http://dx.doi.org/10.14400/JDC.2016.14.2.65

사물인터넷 시대의 정보 프라이버시 염려에 대한 실증 연구

박천웅*, 김준우**
한국데이터베이스진흥원 유통사업실*, 인천대학교 경영학과**

An Empirical Research on Information Privacy Concern in the IoT Era

Cheon-Woong Park*, Jun-Woo Kim**
Dept. of Data Distribution & Business, Korea Database Agency*
Dept. of Business Administration, Incheon National University**

요 약 사물인터넷(IoT), 빅데이터 등 새로운 IT 환경시대가 도래한 지금 우리는 법 테두리 안에서 개인의 정보가 포함되지 않은 정보를 제공하더라도, 다양한 정보와 결합하여 개인 식별이 가능한 시대에 살고 있다. 이로 인하여, 개인정보 피해가 발생할 수 있으며, 또한 2차 피해로 발전 될 수 있다. 특히, IoT를 통해 수집되는 데이터에는 단기간에는 개인을 식별할 수 없지만, 시간이 지남에 따라 축적된 데이터를 기반으로 특정 개인을 인식 할 수 있는 위험성이 존재한다. 이에 따라 본 연구는 IoT 시대에 개인정보 제공에 대한 염려를 낮추는데 영향을 주는 요인들을 도출하여 실제로 개인정보 제공의도와 연결될 수 있도록 하기위해 실증적으로 분석하여 검증하고자 하였다. 이를 바탕으로 정보 프라이버시가 개인정보 제공의도에 어떠한 영향을 미치는지에 대한 영향도를 분석하였다. 연구 결과, 정보 프라이버시 위험이 정보 프라이버시 염려에 가장 큰 설명력을 보였으며, 정보 프라이버시 정책, 정보 통제 그리고 침해 경험 순으로 설명력을 보였다. 따라서 소비자에게 정보 프라이버시 염려를 낮추는 정책이나 제도개선 및 기술개발을 통해 안전한 환경을 제공하면 개인정보를 제공할 것이다.

주제어 : IoT, 개인정보, 정보 프라이버시, 제공의도, IT 융복합

Abstract This study built the theoretical frameworks for empirical analysis based on the analysis of the relationship among the concepts of risk of information privacy, the experience of information privacy, the policy of information privacy and information control via the provision intention studies. Also, in order to analyze the relationship among the factors such as the risk of information privacy, intention to offer the personal information, this study investigated the concepts of information privacy and studies related with the privacy, established a research model about the information privacy.
Followings are the results of this study: First, the information privacy risk, information privacy experience, information privacy policy, and information control have positive effects upon the information privacy concern. Second, the information privacy concern has the negative effects upon the provision intention of personal information.

Key Words : IoT, Personal information, Information Privacy, Intention, IT Convergence

* This research was supported by the 2014 Incheon National University Research Fund.
Received 24 November 2015, Revised 28 January 2016
Accepted 20 February 2016, Published 28 February 2016
Corresponding Author: Jun-Woo Kim
(Incheon National University)
Email: jwkim@incheon.ac.kr

ISSN: 1738-1916

1. 서론

스마트 기기가 인터넷과 연결 되면서 기존의 웹 기반 IT 플랫폼이 모바일 기반으로 변화하기 시작하였다. 또한 스마트 기기의 발전으로 사람과 사람뿐만 아니라 사람과 동물, 사물, 환경 등 모든 것으로 연결범위가 확대되고 있다. 이러한 사회를 초연결사회(Hyper Connection Society)라 부르고 있으며, 이 사회의 기본이 되는 기술과 서비스가 바로 스마트기기를 포함한 사물인터넷(Internet of Things)이다.

이러한 사물인터넷은 시간과 장소의 제약 없이 모든 사물이 인터넷을 통해 정보를 공유하거나 처리하여 새로운 융합 서비스를 제공하는 것을 의미하고 있으며, 이를 통해 새로운 부가가치를 창출하는 핵심동력으로 기대를 모으고 있다.

하지만, 클라우드 컴퓨팅, 데이터 마이닝, 사물인터넷 등 정보기술의 변화로 수집되는 데이터의 양도 기하급수적으로 증가하면서 개인정보 보호와 활용에 대한 이슈가 부각되고 있다. 이는 빅데이터, 사물인터넷으로 대표되는 스마트폰, 태블릿 PC, 스마트 워치, 스마트 안경 등 다양한 기기를 기반으로 수집·저장·관리·공유되는 개인정보가 증가하면서 개인정보에 대한 침해 및 피해가 우려되고 있다. 특히, 사물인터넷을 기반으로 수집된 정보가 개인을 식별할 수준의 정보가 아니라고 하더라도 개별 정보들을 조합할 경우 시간과 장소와 같은 개인의 활동 내역 등 보다 구체적이고 민감한 사생활 정보가 생성될 수 있다. 이러한 상황을 통해 기존에는 없었던 새로운 형태의 개인정보가 되거나 또는 개인정보 침해 가능성이 발생하게 된다.[1)]

실제로 사물인터넷 환경에서 스마트기기를 통한 개인정보 수집 및 운영방법의 변화로 피해가 발생하고 있다. 예컨대, 무인기(Drone)를 활용해 스마트폰을 해킹하여 개인정보 유출이 가능하다는 것을 확인하였으며, GPS해킹, 스마트 카 해킹, 스마트 TV, 헬스케어 기기 등 대부분의 사물인터넷 기기들이 보안에 취약하여 개인정보의 유출 등 보안문제가 발생하는 것으로 나타났다[1]. 또한 최근에는 개인들도 무의식적으로 개인정보를 SNS 등에 공개함으로써 개인정보 침해에 대한 우려가 증가하고 있으며, 실제 개인정보 침해 사고도 빈번하게 발생하고 있다. 이러한 IoT 환경에서 생산되는 정보와 지식은 삶을 풍요롭고 편리하게 변모 시키고 있지만, 이렇게 생산된 정보가 무분별하게 확대되고 재생산 되는 등 정보의 역기능도 많이 발생하고 있다[2].

이를 해결하기 위해 IoT 기반의 정보 프라이버시와 관련된 연구들이 최근 활발하게 진행되고 있으며, 이를 기반으로 정보 프라이버시 보호를 위한 법·제도적 정책 연구와 기술적 방법을 다양하게 제시되고 있지만, 아직은 미흡한 것이 현실이다. 이는 IoT, 빅데이터, 클라우드 컴퓨팅 등 정보기술의 발전과 확산을 기존의 제도가 따라가지 못하는 데에 기인하고 있으며, 또한 기존의 정보 프라이버시 연구들이 가지고 있던 한계에서도 이유를 찾을 수 있을 것이다. 기존 연구는 개인정보 침해 및 보호를 기술적·도구적 관점에서 사용자의 위험과 이익에 대한 내용으로 설명하였고, 법·제도적 측면에서는 정보 프라이버시 보호를 목적으로 연구하였기 때문에 이를 충분히 반영할 수 없었다.

따라서 본 연구에서는 위와 같은 IoT 환경에서의 정보 프라이버시의 필요성과 문제점을 해결하고, 기존의 개인정보 보호와 관련된 연구의 한계점을 극복하고 정보 프라이버시에 따른 개인정보 제공의도 간의 관계를 실증 분석하고자 한다.

2. 이론적 배경

2.1 사물인터넷(IOT)

사물인터넷(Internet of Things, IoT)은 사용자의 제어에 의하여 작동하는 스마트기기뿐만 아니라 센서를 포함한 모든 기기들이 내·외부 환경과 상호 작용할 수 있도록 인터넷과 연결할 수 있는 기술이다[3]. 기존의 사물간 통신인(Machine to machine, M2M)이 기기 중심의 하드웨어적 접근이었다면, IoT는 소프트웨어 중심의 서비스 지향적인 접근이라 할 수 있다. 식별 가능한 사물(Things)이 만들어낸 정보가 인터넷을 통해 공유하는 환경으로 모바일 인터넷보다 진보한 단계의 인터넷을 의미한다[4]. 사물인터넷은 개인정보, 정보와 콘텐츠의 전송 보호 등이 보장되면, 다양한 산업영역에서 새로운 지능형 프로그램, 서비스, 제품 등이 만들어 질 것이며, 이로 인하여

1) 정보통신산업진흥원, 스마트 그리드에서의 프라이버시 보호 방안 연구, 2011

사회와 개인에게 실질적인 혜택이 주어지는 환경이 될 것이라고 하였다[5].

사물인터넷의 확산은 데이터 수집이 가능한 기기의 증가, 방대한 양의 데이터 축적과 다양한 곳에서 데이터 활용이라는 측면에서 개인정보보호에 대한 요구를 증가시키고 있다[4]. IoT 환경에서 개인정보를 수집, 저장 및 가공·분석 측면에서 볼 때, 기술적으로 진보되고, 자동화된 기기 및 센서의 사물 식별능력, 센서를 통한 데이터 수집능력은 개인의 성향, 흥미, 취향 등 민감정보를 포함한 다양한 종류의 개인 데이터를 수집·저장하고, 프로파일링, 추적성들을 확보할 수 있게 되어 개인정보 침해에 큰 위협이 될 수 있다. 또한, 수집된 데이터의 가공 및 분석이 이루어질 경우, 다양한 서비스 기기로부터 데이터를 결합하여 데이터마이닝을 수행할 수 있기 때문에 새로이 창출된 정보와 기존의 정보가 결합됨으로써 개인을 특정화할 수 있다[6]. 아울러, 개인정보 이용 및 제공 측면에서도 기존에 비해 위협요소가 많아지게 되며, 개인이 원하지 않는 데이터 처리가 일어나는지 확인하기 힘들고 사업자 입장에서도 개인정보 제공자에게 알리기도 어려울 것이다. 이와 함께 데이터 가공을 통해 얻어진 식별가능한 개인정보 보호를 위한 원칙이 필요하며, 개인정보 최소 수집 및 목적 외 이용금지 원칙이 어떻게 적용될지도 개인정보 보호를 위협하는 요소가 될 수 있다[4].

IoT시대에는 개인정보 보호를 위해서는 기존의 정책을 적용하기 보다는 환경에 맞도록 개인정보 보호 정책을 좀 더 유연하게 수립해야 한다고 하였다[7]. 또한 IoT 시대가 활성화하기 위해서는 보안환경의 관점에서 데이터 통합, 개인정보 보호 및 사용자의 기기에 대한 보안도 필요하다고 하였다[8].

2.2 정보 프라이버시

온라인을 통한 정보 교류, 상호작용 등이 증가하면서 프라이버시의 정보적인 측면 또한 강조되었다[9, 10]. 이는 개인과 개인, 개인과 사회의 정보 교류와 상호작용이 활발해지면서 개인정보가 다양한 목적에 의하여 수집·분석되고 있어 개인이 자신의 정보를 스스로 통제하는 능력이 더욱 중요해졌다.

온라인에서는 정보 주체의 의지와 상관없이 개인정보가 수집·유통되고 기업은 온라인 시장을 중심으로 개인정보를 수집하기 때문에 정보 프라이버시는 중요한 문제로 인식되고 있다. 이런 점으로 인해 정보 프라이버시는 오프라인보다 주로 온라인에서의 정보에 대한 통제력을 가지는 정도를 의미하며, 온라인에서의 활동이 증가함에 따라 정보 프라이버시 침해에 대한 불안감이 증가하고 있다[9]. 이는 정보화 시대의 프라이버시 개념이 개인정보에 대한 타인의 접근을 통제할 수 있는 적극적이고 능동적인 권리로 변화했음을 의미한다[11]. 즉 정보 프라이버시는 어떠한 대상이 개인에 관한 정보를 수집, 보유 할 것인지, 정보제공에 따른 정보 보유와 운영이 안전한지에 대한 문제라 할 수 있다. 이러한 점에서 정보 프라이버시의 침해는 '개인정보의 부적절한 이용에 따른 사생활 침해'로 정의할 수 있다[2].

정보 프라이버시는 개인정보가 수집된 목적 외에 다른 목적으로 사용되는 이차적 사용에 대한 통제력을 포함하고 있으며, 이러한 상황에 대해 스스로 통제할 수 있는 자기결정권을 의미한다[12]. <Table 1>은 정보 프라이버시의 개념이 시대와 사회에 따라 변화하고 있다는 것을 보여주고 있다.

〈Table 1〉 Evolution of the Information Privacy Concept Following the Evolution of IT(adapted from Westin 2003)

Period	Characteristics
Privacy Baseline 1945-1960	Limited information technology developments, high public trust in government and business sector, and general comfort with the information collection.
First Era of Contemporary Privacy Development 1961-1979	Rise of information privacy as an explicit social, political, and legal issue. Early recognition of potential dark sides of the new technologies (Brenton 1964), formulation of the Fair Information Practices(FIP) Framework and establishing government regulatory mechanisms established such as the Privacy Act of 1974.
Second Era of Privacy Development 1980-1989	Rise of computer and network systems, database capabilities, federal legislation designed to channel the new technologies into FIP, including the Privacy Protection Act of 1984. European nations move to national data protection laws for both the private and public sectors
Third Era of Privacy Development 1990-present	Rise of the Internet, Web 2.0 and the terrorist attack of 9/11/2001 dramatically changed the landscape of information exchange. Reported privacy concerns rose to new highs.

2.2.1 정보 프라이버시 염려

정보 프라이버시 염려를 '개인정보에 대한 감시, 저장,

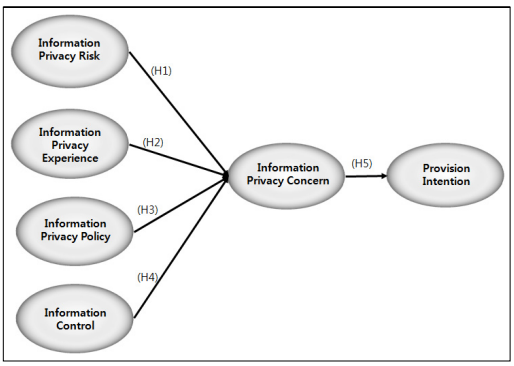
검색 그리고 커뮤니케이션을 위해 향상된 정보기술의 존재에 대해 소비자가 느끼는 위협[13]이며, 정보 프라이버시 염려는 '수집, 비인가된 2차사용, 부적절한 접근, 오류, 자료의 결합 등 다양한 우려가 결합되어 나타난다[14].

정보 프라이버시 염려는 정보 프라이버시에 대한 개인의 걱정을 측정하는 요인으로 개인의 인식을 반영하고 있어 다양한 요인이 존재하며, 이는 개인정보 유출, 침해 등과 같이 개인정보가 부적절하게 사용되는 것과 관련하여 발생한다. 즉, 개인정보가 무단으로 수집되는 것, 안전하게 보호되지 않는 것, 소비자의 동의 없이 2차적으로 사용되는 것, 그리고 3자에게 판매되는 것과 관련이 있다[14]. 이러한 정보 프라이버시 염려는 전자상거래를 위축시킬 뿐만 아니라 정보 시스템 연구 분야인 온라인 환경을 변화 시킬 수 있기 때문에 개인의 정보 프라이버시 염려는 중요한 요인으로 연구되고 있다.

3. 연구설계

3.1 연구모형

본 연구는 최근 부각되고 있는 IoT, 빅데이터 분석 등 데이터 유통과 활용을 위해 개인정보를 제공하기 위한 정보 프라이버시와 개인정보 제공의도에 대한 영향을 분석하고자 한다. 본 연구는 소비자의 인지적 경험을 기반으로 사용자의 행동을 알아보기 위하여 기존 연구를 바탕으로 [Fig. 1]과 같이 제시하였다.



[Fig. 1] Research Model

3.2 연구가설

[Fig. 1]을 바탕으로 IoT 시대의 정보 프라이버시 염려가 개인정보 제공의도에 미치는 영향을 알아보기 위하여 가설을 제시하지만, IoT 환경에서의 정보 프라이버시에 관한 연구가 미흡하여 기존 온라인 시스템에서 제시되었던 연구를 바탕으로 가설을 설정하였다.

가설 1 : IoT 시대의 정보 프라이버시 위험은 정보 프라이버시 염려에 정(+)의 영향을 미칠 것이다.

가설 2 : IoT 시대의 정보 프라이버시 침해경험은 정보 프라이버시 염려에 정(+)의 영향을 미칠 것이다.

가설 3 : IoT 시대의 정보 프라이버시 정책은 정보 프라이버시 염려에 정(+)의 영향을 미칠 것이다.

가설 4 : IoT 시대의 정보 프라이버시 통제 기능이 적을수록 정보 프라이버시 염려에 정(+)의 영향을 미칠 것이다.

가설 5 : IoT 시대의 정보 프라이버시 염려는 개인정보 제공의도에 부(-)의 영향을 미칠 것이다.

3.3 변수의 조작적 정의

본 연구는 IoT 시대의 개인정보 보호와 활용을 위한 개인정보 제공의도를 연구하기 위해 개인정보 침해위험, 침해경험, 정책 및 정보통제 등의 변수가 정보 프라이버시 염려에 어떠한 영향을 주는지 그리고 개인정보 제공의도에 어떠한 영향을 미치는지를 파악하기 위하여 다음과 같은 내용으로 설문 항목을 구성하였다. 또한 본 연구에서 적용된 변수는 기존에 진행되었던 선행연구를 기반으로 개인정보 보호 및 활용에 맞도록 새롭게 구성하여 실행하였으며, Measurement of variables은 <Table 2>와 같으며, 모든 항목은 5점 Likert 스케일로 하였다.

〈Table 2〉 Measurement of variables.

Variables	Contents
Information Privacy Risk	·Misuse of Personal information ·Inappropriately used of Personal Information.
Information Privacy Experience	·Privacy Experience ·Damage caused by privacy invasion
Information Privacy Policy	·Notice, Choice, Access, Security, Enforcement
Information Control	·Control over the reuse or diffusion of private information ·Control over the accesses on the private information
Information Privacy Concern	·Collection, Secondary use, unauthorized access ·Concerns of giving out personal information
Provision Intention	·Personal information provision intention

4. 실증분석 및 논의

4.1 자료수집 및 표본의 특성

본 연구는 설정된 연구 모형을 검증하기 위한 실증연구로 2015년 6월 11일부터 30일까지 20일간 온라인과 오프라인으로 설문을 진행하였으며, 총 376명이 설문에 응답하였으며, 결측치를 포함하거나 불성실한 응답 28부를 제외한 348부가 최종적으로 본 연구의 실증분석에 이용되었다. 설문을 통해 응답한 유효 표본은 윈도우용 Excel 2010, SPSS 18.0 버전을 사용하여 정리하였다. 또한 본 연구의 가설을 검증하기 위하여 AMOS 18.0을 활용한 구조방정식의 경로분석을 추진하였다. 연령은 10대는 31명으로 8.9%, 20대가 137명으로 39.4%, 30대는 96명인 27.6%로 조사되었으며, 40대는 48명으로 13.8%, 50대 이상은 36명 10.3%를 나타내고 있다. 학력은 중/고교재학 32명(9.2%), 고교졸업 11명(3.2%), 전문대(재학/졸업) 17명(4.9%), 4년제 대학재학 113명(32.5%), 4년제 대학졸업 92명(26.4%), 대학원 이상 83명(23.9%)로 조사되었다. 특히, 본 연구에서 대다수를 차지하고 있으며 사물인터넷 환경에서 스마트기기를 활용하여 다양한 정보를 생산·활용하는 주 이용자인 20~30대를 중심으로 연구를 진행하였다.

4.2 요인분석 및 신뢰도 분석

본 연구에서는 각 변수의 조작적 정의를 토대로 다양한 측정항목의 신뢰성 검토를 위해 Cronbach's Alpha(α) 계수를 활용하였다. 측정결과 모든 변수가 0.6이상으로 나타나 기준을 충족시켰으며, 모든 요인이 높은 내적 일관성을 지니고 있는 것으로 나타났다. 요인결정방식으로 고유값(Eigen Value)이 1이상인 요인을 선정한 결과 <Table 3>과 같이 6개의 요인으로 묶였다.

〈Table 3〉 Factor and reliability analysis

Factor			Reliability	Eigen Value
Information Privacy Risk	Risk1	.544	.633	1.176
	Risk2	.723		
	Risk3	.763		
Information Privacy Experience	Exp1	.834	.689	1.551
	Exp2	.776		
	Exp3	.652		
Information Privacy Policy	Pol1	.820	.877	2.981
	Pol2	.820		
	Pol3	.841		
	Pol4	.721		
	Pol5	.694		
Information Control	Ic1	.867	.798	1.723
	Ic2	.874		
	Ic3	.705		
Information Privacy Concern	Con1	.769	.893	7.271
	Con2	.837		
	Con3	.754		
	Con4	.666		
	Con5	.733		
	Con6	.731		
Provision Intention	Int1	.725	.877	2.105
	Int2	.824		
	Int3	.848		
	Int4	.829		
	Int5	.810		

4.3 가설검증

본 연구는 IoT 시대의 정보 프라이버시에 관해 개발한 모델을 검증하기 위해 가설을 설정하였고, 이를 측정하고 검증하기 위하여 <Table 3>과 같이 요인분석과 신뢰도 분석을 실시하였다. 또한 가설 검증을 위한 방법으로 다수의 독립, 종속 변수들 간의 인과관계를 확인하기 위해 구조방정식을 이용하여 경로분석을 실시하였다.

모형과 가설을 검증하는데 사용된 유효한 표본의 수는 348개이며, 계수 추정을 위한 최우도추정법(ML : Maximum Likelihood)이 사용되었다. 먼저, 모델 적합도는 X^2 = 2864.634(df =264 / p =.000), RMR =.045, GFI =.884, AGFI = .858, RMSEA =.075이며, CFI =.878 등으로 나타나 양호한 모델 적합도를 보여주는 것으로 나타났다. 다음은 가설에 대한 통계 검증의 결과이다.

우선, 정보 프라이버시 위험과 염려에 대한 표준화 경로계수는 .463이고 C.R값은 11.711**(p <.000)로 나타나 정보 프라이버시 위험은 염려에 정(+)의 영향을 미치는 것으로 나타나 가설 1은 채택되었다. 둘째, 정보 프라이버시 침해경험과 염려에 대한 표준화 경로계수는 .051이고 C.R값은 1.968*(p <.05)로 나타나 정보 프라이버시 침해경험은 염려에 정(+)의 영향을 미치는 것으로 나타나 가설 2도 채택되었다. 셋째, 정보 프라이버시 정책과 염려에 대한 표준화 경로계수는 .285이고 C.R값은 10.252**(p <.000)로 나타나 정보 프라이버시 정책은 염려에 정(+)의 영향을 미치는 것으로 나타나 가설 3도 채택되었다. 넷째, 정보 프라이버시 통제기능과 염려에 대한 표준화 경로계수는 .116이고 C.R값은 4.631**(p

<.000)로 나타나 정보 프라이버시 통제기능이 적을수록 염려에 정(+)의 영향을 미치는 것으로 나타나 가설 4도 채택되었다. 마지막으로, 정보 프라이버시 염려와 개인정보 제공의도에 대한 표준화 경로계수는 -.276이고 C.R값은 -10.008**(p <.000)로 나타나 정보 프라이버시 염려는 개인정보 제공의도에 부(-)의 영향을 미치는 것으로 나타나 가설 5도 채택되었다.

〈Table 4〉 Standardized factor loading, CR, P and SC

Constructs			UC	SE	C.R	P	SC
Risk	→	Con	.529	.045	11.711	.000	.463
Exp	→	Con	.036	.019	1.968	.049	.051
Pol	→	Con	.401	.039	10.252	.000	.285
Ic	→	Con	.134	.029	4.631	.000	.116
Con	→	Int	-.299	.030	-10.008	.000	-.276

5. 결론

IoT, 빅데이터, 클라우드 컴퓨팅 등 급격한 IT환경의 변화로 많은 양의 데이터가 생산·저장되고 있으며, 이렇게 생산된 데이터에는 일반정보 외에 개인정보도 포함되어 있지만, 일반정보 이지만 다른 데이터와 결합하여 개인이 식별 가능한 데이터 등이 생산 되는 등 이전의 정보 프라이버시 문제에서 확장되었다고 할 수 있다. 이처럼 IoT 시대에서의 정보 프라이버시 문제는 학계와 산업계 뿐만 아니라 법조계 에서도 많은 논란이 되고 있다. 특히 스마트 가전에서 생산하는 정보, 자동차에서 발생하는 정보, 각종 기기에서 발생하는 정보 등 IoT 시대에는 개인정보를 수집·저장 및 활용하는 것이 법·제도 등에 따라 쉽지 않다. 따라서 정보 프라이버시 관점에서 개인정보 제공 및 활용을 위한 이슈는 결국 사용자들이 어떠한 상황에서 자신의 정보를 제공하려고 하는지에 대한 논의로 귀결 될 수 있다.

따라서 본 논문은 IoT 활성화를 위해 개인의 정보를 보호하면서 동시에 활용 가능하도록 하는 방법을 도출하기 위해 정보 프라이버시에 따라 개인정보를 제공할지의 연구 주제를 설정하고 실증분석을 진행하였다. 이에 본 연구의 분석과정을 요약하면 다음과 같다.

첫째, 정보 프라이버시 위험, 침해경험, 정책 및 정보통제 기능이 정보 프라이버시 염려의 선행변수로 설정하여 연구한 결과, 정보 프라이버시 위험은 염려에 정(+)의 영향을 주는 것으로 나타났다. 이는 기존의 선행연구[8]에서 제시된 정보 프라이버시 위험에 대한 인식이 높아질수록 개인의 정보 프라이버시 염려가 높아진다는 것과 동일한 결과를 보여주었고, 침해경험은 정보 프라이버시 염려에 정(+)의 영향을 미치고 있는 것으로 나타났다. 이는 이전의 개인정보 침해경험이 있는 자는 개인정보에 대한 정보 프라이버시 염려도를 증가시킨다는 연구와 동일한 결과를 보여주었다.

정보 프라이버시 정책과 염려간의 연구 결과 정책은 정보 프라이버시 염려에 정(+)의 영향을 미치는 것으로 나타났다. 이는 개인정보를 수집·취급하는 기업에서 정보 프라이버시 정책 내용을 소비자가 쉽게 이해하고 명확하게 인식할 수 있도록 정비가 필요하다는 것을 의미한다.

정보 프라이버시 통제 기능과 염려간의 연구 결과 자신의 정보에 대한 통제 기능이 적다고 느끼면 염려에 정(+)의 영향을 주는 것으로 나타났다[15]. 이에 따라 개인정보를 정보를 제공하는 소비자에게 자신의 정보를 통제할 수 있는 기능을 추가하여 정보 프라이버시에 대한 염려도를 낮추어 스스로 정보를 통제할 수 있다는 의식을 마련해 줄 필요성이 있다고 판단된다.

둘째, 정보 프라이버시 염려와 개인정보 제동의도간의 연구결과 자신이 느끼는 정보 프라이버시 염려가 높아질수록 개인정보 제공의도에 부(-)의 영향을 주는 것으로 나타났다[16]. 이러한 결과를 비추어 보면, 개인정보를 수집·활용하는 기업은 정보 프라이버시 염려를 낮출 수 있는 방안을 연구하여 소비자에게 제공한다면 개인정보 제공의도가 높아질 것이다.

셋째, 회귀계수의 중요도를 나타내는 표준화 계수는 정보 프라이버시 위험이 .463으로 가장 크게 나타났으며, 정보 프라이버시 정책이 .285, 정보 통제가 .116 그리고 침해 경험이 .051로 가장 낮은 설명력을 보였다. 이는 정보 프라이버시에 대한 위험요인이 정보 프라이버시 염려에 가장 큰 설명력을 보이는 것으로 나타났다.

본 연구에서 제안된 정보 프라이버시 위험, 침해경험, 정책, 통제 기능 및 염려가 개인정보 제공의도에 미치는 영향도를 분석하기 위해 연구모델과 가설을 검증한 결과,

다음과 같은 시사점을 찾을 수 있다.

우선, 정보 프라이버시 위험, 침해경험, 정책 및 통제 기능 등 4개 요인이 정보 프라이버시 염려에 주는 설명력(51.3%)을 고려하면, 충분히 설명하고 있다고 판단되지만, 새로운 외생 변수에 대한 연구가 필요하다고 볼 수 있다. 따라서 본 연구는 IoT 시대의 정보 프라이버시에 대한 연구 모형을 확장할 수 있는 이론적 기초를 제공할 수 있다고 판단된다.

둘째, 정보 프라이버시 염려가 개인정보 제공의도에 주는 영향도를 고려하였을 때 개인정보 제공의도에 대한 설명력이 매우 약하게 나타났다. 이는 IoT, 빅데이터, 클라우드 컴퓨팅 등 다양한 정보기술이 등장하여 많은 정보가 수집되어 별도로 개인정보 제공에 생각이 줄었으며, 또한 최근에 발생한 개인정보 유출 사고로 인하여 개인정보 제공에 대한 생각이 감소했다는 것으로 판단할 수 있다. 마지막으로 개인정보를 활용하여 의료, 복지, 교육 등 맞춤형 서비스를 제공하려는 기업들은 정보 프라이버시에 대한 이슈가 소비자의 개인정보 제공의도를 저해한다는 점을 인식하고 정보 프라이버시와 관련한 정책을 마련해야 할 것이다.

본 연구는 학문적, 실무적인 측면에서 몇 가지의 시사점을 지니고 있지만, 한계점도 지니고 있어 이를 지적하고 향후 연구방향을 제시하고자 한다.

기존의 연구들은 개인정보 보호에 대해 연구가 진행되어 왔으며, 새로운 정보환경인 IoT 시대에 대한 연구가 별로 없는 상황이다. 또한 개인정보의 이용과 활용 측면에 대한 연구도 별로 없기 때문에 이를 설명하기 위해 개인정보 보호와 관련한 변수를 활용하기에는 무리가 있다.

따라서 향후 연구에서는 새로운 정보환경에 적용 가능한 정보 프라이버시 요인을 개발하여 연구를 추진해야 할 것이다. 또한 개발된 요인을 활용하여 IoT 기반의 서비스인 커넥티드 카, 스마트 가전, 헬스 케어 및 스마트 시티 등에서 발생 할 수 있는 정보 프라이버시 및 개인정보 침해 방지를 위한 연구로 확대 할 수 있을 것이다.

ACKNOWLEDGMENTS

This research was supported by the 2014 Incheon National University Research Fund.

REFERENCES

[1] Personal Information Protection Commision, "Research of personal information protection measures due to the widespread use of smart devices", 2014.

[2] Cheon-Woong Park, Jun-Woo Kim. An Empirical Research on Information Privacy and Trust Model in the Convergence Era, Journal of Digital Convergence, Vol. 13, No. 4, pp.219-225, 2015.

[3] Gartner, "Gartner Says the Internet of Things Installed Base Will Grow to 26 Billion Units By 2020", (http://www.gartner.com/newsroom/id/2636073)

[4] Min Kyung Sik, Park Hee Woon, Global Trends discussion on privacy in the IoT environment, Institute for Information & communications Technology Promotion, pp. 12-23, 2015. 06.17.

[5] O. Garcia-Morchon, D. Kuptsov, A. Gurtov, K. Wehrle, Cooperative security in distributed networks, Comp. Commun. Vol. 36 No. 12, pp. 1284 - 1297, 2013.

[6] Na Sung Hyun, Privacy issues in IoT environment, Korea Information Society Development Institute, Premium Report, Vol. 15, No. 06, 2015.

[7] Rodrigo Roman, Jianying Zhou, Javier Lopez. On the features and challenges of security and privacy in distributed internet of things, Computer Networks, Vol. 57, pp. 2266-2279, 2013.

[8] Eleonora Borgia, The Internet of Things vision: Key features, applications and open issues, Computer Communications, Vol. 54, pp. 1-31, 2014.

[9] Son, J. Y. and Kim S. S, Internet Users' Information Privacy - Protective Responses: A Taxonomy and a Nomological Model, MIS Quarterly, Vol. 32, No. 2, pp. 503-529, 2008.

[10] Dinev, T. and Hart, P. Privacy Calculus Model in E-commerce - A Study of Italy and the United States, European Journal of Information Systems, 15, pp.389 - 402, 2006.

[11] Buchanan, T., Paine, C., Joinson, A. N., Reips, U. D. Development of Measures of Online Privacy Concern and Protection for Use on the Internet, Journal of the American Society for Information

Sciences and Technology, Vol. 58, pp.157-165, 2007.
[12] Sanghyun Kim, Hyunsun Park. An Analysis of Influence Factors on Privacy Protection Awareness and Protection Behavior and moderating Effect of Privacy Invasion Experience, The Journal of Internet Electronic Commerce Research, Vol. 13, No.4, pp. 79-105, 2013.
[13] Culnan, M. J. How Did They Get My Name? : An Exploratory Investigations of Consumer Attitudes toward Secondary Information Use, MIS Quarterly, Vol. 17, No. 3, pp.341-363, 1993.
[14] Smith, H. J., Milberg, S. J., and Burke, S. J. Information Privacy: Measuring Individuals Concerns about Organizational Practices, MIS Quarterly, Vol. 20, No. 6, pp.167-196, 1996.
[15] Malhotra, N. K., Kim, S. S., and Agarwal, J. Internet Users Information Privacy Concerns : The Construct, the Scale, and Causal Model, Information System Research, Vol. 15, No. 4, pp.336-355, 2004.
[16] Yuan Li. The Impact of Disposition to Privacy, Website Reputation and Website Familiarity on Information Privacy Concerns, Decision Support Systems, Vol. 57, pp.343 - 354, 2014.
[17] Jun-Young Go, Keun-Ho Lee, "SNS disclosure of personal information in M2M environment threats and countermeasures", Journal of the Korea Convergence Society, Vol. 5, No. 1, pp. 29-34, 2014.
[18] Hyeon-Ho Park, Hee-Ock Nho, Yong-Ho Kim, "The Impact of Perceived IT Threat on Convergence Information System Performance", Journal of the Korea Convergence Society, Vol. 6, No. 3, pp. 65-71, 2015.

박 천 웅(Park, Cheon Woong)

- 2003년 2월 : 인천대학교 독어독문학과 (문학사)
- 2006년 2월 : 인천대학교 경영학과 (경영학 석사)
- 2015년 2월 : 인천대학교 경영학과 (경영학 박사)
- 2007년 12월 : 한국문화관광연구원 통계정보센터 연구원
- 2009년 7월 ~ 현재 : 한국데이터베이스진흥원 선임연구원
- 관심분야 : 프라이버시, 데이터 유통, 개인정보 활용
- E-Mail : cwpark@kodb.or.kr

김 준 우(Kim, Jun Woo)

- 1985년 8월 : 서강대학교 경제학과 (경제학 석사)
- 1988년 8월 : University of Virginia(경영학 석사)
- 1992년 8월 : University of Virginia (경영학 박사)
- 1992년 8월 : 한국통신 선임연구원
- 1994년 8월 ~ 현재 : 인천대학교 교수
- 관심분야 : 프라이버시, MIS, 데이터베이스
- E-Mail : jwkim@incheon.ac.kr