로운 기술을 사용하려고 하지 않을 것이다. 이전의 연구에 따르면 새로운 기술의 도입에 있어서 프라이버시 침해에 대한 우려는 사용자들이 느끼는 우려 중 하나의 중요한 요소에 해당한다고 볼 수 있다(Culnan & Armstrong, 1999).

또한 사용자들은 기업들이 자신들의 정보를 동의 없이 활용하고, 프라이버시를 침해 할 것이라는 염려 때문에 자신의 정보프라이버시에 대해 확신을 하지 못하기 때문에 (Hann et al., 2002), 사용자들의 프라이버시 우려를 감소시키는 것이 중요하다. 사용자의 프라이버시 우려를 감소시키는데 있어서 기업과 정보의 역할이 중요하다 (Xu & Teo, 2004). 따라서 기업들의 서비스를 제공하기위해 사용자들의 개인정보를 사용하는 방식과 사용자의 프라이버시를 보호하고 구제하기 위한 정부의 방안은 사용자가 IoT 서비스를 받아들이는데 영향을 미칠 것으로 예상된다.

2.2 IoT 환경에서의 프라이버시 이슈

사용자가 언제 어디서나 정보에 접근하고 활용할 수 있는 유비쿼터스 사회는 IoT 기술의 출현으로 보다 구체화 되었다. IoT 기술은 네트워크로 연결된 디바이스들이 사용자의 개입 없이 스스로 커뮤니케이션 하며

정보를 수집, 저장, 활용하여 인지된 상황을 통제할 수 있는 기술을 의미한다. IoT 제품이나 서비스에 사용되는 IT 기술(RFID, GPS, WSN 등)들은 IoT 디바이스들을 확인하고, 추적할 수 있는 능력이 있다 (Sheng et al., 2008). 앞선 기술을 통해 정보를 수집, 저장, 활용하면서 사용자의 이익과 가치를 향상할 수 있고, 또한 서비스 제공자의 수익을 높일 수 있다 (Sheng et al., 2008).

네트워크, 어플리케이션, 디바이스, 데이터 동기화 등의 기술은 고객의 니즈를 만족시키는 다양한 IoT 제품과 서비스를 실현할 수 있게 하였다 (Sheng, et al., 2008). IoT 환경에 사용되는 정보들은 3가지 측면으로 특징지어진다 - 신원정보, 시간정보, 그리고 위치정보 (Junglas & Watson, 2006). 신원정보는 IoT의 중요한 특징으로써, 디바이스에 저장된 정보를 통해 사용자의 개인정보, 위치정보, 상태정보를 실시간, 지속적으로 확인할 수 있다 (Roussos. et al., 2003). 기업은 이러한 정보를 통해 사용자가 누구인지(who they are), 무엇을 원하는지(what they want)를 파악할 수 있다 (Watson et al., 2002). 시간정보 또한 중요한 특징으로써 (Sheng et al, 2008), 디바이스에 저장되는 정보의 시간적인 속성을 의미하며, 기업은 이러한 정보를 실시간으로 파악하고 분석하여 고객의 니즈에 실시간으로 대응할 수 있게 되고, 고객은 실시간으로 분석되어 제공되는 매끄러운 서비스를 통해 편리하고 유용함을 느낄 수 있다. 위치정보는 또 다른 중요한 정보로써 (Junglas & Watson, 2006), IoT 디바이스 내의 GPS나 RFID의 추적을 통해 디바이스나 사용자의 위치 정보를 인식할 수 있다 (Xu & Teo, 2004). 사용자의 위치의 추적을 통해, 사용자의 패턴을 분석하고, 사용자의 니즈를 더 잘 파악할 수 있어서 더욱 가치가 부가 된 서비스가 제공된다.

과거 온라인 프라이버시 이슈나 모바일 프라이버시 이슈들처럼, IoT 환경에서도 네 가지 측면(정보의 수집, 저장, 사용, 노출)에서 프라이버시 이슈들이 존재한다. 컴퓨팅 디바이스가 장착된 물체들은 사용자의 상황을 인식하고, 사회 곳곳에 존재하기 때문에 IoT 환경에서는 과거 온라인 프라이버시 이슈나 모바일 프라이버시 이슈들 보다 더욱 복합적이고 심각하게 발생할 것이다 (Thierer, 2014). IoT 환경에서 사용자들의 대표적인 프라이버시 우려는 1) 사용자에 관해 수집되는 정보의 종류, 2) 정보에 접근하는 단체, 3) 어떻게 정보가 사용되는지, 4) 개인정보의 분실이나 허가되지 않은 사용에 대한 보호여부, 5) 중요하고 민감한 정보를 수집하는 단체에 대한 신뢰성 과 관련 있다 (Galanxh & Nah, 2006). 또한 IoT 환경에서 사용자의 프라이버시 침해는 1) 사용자의 정보에 지속적으로 접근이 가능하고, 추적할 수 있으며 2) 디지털 정보의 특성상 쉽게 사용되고, 되는 특징을 가지고 있기 때문에 발생한다 (Günther & Spiekermann, 2005).

사물이 지닌 인터넷 기능은 그들을 보다 지능적이고 상호작용적이게 해준다 (Sheng et al, 2008). 이처럼 스마트 오브젝트[3]의 다른 사물들과 네트워킹 할 수 있는 능력은 다른 사물과 환경, 그리고 과거의 시스템에까지 연결되어 서로 상호작용 할 수 있다 (Medaglia & Serbanati, 2010). 스마트 오브젝트는 다양한 네트워크를 통해 그들의 상황 또는 주변 환경에 대한 정보를 인식하고 수집하여 RFID와 같은 저장소에 저장한다. 스마트 오브젝트들의 상호작용 또는 데이터 전달은 자동으로 그리고 지속적으로 발생하기 때문에 새로운 프라이버시 이슈가 발생 한다 (Medaglia & Serbanati, 2010). RFID의 경우, 저장되어 있는 정보를 무선으로 확인하기 때문에 사용자에게 편리함을 제공하지만, 허가되지 않은 RFID 리더기가 정보를 인식할 수 있고, 허가되지 않은 정보가 RFID 리더기를 통해 수집될 수 있기 때문에 의도하지

3) 인터넷 접속 제어 기능이 내부에 구축되어 언제 어디서나 온라인에 손쉽게 접속할 수 있도록 해 주는 지능형 전자 기기.

않게 사용자의 프라이버시가 노출 될 수 있다.

컴퓨터의 소형화와 저전력 기술은 스마트 오브젝트를 오래 동안 사용하고, 휴대가 가능하게 만들었다. 이러한 기술의 발달은 IoT 제품 및 서비스가 빠르게 보급되는 원동력이 되었다. 하지만 사용자는 소형화된 컴퓨팅 센서가 사물의 어디에 부착되어있는지 알 지 못하고, 데이터의 교환이나 수집이 이루어질 때 음향이나, 시각적인 표시가 없기 때문에 사용자는 데이터를 잃거나 자신이 추적당하고 있는 상황을 인지하지 못 한다 (Weber, 2010). 또한 휴대가 가능한 특성은 스마트 오브젝트의 이동성을 강화하였다. 이를 통해 사용자들은 보다 다양한 장소에서 정보가 유출될 수 있는 가능성을 가지게 되었으며, 특히 다른 나라, 장소에서 프라이버시 위협에 노출 되었을 때 프라이버시 구제의 어려움을 겪을 수 있다.

모바일 스마트 오브젝트의 특징 중의 하나는 위치 기반의 정보를 수집한다. 위치를 인식하는 IoT 제품이나 서비스는 과거에 비해 저렴하고, 정확하게 위치정보를 수집할 수 있다. 기업은 시간과 위치정보를 수집하여 사용자의 니즈를 충족시킬 수 있는 다양한 제품과 서비스를 제공 할 수 있게 되었다. 위치 인식 모바일 디바이스를 통해서 우리의 삶의 안정성, 편리성, 유용성이 보다 강화되었다 (Minch, 2004). 하지만 사용자의 위치정보의 수집, 저장, 사용 및 노출로 인해 사용자는 정보 프라이버시 이슈뿐만 아니라 물리적인 프라이버시 이슈의 위협의 가능성이 생겼다. 예를 들면, 기업은 그들의 마케팅활동을 위해 쇼핑이나 여행 패턴을 기반으로 사용자를 프로파일링 할 수 있다. 사용자들은 글들의 위치정보가 노출되면서 스토커의 위협에 시달릴 수도 있다 (Minch, 2004).

또한 IoT 환경에서는 기업과 이해관계자들 간의 거래를 지원한다. 이해관계자는 고객, 공급자, 정부, 매니저, 직원 등을 포함 한다 (Junglas and Watson, 2006). 기업은 IoT 기술을 활용하여 다양한 환경의 정보들을 수집, 저장, 활용하고자 한다. 기업은 사용자들의 니즈를 파악하고, 마케팅정보로 활용하고, 제3자에게 판매를 통한 수익을 올리기 위해 고객의 데이터를 프로파일링, 마이닝한다 (Galanxh & Nah, 2006). 특히 서비스제공자들은 사용자의 정보(개인정보, 위치정보, 상황정보)를 수집하여 개인화, 고객화 된 서비스를 제공할 것이다. 개인화된 서비스는 사용자에게 편리함과 가치를 제공하지만, 이를 위해서 사용자는 지속적으로 정보가 수집되고 추적 되어야한다. 기업은 개인화된 제품이나 서비스를 제공하기 위해 사용자의 정보를 가능한 한 많은 획득하고자 하기 때문에 사용자에게 개인화된 서비스를 사용하기 위해서는 그들의 어느 정도의 개인정보를 포기하려 할 것을 요구 한다 (Adomavicius & Tuzhilin, 2005). 사용자는 그들의 개인 데이터들이 허가받지 않은 외부 자원들에 의해 그들의 동의 없이 사용될까 우려한다 (Roussoes et al., 2002). 이러한 것들이 사용자의 프라이버시 우려를 증가시킨다 (Culnan & Armstrong, 1999).

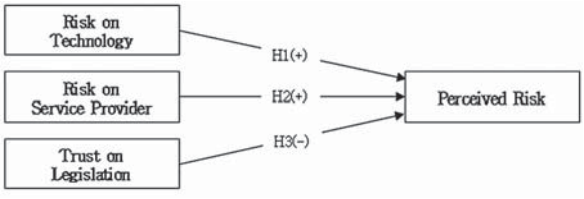
IoT 환경에서는 모든 물체들에 컴퓨팅 디바이스들이 들어있고, 네트워크를 통해서 물리적인 환경들과 엮여 있다. M2M기술을 통해서 사용자들은 편리하고, 유용한 서비스를 서비스 제공자로부터 제공받을 수 있다. 하지만 이러한 엄청난 혜택이 사용자에게 제공됨에도 불구하고, 사용자의 프라이버시 우려는 IoT 제품이나 서비스를 수용하는데 있어서 큰 장애와 사회적 문제가 될 것으로 보인다 (Asif, 2005).

3. 연구모형 및 가설

3.1 연구모형의 설계

본 연구 에서는 IoT 환경 하에서 세 가지 요인(기술적인 위협, 서비스 제공자의 위협, 정부에 대한 신뢰)을 통해 사용자의 인지된 프라이버시 우려의 수준을

확인하고자 사용자 프라이버시와 관련된 선행연구를 참고하여 <그림 1>과 같은 연구모형을 구성하였다.



[그림 1] 연구모형

3.2 가설설정

본 연구 에서는 연구모형에 포함된 독립변수(기술에 대한 위험, 서비스 제공자에 대한 위험, 프라이버시 법률에 대한 신뢰) 및 종속변수(인지된 위험)간의 인과관계를 통계적으로 검증하기 위하여 선행연구들을 바탕으로 다음과 같은 연구 가설을 설정하였다.

3.2.1 Perceived risk(RISK)

지각된 위험(Perceived risk)이라는 개념은 Bauer(1960)에 의해 마케팅 분야에서 처음 소개되었다. 지각된 위험은 객관적 위험과는 다르게 소비자가 브랜드/상점/구매 방식 등의 선택상황에서 주관적으로 인식하는 위험으로 정의 된다. 즉, 지각된 위험은 상품 또는 서비스의 불확실성에 대한 인지가 구매의 결과로 이어지는 것을 의미한다 (Grahame & Richard, 1994). 특히, 온라인 쇼핑과 같은 온라인 환경에서의 재구매에 있어 지각된 위험을 감소시키는 것이 중요하며 (Chiu et al., 2014), 개인신상정보와 관련된 프라이버시위험이 주요한 위험유형으로 분류된다 (Jarvenpaa & Todd, 1997). 따라서 본 연구에서는 사용자의 프라이버시와 관련한 지각된 위험이 미래에 IoT 서비스를 수용하는데 있어서 중요한 요소로 본다.

3.2.2 정보기술로부터의 위험 (TECHNOLOGY)

IoT 기술과 관련한 프라이버시 침해는, 서비스를 사용하는데 있어서 발생하는 데이터를 수집, 저장, 사용할 때 발생할 수 있다 (Minch, 2004). IoT 서비스는 기술의 특성상 프라이버시 침해가 발생할 요인들이 다수 존재한다. 예를 들어, 기기 간에 무선으로 데이터를 송/수신하는 경우 외부의 침입을 통해 프라이버시 침해가 발생할 수 있고, 또한 서버에 수집, 저장된 데이터를 활용하는 과정에서 개인 정보가 부적절하게 사용되거나 노출 될 수 있다. 서비스에 사용되는 기술들이 공정하고 합법적인 방식으로 사용자의 정보를 수집, 저장, 사용한다고 느껴질 때, 사용자들은 IoT 서비스를 신뢰하며 사용할 것이다. 하지만 이러한 기술에 대한 이해와 통제가 부족하다고 인식할 때 사용자는 프라이버시가 침해된다고 생각한다 (Culnan, 1993).

[가설 1] 개인정보 유출과 관련된 정보기술에 대한 위험은 지각된 프라이버시 위험을 증가시키다.

3.2.3 서비스제공자에 기인한 위험 (SERVICE PROVIDER)

IoT 서비스에서 발생할 수 있는 프라이버시 침해 요소 중의 하나는 기업이 사용자의 정보를 부적절하게 사용하거나, 사용자의 동의 없이 사용자 정보를 지속적으로 활용하는 것 등이 있다. 따라서, 해당 산업분야의 자체적인 보호노력이 사용자의 프라이버시 위험에 대한 염려를 줄여줄 수 있을 뿐만 아니라 (Xu et al., 2011), 개별 서비스 제공자의 소비자 프라이버시 보호에 대한 신뢰는 사용자의 프라이버시 인식에 중대한 영향을 끼칠 수 있다. 기존 프라이버시 연구에 따르면, 정보가 2차적 목적으로 정보 제공자의 동의 없이 사용될 때 소비자의 프라이버시를 침해하게 된다고 하였다 (Culnan & Bies, 2003). 또한, 기업이 사용자의 개인정보를 보유할 때 프라이버시를 침해할 가능성이 존재하며, 이러한 프라이버시 침해에 대하여 우려하는 정도가 큰 사용자는 기업이 자신의 정보를 사용하

는 것을 원하지 않는다고 주장 한다 (Cespedes and Smith, 1993). 따라서 다음과 같은 가설을 설정하였다.

[가설 2] 서비스 제공자와 관련된 개인정보 유출에 대한 위험은 지각된 프라이버시 위험을 증가시키다.

3.2.4 관련 정책에 대한 신뢰 (LEGISLATION)

정부 프라이버시 관련 입법을 통해 소비자 정보의 유출과 잘못된 사용을 통제하는 방법은 사용자가 가진 인지된 프라이버시 위협을 완화 시킬 수 있다 (Xu et al., 2011). 이는 기업이 소비자 정보의 유출하거나 잘못된 방식으로 사용할 때, 정부의 프라이버시 법안이 이러한 상황을 통제해야 함을 말한다. 즉, 사용자는 정부가 프라이버시 법안을 통해 소비자의 프라이버시 손실을 보호 할 것이라 기대한다. 기존의 사회학적, 법학적 연구에서는 정부의 프라이버시 법안이 사용자가 자신의 정보가 보호되고 있음을 느끼도록 하는데 긍정적인 영향을 미친다고 주장한다 (Bandura, 1986; Faden, et al.. 1986). 정부의 프라이버시 법안은 소비자 정보의 잘못된 사용이나 유출을 통제함으로써, 소비자의 개인정보 손실을 막을 것으로 기대된다. 따라서 IoT 서비스에 있어서, 정부의 프라이버시 법안에 대한 신뢰는 사용자의 인지된 프라이버시 위험을 완화 시킬 것이다.

[가설 3] 개인정보 보호 관련 정책에 대한 신뢰는 지각된 프라이버시 위험을 낮춘다.

4. 연구방법론 및 데이터 수집

4.1 데이터 수집과 표본의 특성

본 연구의 핵심인 IoT 기술은 개인 및 기업에서 다양한 방식으로 활용되고 있다. 하지만 본 연구에서는 IoT 기술을 활용한 서비스 중에서 프라이버시 침해와 직접적으로 관련이 있으며, 설문 대상자들이 서비스에 대해 보다 쉽게 이해하고, 또한 실제 사용할 용의가 있는 액티비티 트래커(Activity tracker)가 가장 적합한 서비스로 판단하여 연구 대상으로 설정하였다.

본 연구의 연구모형 검증을 위한 자료 수집은 2014년 1월 전문 조사기관을 통해 실시되었다. 설문은 전국 220명을 대상으로 실시되었다. 표본의 일반적 특성을 살펴보면, 남성이 47.3%를 차지하고 있으며, 여성은 52.7%를 차지한다. 연령은 30~34세가 75명으로 가장 많았고, 다음으로 20~24세(73명), 24~30세(62명), 35세 이상(10명) 순이었다. 으로 나타났다. 설문 응답자들의 인구통계학적 특성은 <표 1>과 같다

[표 1] 표본의 인구통계학적 특성

항목		빈도	백분율(%)
성별	남자	104	47.3
	여자	116	52.7
연령	20-24	73	33.2
	25-29	62	28.2
	30-34	75	34
	>35	10	4.5
교육수준	고등학교 이하	12	5.5
	전문대학(2년제)	50	22.7
	대학교(4년제)	145	65.9
	대학원 이상	13	5.9
직업	회사원	83	37.7
	전문직	30	13.6
	자영업	7	3.2
	서비스업	17	7.7
	학생	74	33.6
	기타	9	4
월 평균 소득	100만원 미만	60	27.2
	100~200만원	67	30.5
	200~300만원	60	27.7
	300~400만원	23	10.5
	500만원 이상	10	4.5
합		220	100

4.2 측정문항개발

본 연구에서는 연구모형의 가설 검증을 위해 설문지를 구성하였다. 사용된 설문항목은 관련 선행연구들의 요인들과 설문항목을 참고하여 작성하였으나, IoT 서비스가 최근에 나온 서비스라는 점을 고려하여 일부 항목들을 연구목적에 맞게 수정하고 보완하였다.

프라이버시 우려와 관련하여, 기술에 대한 위협, 서비스 제공자의 프라이버시 정책, 정부의 프라이버시 법안에 관련 연구가 프라이버시 우려를 완화시키는 요인으로 제안된 바가 있다 (Xu & Teo, 2004). IoT 기술에 대한 프라이버시 위협에 대한 문항은 제3자의 부적절한 접근, 위치정보에 대한 걱정, 정보수집 과정상의 우려로 구성되어 있다. 서비스 제공자에 의한 프라이버시 위협에 대한 문항은 과도한 개인정보 수집, 개인정보의 2차사용, 동의 없는 개인정보의 2차사용으로 구성되어 있으며, 정부의 프라이버시 정책에 대한 신뢰는 프라이버시 보호에 대한 노력 및 적절성 그리고 정책에 대한 신뢰의 3항목으로 구성하였다.

종속변수인 프라이버시에 대한 인지된 위험은 액티비티 트래커에 대한 불신, 프라이버시 염려, 위치노출에 대한 염려 등 4개 측정항목으로 구성하였다. 각 측정항목은 1점에 해당하는 '전혀 그렇지 않다'에서 7점에 해당하는 '매우 그렇다'까지 응답할 수 있는 리커트 7점 척도로 구성하였다. 설문을 위한 측정도구는 <표 2>와 같다.

5. 가설검증과 결과분석

본 연구에서는 자료 분석을 위하여 PLS(Partial Least Squares) 분석을 실시하였다.[4] 먼저 측정모형을 평가한 후, 구조모형 분석을 통해 가설검정을 하였다. 본 연구는 새로운 환경인 IoT에 대한 탐색적 성격의 연구라는 점에서 PLS를 활용하였다 (Teo et al. 2003).

[표 2] 측정도구

Construct	Item	Wording
기술에 대한 위험 (TEC)	TEC1	나는 운동추적기에 저장되는 사용자들의 정보들이 외부의 침입으로 인해 수정되거나 유출 될 수 있다고 생각한다.
	TEC2	나는 운동추적기를 사용하는 동안 수집되는 위치정보가 유출되어 사생활 침해가 발생할까 걱정된다
	TEC3	나는 운동추적기의 정보가 스마트폰으로 전송될 때, 정보를 훔쳐갈 수 있다고 생각한다.
서비스 제공자에 대한 위험(SP)	SP2	나는 운동추적기 서비스 제공회사가 나에 관해서 너무 많은 개인정보를 수집하는 것에 대하여 염려한다.
	SP3	나는 운동추적기에 저장되는 정보를 회사가 서비스 이외의 목적으로 사용하는 것이 걱정된다.
	SP4	내가 운동추적기를 사용할 때 수집된 정보들은 서비스 사용이 끝난 후에도 나의 동의 없이 계속 사용될까 걱정된다.
정부법안에 대한 신뢰(LEG)	LEG1	정부는 정보기술 사용자들의 프라이버시 보호를 위해 노력하고 있다.
	LEG2	정부의 소비자 프라이버시 정책은 적절한 수준이다.
	LEG3	정부의 개인정보보호에 대한 정책은 신뢰할 만하다.
인지된 위험(PR)	PR1	운동추적기를 사용하는 것은 위험하다
	PR2	운동추적기 사용시 내 정보들이 보호되지 않을까 걱정된다.
	PR3	운동추적기 사용시 내 위치가 제3자에게 노출될까 불안하다
	PR4	운동추적기 사용시 불안감을 느낀다.

5.1 측정모형의 평가

본 연구에서는 구조모형의 검증을 통한 가설검증에 앞서, 연구모형에 포함되어 있는 변수와 그 측정을 위한 설문항목들의 신뢰성과 타당성을 검증하기 위해 확인적 요인분석(CFA: Confirmatory Factor Analysis)

4) 본 연구에서는 분석을 위해 Smartpls를 사용하였다.

을 이용하여 개별문항에 대한 집중타당성(convergent validity), 내적일관성(internal consistency), 판별타당성(discriminant validity)에 대한 분석을 실시하였다. 측정항목의 집중타당성은 PLS의 부스트랩(Bootstrap)방식으로 측정되며, 구성개념에 적재된 측정항목의 요인 적재량과 그 t-값을 분석하였다. <표 3>에 나온 분석결과와 같이 13개의 측정항목 중 모든 문항의 요인 적재량이 기준치 0.7이상이고 (Fornell & Larcker, 1981), <표 4>에 나온 분석결과와 같이 모든 문항의 요인 적재량의 t-값이 2.567 이상으로 나타나 모두 유의수준 1%에서 유의하였다.

일반적으로 신뢰성은 동일한 개념에 대해서 비교가 가능한 독립된 측정도구를 사용하여 반복적으로 측정하였을 때, 유사하거나 동일한 측정값을 얻을 가능성을 말한다. PLS 분석방법에서는 복합신뢰도(Composite Reliability)를 사용하여 신뢰성을 검증하며, 일반적으로 CR값이 0.7 이상이면 내적 일관성이 양호하다고 판단한다 (Fornell and Larcker, 1981). 따라서, <표 4>에 나온 분석결과와 같이 본연구의 측정변수들은 CR값이 모두 0.7이상이므로 내적일관성이 양호하다고 볼 수 있다.

또한 연구모형의 수렴타당성과 판별타당성 분석을 통해 각 변수들에 대한 개념타당성을 평가하였다.

[표 3] 확인적 요인분석 결과 (전체 표본에 대한 요인 적재값)

	서비스 제공자에 대한 위험(SP)	인지된 위험(PR)	정부 법안에 대한 신뢰(LEG)	기술에 대한 위험(TEC)
SP2	0.869	0.579	-0.193	0.463
SP3	0.914	0.588	-0.265	0.454
SP4	0.885	0.516	-0.235	0.454
PR1	0.326	0.716	-0.059	0.309
PR2	0.614	0.882	-0.31	0.536
PR3	0.613	0.885	-0.266	0.546
PR4	0.482	0.847	-0.175	0.49
LEG1	-0.189	-0.182	0.861	-0.053
LEG2	-0.283	-0.252	0.891	-0.234
LEG3	-0.185	-0.235	0.827	-0.128
TEC1	0.457	0.478	-0.215	0.886
TEC2	0.469	0.584	-0.098	0.891
TEC3	0.429	0.463	-0.153	0.872

[표 4] 요인의 집중타당성 및 판별타당성 분석

구성개념	측정항목	요인 적재량	t-값	복합 신뢰도	크론바하 알파	AVE	판별타당성 분석			
							TEC	SP	LEG	PR
기술에대한 위험 (TEC)	TEC1	0.886	48.69	0.86	0.914	0.78	0.883*			
	TEC2	0.891	55.84							
	TEC3	0.872	44.8							
서비스제공자에 대한 위험 (SP)	SP2	0.869	36.44	0.868	0.919	0.792	0.513	0.889		
	SP3	0.914	68.07							
	SP4	0.885	44.04							
정부 법안에 대한 신뢰(LEG)	LEG1	0.861	15.32	0.825	0.895	0.739	0.171	0.259	0.859	
	LEG2	0.891	12.36							
	LEG3	0.826	10.48							
인지된 위험 (PR)	PR1	0.716	12.6	0.858	0.901	0.699	0.582	0.632	0.264	0.836
	PR2	0.882	52.92							
	PR3	0.885	58.27							
	PR4	0.847	34.52							

* 판별타당성 분석에서 진하게 표시된 대각선의 값은 평균분산추출값(AVE)의 제곱근임.

PLS에서 수렴타당성은 요인적재량, 복합신뢰도(Composite Reliability), 평균분산추출값(AVE)를 통해 검증한다. 요인 적재량은 대략 0.7 이상을 권장하고(Srite and Karahanna, 2006), 그 요인 적재량은 다른 구성개념의 요인적재량보다 커야한다 (Gefen and Straub, 2005; Srite and Karahanna, 2006). <표 3>에 나온 확인적 요인분석(CFA: Confirmatory Factor Analysis) 결과에 따르면 구성개념에 대한 요인적재량이 기준을 충족함을 알 수 있다. 또한 합성신뢰도는 기준치 0.7을 모두 초과하는 것으로 나타났으며, 각 구성개념의 평균분산추출값(AVE) 또한 기준치 0.5 (Chin, 1998) 보다 높기 때문에 종합적으로 수렴타당성이 존재한다.

판별타당성 분석을 위해 <표 4>의 대각선 축에 표시되는 평균분산추출값(AVE)의 제곱근 값과 다른 구성개념들 간의 상관계수(Correlation)를 비교하였다 (Fornell, and Lacker, 1981). 이를 통해 각 구성개념들이 관련 측정항목들과 공유하는 분산이 다른 구성개념들과 공유하는 분산보다 더 큰 것을 확인할 수 있다. 따라서 본 연구의 측정항목들이 판별 타당성을 적절히 갖추고 있는 것으로 평가된다. 따라서 본 연구에서 활용된 측정변수들은 집중타당성, 내적일관성, 그리고 판별타당성이 만족스럽다고 할 수 있으며, PLS 경로분석을 수행하기에 적합한 변수들이라고 판단할 수 있다.

5.1 구조모형의 검정

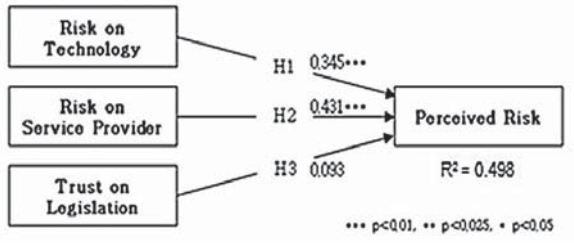
측정모형의 타당성 평가에 이어서, 구조모형에 대한 경로계수의 유의성을 검증하였다. 경로계수를 추정하기 위한 방법으로 부스트랩(Bootstrap)기법을 사용하여 경로계수과 t-값을 구하였다. 이는 경로계수의 유의성을 평가하기 위해 일반적으로 사용하는 방법이다 (Tenenhaus et al., 2005; Wetzels et al., 2005). 또한, 모델의 적합도 분석을 위해서, PLS는 GoF(Goodness-of-Fit)를 사용한다 (Tenenhas, et al., 2005). 이는 잠재변수에 대해 평균 공통성(Communality)과 평균 R^2의 기하평균에 의해 구한다.

적합도의 크기는 최소 0.1이상이어야 하며, 0.36 이상은 상, 0.25 이상에서 0.36 미만은 중, 0.1 이상 0.25 미만은 하로 분류된다 (Tenenhaus et al., 2005). 본 연구의 GoF값은 0.621로서 PLS 구조방정식 모형의 적합도가 매우 높은 것으로 나타났다.

<그림 2>와 <표 5>에 나타난 바와 같이, 본 연구 모형의 가설검증 결과 변수간의 경로계수는 0.093 ~ 0.431로 나타났으며, [H3]를 제외한 나머지, [H1], [H2]가 유의한 수준에서 채택되었다. 기술에 대한 위험(Risk on Technology)은 경로계수 0.345로 인지된 위험(Perceived Risk)에 정(+)의 영향을 미치는 것으로 나타났다($p<0.01$). 따라서 '기술에 대한 위험은 인지된 프라이버시 위험을 증가시킨다.'는 가설 1이 채택되었다. 그리고 서비스제공자에 대한 위험(Risk on Service Provider)은 경로계수 0.431로 인지된 위험(Perceived Risk)에 정(+)의 영향을 미치는 것으로 나타났다($p<0.01$). 따라서 가설 2 '서비스 제공자에 대한 위험은 인지된 프라이버시 위험을 증가시킨다.'는 채택되었다. 그러나 인지된 위험(Perceived Risk)에 영향을 주는 정부의 프라이버시 법안에 대한 신뢰(Trust on Legislation)는 유의하지 않은 것으로 나타나($\beta=0.093$, $p>0.05$), 가설 3 "정부의 프라이버시 법안에 대한 신뢰는 인지된 프라이버시 위험을 낮춘다."는 기각 되었다. 경로분석결과는 <표 5>에 요약되어 있다.

또한, <그림 2>에 나타난 바와 같이 기술에 대한 위험, 서비스제공자에 대한 위험, 정부의 프라이버시 법안에 대한 신뢰는 사용자의 인지된 위험을 49.8% 설명하고 있다. 이는 적정 검정력 10%보다 높다 (Falk and Miller, 1992).

다음으로 내생변수 R^2값으로 적합도를 평가하였다. R^2값의 효과는 0.26이상은 상, 0.13이상에서 0.26 미만은 중, 0.02이상 0.13 미만은 하로 분류된다 (Cohen, 1988). 본 연구에서 인지된 위험의 결정계수 R^2값은 0.498로 상으로 나타났다. 따라서 R^2값에 의한 본 연구의 PLS 구조방정식 모형은 적합하다고 볼 수 있다.



[그림 2] 경로분석

[표 5] 경로분석 결과

가설	경로	Coefficient (Std. error)	t-값	채택여부
가설1 [H1]	TEC → PR	0.345** (0.058)	6.723	채택
가설2 [H2]	SP → PR	0.431** (0.064)	5.989	채택
가설3 [H3]	LEG →PR	0.093 (0.064)	1.466	기각

** p<0.01, * p<0.05

6. 결론

6.1 결과 및 시사점

다양한 정보를 수집하고, 그것들의 분석에 기반한 전략 수립을 지식경영의 핵심이라고 할 때, IoT기술에 의한 빅데이터는 지식경영분야의 새로운 성장동력이 될 수 있다. 사용자 혹은 소비자에 대한 IoT기술은 보다 풍부한 데이터의 수집이 가능한 환경을 제공할 수 있다는 점에서 지식경영분야가 주목해야 하는 기술이다.

본 연구는 최근 주목을 받는 IoT 서비스에서 소비자 프라이버시 침해 우려에 영향을 미치는 요인들의 수준을 측정하였다. 연구 모형과 가설 검증을 위한 분석을 통해 다음의 흥미로운 결과들이 도출되었다.

소비자들은 인지된 프라이버시 위험(Perceived risk)의 두 가지 요인인 기술에 의한 위협(Risk on technology)과 서비스 제공자에 의한 위협(Risk on service provider) 중 서비스 제공자에 의한 위협을 더 크게 느끼는 것으로 나타났다. 이는 데이터를 수집, 저장, 교환하는 기술적인 요인보다 저장된 데이터를 서비스 제공자들이 부적절하게 활용하거나 유출할 것이라는 것에 대하여 소비자들이 더욱 우려를 표하고 있음을 의미한다. 따라서, 소비자들은 서비스 제공자들이 소비자의 프라이버시를 보호하는데 많은 노력을 기울이지 않거나, 심지어 자신들의 이득을 위해 소비자의 정보를 동의없이 사용할 수 있다는 의심을 반영하는 결과이다. IoT환경에서는 소비자에 대한 방대하고 다양한 데이터를 수집할 수 있다는 점에서, 고객 데이터를 기본적 자원으로 하는 지식경영분야 성장이 예견됨에도 불구하고, 소비자의 프라이버시 우려는 그러한 성장을 막을 수 있다. 이전 연구에 따르면 서비스 제공자의 사용자 프라이버시 보호 노력은 사용자의 프라이버시 우려를 완화시킨다고 한다 (Xu and Teo, 2004). 따라서 IoT 서비스 제공자는 소비자의 프라이버시를 보호하기 위해 노력하고 있다는 인식을 심어주기 위한 구체적인 전략을 구상하여야 한다.

흥미로운 점은 정부의 프라이버시 보호정책에 대한 소비자의 인식이 액티비티 트래커 사용으로 발생할 수 있는 프라이버시 침해에 대한 인식에 영향을 끼치지 않는다는 것이다. 이것은 정부의 프라이버시 법안이 사용자들의 인지된 프라이버시 우려를 낮출 수 있다고 하는 이전연구와 다른 결과이다. 실제로 프라이버시 우려를 연구하는 여러 학자들은 사용자가 정부의 프라이버시 정책을 신뢰할 때 프라이버시에 대한 우

려가 줄어든다고 주장하고 있다 (Culnan, and Bies, 2003; Xu and Teo, 2004). 본 연구의 조사에서는 정부규제에 대한 신뢰도 질문에 대한 응답의 평균값은 7점 척도에서 2.068(1.260)로서, 응답이 넓게 분포되어 있지 않고, 전체적으로 낮은 신뢰도(평균값)에 집중되어 있었다. 따라서 프라이버시 염려에 대한 영향이 통계학적으로 무의미하게 나온 것으로 추측된다. 이것은 최근 일어나고 있는 개인정보 유출 사고와 관련한 정부의 미흡한 대처가 반영된 결과라고 생각된다. 최근 고객정보유출사건으로 알려진 한 통신사는 정보보호관리체계(ISMS) 인증을 받는 등 정부의 정보보호규제를 준수하였지만 사고는 피하지 못하였다. 이는 정부의 정보보호규제가 기업들의 정부규제준수를 배상책임 면제의 수단으로 사용될 뿐, 규제를 통한 실질적인 사용자의 정보보호가 이어지지 않았음을 나타낸다. 따라서 조사대상자들은 현재 정부의 프라이버시 보호 노력을 신뢰하지 못하고, 프라이버시 침해 피해 이후의 정부의 대처방안을 믿지 않고 있다고 볼 수 있다.

위와 같이 논의된 바탕으로 도출된 시사점은 다음과 같다.

첫째, 사용자는 서비스를 사용할 때 기업이 자신의 정보를 올바로 사용하는지에 대한 의구심을 가지고 있으며, 이는 차후 서비스 수용에 있어 부정적인 요인이 될 것으로 보인다. 따라서 기업은 IoT 제품 및 서비스를 제공하고자 할 때 설계부터 운영까지 전 영역에 걸쳐 보안을 고려해야 하고, 사용자들에게 IoT 서비스를 통해 수집된 정보가 제한된 원래의 목적의 한계 내에서 엄격한 관리 하에서 악용의 우려 없이 서비스가 운영된다는 확신을 전달 할 필요가 있다. 또한 개인정보정책을 통해 사용자의 데이터가 수집되고 활용될 때 서비스 제공자의 정보 이용목적 등을 사용자가 판단하기 쉽게 명확히 명시해야 한다.

둘째, 사용자는 정부의 프라이버시 정책 및 구제방안을 신뢰하고 있지 못하다. 이는 최근 국내에 발생하고 있는 개인정보유출 사고시 정부의 대처방안이 사용자들의 불편함을 해소해주지 못했다는 것을 의미한다. 따라서 개인정보보호에 대한 투자를 늘리고, IoT 산업에 특화된 정책 마련을 통해 IoT 서비스 사용자들에게 믿음을 주는 안전한 IoT 환경을 구축하는 노력이 요구된다.

셋째, 소비자는 IoT 제품과 서비스를 사용할 때 강력한 패스워드를 설정하고, 인증되지 않은 무선인터넷에 함부로 접속하지 않는 등 프라이버시 침해에서 벗어나기 위한 다각적인 노력의 자세가 요구 된다고 볼 수 있다.

앞으로 IoT 서비스는 더욱 다양한 센서를 통해 다각적인 정보를 수집할 것이며 이에 따른 다양한 서비스들이 잇따라 나올 것으로 기대된다. 이는 사용자들의 삶을 보다 편하고 다채롭게 할 것이다. 하지만 새로운 서비스와 함께 발생할 수 있는 프라이버시 위협들을 해결하지 않는다면, 사용자는 서비스 수용을 거부할지도 모른다. 따라서 IoT 서비스와 관련한 프라이버시 보호 정책, 법안들이 IoT 산업의 발전에 부정적인 영향을 미칠 수는 있지만, 장기적인 안목에서 사용자의 프라이버시를 보호하는데 투자를 하는 것이 바람직하다고 할 수 있겠다.

6.2 연구의 한계점 및 향후 연구과제

본 연구는 IoT 서비스에 있어서 소비자의 프라이버시 침해에 대한 우려 수준을 실증적으로 측정하였다는 점에서 의의를 갖는다. 하지만 본 연구는 다음과 같은 몇 가지 한계점을 가지고 있으며, 이에 향후 연구과제에 대하여 다음의 내용을 보완해야 할 것이다.

첫째, 사용자가 IoT 서비스를 사용하면서 느끼는 프라이버시 위협은 본 연구에 사용된 3가지 변수 이외에도 더 많이 존재할 것이며, 보다 복합적인 형태로 사용자의 프라이버시를 위협할 것이다. 또한 개인의 성격이나 신념에 따라서 프라이버시 위협을 느끼는 수준이

달라 질 수 있음에도 불구하고 고려되지 못하였다.

둘째, 최근 개인정보 유출과 관련된 이슈들은 조사대상자들의 프라이버시 인식 수준을 변화시켰을 것이다. 즉, 같은 조사대상자에게 설문을 하였다고 하더라도 조사 시기와 프라이버시 피해 여부에 따라서 프라이버시 우려를 다르게 느낄 수 있다. 따라서 사용자들의 프라이버시 우려수준의 변화과정을 시계열 연구를 통해서 관찰 해 볼 필요가 있다.

셋째, 본 연구에서는 향후 IoT 서비스를 보다 적극적으로 수용할 것으로 예상되는 20~30대를 대상으로 표본을 구성하였다. 따라서 본 연구의 결과가 전 연령층의 프라이버시 우려수준을 대표한다고 볼 수는 없다. 향후 전 연령층의 IoT 사용자를 대상으로 프라이버시 침해에 관련된 연구를 한다면, IoT 서비스 산업에서 소비자가 추구하는 가치에 대해 이해할 수 있는 중요한 연구가 될 것이다.

넷째, IoT 서비스는 아직 초기단계이며 서비스가 활성화되지 않았기 때문에 실제 사용자를 대상으로 한 실증연구가 진행되기 어려운 상황이다. 차후, IoT 서비스가 보다 활성화되었을 때에는, 실제 사용자들이 느끼는 프라이버시 위협에 대한 조사를 통해 연구의 정확성을 높일 수 있을 것으로 기대한다.

다섯째, IoT 기술의 특성상 앞으로 다양한 서비스가 제공될 것으로 예상되며, 각 IoT 서비스가 사용하는 센서 또는 수집하는 정보에 따라서 다양한 프라이버시 위협상황이 발생될 것이다. 따라서 각 IoT 서비스에서 발생하는 프라이버시 위협상황을 정리할 필요가 있으며 이에 따른 비교 분석은 IoT 산업의 발전에 많은 도움을 줄 수 있을 것이라 기대한다.

마지막으로, IoT 서비스가 초기 단계에 있어 실제 사용자가 아닌 잠재적 사용자를 응답자로 하였기 때문에, 인지된 프라이버시 위험이 실제 IoT 서비스의 수용에 어떤 영향력이 있는 지는 검증하지 못하였다. 향후 연구에서는 실제사용자를 대상으로 하여 프라이버시 위험이 IoT 서비스 맥락에서 얼마나 실제적인 영향력이 있는 지 탐색하는 것이 필요하다.

참 고 문 헌

[국내문헌]

[1] 김병수 (2012), 모바일 소셜네트워크서비스 환경에서 지속 사용 의도의 선행 요인에 관한 연구: 신뢰와 프라이버시 우려의 역할, 지식경영연구, 제13권, 제 4호, 83-100.

[2] 심재문, 권오병, 강지욱 (2010), 상황인식 기술을 이용한 운전자 선호도 기반 교통상세정보 추천 시스템, 지식경영연구, 제11권, 제2호, 75-93.

[3] 한국정보화진흥원 (2014), 웨어러블 디바이스 기반의 창조경제 활성화 전략.

[국외문헌]

[1] Adomavicius, G. and Tuzhilin, A. (2005), Personalization Technologies: A Process-oriented Perspective, *Communications of the ACM*, 48(10), 83-90.

[2] Atzori, L., Lera, A. and Morabito, G. (2010), The Internet of Things; A Survey, *Computer Networks*, 54, 2787-2805.

[3] Asif, Z. (2005), Integrating the Supply Chain with RFID: A Technical and Business Analysis, *Communications of the Association for Information Systems*, 15(24), 393-426.

[4] Cespedes, F. V. and Smith, H. J. (1999), Database Marketing: New Rules For Policy and Practice, *Slone Management Review*, 34, pp. 7-23.

[5] Chin, W. W. (1998), Commentary: Issues and Opinion on Structural Equation Modeling, *MIS Quarterly*, 22(1), 7-16.

[6] Chiu, C-M, Wang, E. T. G., Fang, Y-H and Huang, H-Y (2012), Understanding customers' repeat purchase intentions in B2C e-commerce: the roles of utilitarian value, hedonic value and perceived risk, *Information Systems Journal*, 24(1), 85-114.

[7]Cohen, J. (1988), *Statistical Power Analysis for the Behavioral Sciences*, Academic Press, New York.

[8]Culnan, M. J. (1993), How Did They Get My Name?": An Exploratory Investigation of Consumer Attitudes Toward Secondary Information Use, *MIS Quarterly*, 17(3), 341-363.

[9]Culnan, M. J. and Armstrong, P. K. (1999), Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation, *Organization Science*, 10(1), 104-115.

[10]Culnan, M. J, and Bies, R. J. (2003), Consumer privacy: Balancing economic and justice considerations, *Journal of Social Issues*, 59(2), 323-342.

[11]Falk, R. F. and Miller, N. B. (1992), *A Primer for Soft Modeling*. University of Akron Press, Akron.

[12]Featherman, M. S. and Pavlou, P. A. (2003), Predicting e-Services Adoption: A Perceived Risk Facets Perspective, *International Journal of Human-Computer Studies*, 59(4), 451-474.

[13]Fornell, C. and Larcker, D. F. (1981), Evaluating Structural Equation Models with Unobservable Variables and Measurement Error, *Journal of Marketing Research*, 18(1), 39-50.

[14]Garfinkel, S. and Rosenberg, B. (2006), *RFID: Applications, Security, and Privacy*, Addison-Wesley, New Jersey.

[15]Gefen, D. and Straub, D. (2005), A Practical Guide to Factorial Validity Using PLS-graph: Tutorial and Annotated Example,

Communications of the AIS, 16(25), 91-109.

[16] Genaro, V. and Caine, K. (2014), Understanding th Wearability of Head-Mounted Devices from a Human-Centered Perspective, ISWC2014, September 13-17, Seattle, WA, USA.

[17]Goodhue, D. L. and Straub, D. W. (1991), Security Concerns of System Users: A Study of Perceptions of the Adequacy of Security, *Information & Management*, 20(1), 13-27.

[18]Günther, O. and Spiekermann, S. (2005), RFID and the Perception of Control: the Consumer's View, *Communications of the ACM*, 48(9), 73-76.

[19]Hann, I. H., Hui, K. L., Lee, S. Y. T. and Png, I. P. (2002), Online Information Privacy: Measuring the Cost-Benefit Trade-Off, *In Proceedings of the Twenty-Third International Conference on Information Systems*, 1, Barcelona, Spain, 1-10.

[20]Hoffman, D. L., Novak, T. P. and Peralta, M. (1999), Building Consumer Trust Online, *Communications of the ACM*, 42(4), 80-85.

[21]Hui, K. L., Teo, H. H. and Lee, S. Y. T. (2007), The Value of Privacy Assurance: An Exploratory Field Experiment, *MIS Quarterly*, 31(1), 19-33.

[22]Junglas, I. and Watson, R. T. (2006), The U-Constructs: Four Information Drives, *Communications of the Association for Information systems*, 17(1), 26.

[23]Malhotra, N. K., Kim, S. S. and Agarwal, J. (2004), Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model, *Information Systems Research*, 15(4), 336-355.

[24]Margulis, S. T. (2003), Privacy as a Social Issue and Behavioral Concept, *Journal of Social Issues*, 59(2), 243-261.

[25]Mayer-Schönberger, V. (1997), *Technology and Privacy: The new landscape*, MIT Press, Cambridge.

[26]Medaglia, C. M. and Serbanati, A. (2010), *An Overview of Privacy and Security Issues in the Internet of Things*, Springer, New York.

[27] Regan, P. M. (1993), Ideas or Interests: Privacy in Electronic Communications. *Policy Studies Journal*, 21(3), 450-469.

[28]Minch, R. P. (2004), Privacy Issues in Location-Aware Mobile Devices, *Proceedings of the 37th Annual Hawaii International Conference on System Sciences*, Kauai, Hawaii, 1-10.

[29]Roussos, G., Peterson, D. and Patel, U. (2003), Mobile Identity Management: An Enacted View, *International Journal of Electronic Commerce*, 8(1), 81-100.

[30]Sheng, H., Nah, F. F. H. and Siau, K. (2008), An Experimental Study on Ubiquitous Commerce Adoption: Impact of Personalization and Privacy Concerns, *Journal of the Association for Information Systems*, 9(6), 344-376.

[31]Srite, M. and Karahanna, E. (2006), The Role of Espoused National Cultural Values in Technology Acceptance, *MIS quarterly*, 30(3), 679-704.

[32]Stone, E. F. and Stone, D. L. (1990), Privacy in Organizations: Theoretical Issues, Research Findings, and Protection Mechanisms, *Research in Personnel and Human Resources Management*, 8(3), 349-411.

[33]Tenenhaus, M., Vinzi, V. E., Chatelin, Y. M. and Lauro, C. (2005), PLS Path Modeling,

Computational Pstatistics & Data analysis, 48(1), 159-205.

[34]Teo, H. H., Wei, K. K. and Benbasat, I. (2003), Predicting Intention to Adopt Interorganizational Linkages: An Institutional Perspective, *MIS Quarterly*, 27(1), 19-49.

[35] Thierer, A. (2014), The Internet of Things and Wearable Technology, Mercatus Working Paper, http://mercatus.org/sites/default/files/Thierer-Wearable-Tech.pdf

[36]Warren, S. D. and Brandeis, L. D. (1890), The Right to Privacy, *Harvard law review*, 4(1), 193-220.

[37]Watson, R. T., Pitt, L. F., Berthon, P., and Zinkhan, G. M. (2002), U-commerce: Expanding the Universe of Marketing, *Journal of the Academy of Marketing Science*, 30(4), 333-347.

[38]Weber, R. H. (2010), Internet of Things–New Security and Privacy Challenges, *Computer Law & Security Review*, 26(1), 23-30.

[39]Wetzels, M., Odekerken-Schröder, G. and Van Oppen, C. (2009), Using PLS Path Modeling for Assessing Hierarchical Construct Models: Guidelines and Empirical Illustration, *MIS Quarterly*, 33(1), 177-195.

[40] Xu, H., Dinev, T., Smith, J. and Hart, P. (2011), Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances, *Journal of the Association for Information Systems*, 12(12), 798-824.

[41]Xu, H. and Teo, H. (2004), Alleviating Consumers' Privacy Concerns in Location-Based Services: A Psychological Control Perspective, *In Proceedings of the Twenty-Fifth International Conference on Information Systems*, Washington, D.C., 793-806.

[42]Xu, H., Teo, H., Tan, B. C. and Agarwal, R. (2009), The Role of Push-Pull Technology in Privacy Calculus: the Case of Location-Based Services, *Journal of Management Information Systems*, 26(3), 135-174.

저 자 소 개

배 진 석 (Jinseok Bae)

현재 현대오토에버에서 HR시스템 업무를 담당하고 있다. 울산과학기술대학교 경영공학 석사학위를 취득하였고, 주요 연구 관심분야는 빅데이터, IT기업전략, 정보시스템 관리 및 활용 등이다.

정 윤 혁 (Yoonhyuk Jung)

현재 울산과학기술원 경영학부 부교수로 재직 중이다. 루이지애나주립대학교(Louisiana State University)에서 경영정보학 박사학위를 취득하였고, 디지털미디어, 모바일 서비스, 의료정보시스템 영역에서 사용자에 대한 연구를 하고 있다. 정보기술사용자에 대한 연구를 European Journal of Information Systems, Information Systems Journal, Information & Management 외 다수 저널에 게재하였다.

조 우 제 (Wooje Cho)

현재 서울시립대학교 경영학부 조교수로 재직 중이다. 일리노이주립대(어바나샴페인)에서 경영학 박사학위를 취득하였고, IT 전략, IT 기업 전략, 정보 보안 분야에서 연구를 하고 있다. Decision Support Systems, IEEE Transactions on Engineering Management, Information Technology & Management 등의 저널에 게재하였다.