사물인터넷 시대의 개인정보과잉이 정보프라이버시 보호반응에 미치는 영향

소원근* · 김하균**

<요 약>

사물인터넷, 빅 데이터, 클라우드 컴퓨팅 등의 정보과잉시대를 맞이하여 개인의 의지와는 상관없이 데이터가 수집되고 정보가 처리된다. 연구의 목적은 개인정보과잉이 정보프라이버시 위험, 정보프라이버시 염려(수집, 통제, 인식)와 개인정보 프라이버시보호반응에 관련된 모형을 제시하고 실증분석을 하였다.

연구의 주요결과를 요약하면 다음과 같다. 첫째, 개인정보과잉은 정보프라이버시 위험에 유의한 영향을 미치는 것으로 나타났다. 둘째, 개인정보과잉은 정보프라이버시 염려(수집, 통제, 인식)에 유의한 영향을 미치는 것으로 나타났다. 셋째, 정보프라이버시 위험은 정보프라이버시 염려의 수집, 인식에 유의한 영향을 미친 반면, 통제는 유의한 영향을 미치지 않는다. 이러한 결과는 정보과잉으로 인한 개인정보가 개인의도와 다르게 정보가 다른 방향으로 이용될지도 모른다는 것이다. 정보위험을 개인정보사용자는 정보의 수집과정에서 인지하고 있음을 알 수 있다. 정보에 대한 통제는 개인정보사용자가 가능하지 않는 것으로 판단되어, 정보프라이버시 염려(통제)는 유의한 영향을 미치지 않는 것으로 나타났다. 넷째, 정보프라이버시 염려(수집, 인식)는 정보프라이버시 보호반응에 유의한 영향을 미치는 것으로 나타났으나, 정보프라이버시(통제)는 유의한 영향을 미치지 않는 것으로 나타났다.

결론적으로 개인정보사용자는 개인정보과잉으로 인해 정보침해를 염려하고 있으며, 자신의 정보에 대한 보호능력이 강해질 것이다.

핵심주제어: 개인정보과잉, 정보프라이버시 위험, 정보프라이버시 염려, 개인프라이버시 보호반응

논문접수일: 2016년 01월 23일 수정일: 2017년 02월 20일 게재확정일: 2017년 02월 24일
* 수원대학교 경영학부 교수(제1저자), s76412@hotmail.com
** 부경대학교 경영학부 교수(교신저자), kimhk@pknu.ac.kr

I. 서 론

정보기술이 발전함에 따라 정보취득이 사람과 사람에서 사람과 기계, 기계와 기계로의 교환이 되는 시대에 있다. 이러한 새로운 형태의 정보교환시대가 사물인터넷(Internet of Things, Iot)시대이다. 사물인터넷의 장점은 사람의 의지와 상관없이 스스로 데이터를 수집하고 정보를 처리한다. 사물인터넷을 통해 기기와 기기 간의 커뮤니케이션이 가능하며, 상호간 통신하면서 새로운 정보를 생산한다. 사물인터넷은 시간이나 장소에 관계없이 사물이 인터넷을 통해 통제되어 정보를 공유하거나 처리하는 새로운 융합서비스이며, 이를 통해 새로운 부가가치를 창출하는데 기대하고 있다. 사물인터넷을 비롯하여 빅 데이터, 클라우드 컴퓨팅 등의 정보기술의 급변으로 데이터 량이 급격히 증가하면서 개인정보과잉으로 인한 우려가 나타나고 있다. 사물인터넷을 기반으로 수집되는 개인정보과잉은 개인정보에 대한 침해 및 피해가 우려되고 있다(채수연 외, 2016). Smith 등(1996)의 연구에서 개인정보는 정보사용의 목적과 사용량에 상관없이 사용자의 개인정보를 침범할 여지가 있으며, 사용자는 개인정보 침범에 대하여 항상 조심해야한다고 설명하였다.

정보프라이버시의 연구들을 기초로 기존연구에서 정보프라이버시 보호정책과 수단이 다양하게 연구되었다. 하지만 정보프라이버시 침해에 대한 사용자의 염려는 계속적으로 증폭되고 있다. 이는 사물인터넷, 빅데이터 등의 정보가 증가하고 정보기술을 사용한 정보에 대한 분석과 발전이 증가하면서 침해위협도 크게 증가한 결과이다. 사물인터넷 환경에서 스마트기기를 통한 정보수집의 변화로 인한 피해가 발생되고 있으며, GPS해킹, 스마트 TV 및 스마트 워치 등의 사물인터넷 기기 들은 보안에 취약하다. 사물인터넷을 활용함으로 정보취득이 편리해졌지만 사물인터넷으로 생산된 정보가 무분별하게 확대되고 있다(박천웅・김준우, 2016). 기존의 정보프라이버시 연구들은 정책적 관점이나 기술적 관점에서 사용자의 위험을 보호하는데 집중해 왔다. 하지만 개인의 사생활 측면에서 정보프라이버시 보호에 대한 연구는 부족한편이다.

본 연구는 사물인터넷 시대의 정보과잉으로부터 정보침해를 우려하여 정보보호에 어떠한 영향을 주는지 알아보고자 한다. 연구의 목적은 다음과 같다. 첫째, 사물인터넷, 빅데이터 등의 데이터가 많아질수록 개인은 정보에 대한 위험에 노출된다. 개인정보과잉이 정보프라이버시 위험에 영향을 미치는지를 알아본다. 둘째, 개인정보과잉이 정보프라이버시 염려에 영향을 미치는지를 알아본다. 정보프라이버시 염려에 따른 사물인터넷 사용자의 개인정보과잉을 살펴보기 위하여 정보프라이버시 염려(수집, 통제, 인식)를 3가지 변수로 구성된 IUIPC(Internet User Information Privacy Concern)모델을 사용하였다. 셋째, 개인정보과잉으로 개인정보위험을 느끼면 이를 감소시키기 위해 노력하게 된다. 사물인터넷 사용도 좋지만 정보프라이버시 위험을 줄여야 한다. 사물인터넷을 사용할 때 알 수 있는 사용자들의 정보프라이버시 위험과 정보프라이버시 염려사이에 관계가 있는지 알아보고자 한다. 넷째, 정보프라이버시 염려는 사물인터넷 환경에서 정보프라이버시 보호반응을 일으키는 변수로 개인정보의 노출에 대한 염려가 클수록 개인정보노출을 방어하게 될 것이다. 정보프라이버시 염려가 정보프라이버시 보호반응에 영향을 미치는지를 알아본다.

Ⅱ. 이론적 배경

1. 사물인터넷(Internet of Things, Iot)

사물인터넷은 외부에서 사용자의 제어에 의하여 작동하는 스마트기기와 센서를 포함한 모든 기기들이 내·외부 환경과 상호작용하도록 인터넷과 연결하는 기술이다(채수연 외, 2016). 사물인터넷은 개인정보, 기존의 데이터와 데이터의 전송 등이 보장되어야 한다. 사물인터넷의 효과로 다양한 영역(개인, 기업, 산업)에서 새로운 제품, 서비스 및 프로그램 등이 생겨날 것이다. 이로 인하여 개인과 기업에게 실질적인 혜택이 주어진다(Schults와 Vodenbosch, 1998).

사물인터넷의 확산은 데이터 수집, 축척 및 분석이 가능한 기기가 증가하고 있다. 방대한 양의 데이터 생성과 함께 분석이 다양한 분야에서 데이터 활용이 가능하며, 이러한 측면이 개인정보 보호에 대한 관심을 불러일으킨다. 사물인터넷시대에는 사용자정보를 보호를 위해서는 기존의 정보보호정책보다는 사물인터넷환경에 맞도록 정보보호정책을 개정하여야 한다(안주아, 2008; 박영태, 2015). 또한 사물인터넷시대가 활성화하기 위해서는 보안환경에서 데이터 통합, 데이터 분석, 개인정보보호 및 사용자기기에 대한 보안도 필요하다고 하였다(신문식 외, 2012). 미래창조과학부도 국내 IoT 시장 규모가 2013년 2조 3,000억원에서 2020년에 30조원으로 13배 성장할 것으로 예측하고 있다(박영태, 2015).

2. 개인정보과잉(Personal Information Overload)

최근 사물인터넷이 주목받는 이유는 최근에 개인들이 직접적으로 생산하는 정보의 량이 급격히 증가했기 때문이다. 정보량에 대한 정의는 기존연구마다 차이가 있다. 개인정보량이 많아지면 정보처리 능력이 떨어져 의사결정이 합리적으로 이루어지지 않는다는 것은 일반적으로 견해이다. 정보처리의 양이 정보처리 능력을 앞지르거나 정보를 처리할 수 있는 가능한 범위를 벗어난 현상을 “정보과잉(Information Overflow)”이라고 한다(Schults와 Vodenbosch, 1988). 정보과잉이란 사물인터넷 및 빅데이터 등의 정보처리의 증가와 다양화가 정보를 확장시켜주었지만 이용자들이 접근할 수 있는 한계를 넘어섰기 때문이다(김영석, 2002). 정보사용자들은 개인정보과잉에 대하여 다양한 견해와 이해의 차기가 있지만, 과도한 정보는 의사결정력을 떨어뜨린다(Grise와 Gallupe, 2000). 개인정보과잉은 소셜미디어의 발전, 모바일기기의 대량보급과 대용량의 데이터 저장 및 분석이 개인정보과잉의 원인이다. Shenk(1997)는 정보과잉이 개인과 조직에서 중요한 문제가 되었으며 해결책으로 과거에 사용된 기법과 전략은 더 이상 효과적이 않음을 지적했다.

3. 정보프라이버시 위험(Information Privacy Risks)

프라이버시 위험은 계속적으로 연구가 진행되어오고 있다. 인터넷 쇼핑, 소셜미디어 및 간편결제 등의 정보기술이 발달될수록, 기존의 연구에서 정보 프라이버시 위험에 관한 연구가 증가하고 있다. 인터넷 환경에서는 기업과 기업, 정부와 기업, 사용자와 기업이 컴퓨터 네트워크를 통해서 이루어진다. 컴퓨터와 네트워크를 통해서 개인의 정보가 생성, 축척 및 분석되기 때문에 오프라인 환경보다 개인정보위험이 높다.

온라인 환경에서 사용자의 정보프라이버시 위험은 다양하게 도출되고 있으며, 크게 제품에 대

한 불확실성과 관련된 위험과 온라인이라는 특성으로 인해 거래과정에서 발생하는 위험으로 분류된다(안주아, 2008; 전성률・박현진, 2003; 강석주・김창태, 2000). 정보프라이버시 위험은 동일한 상황일지라도 사용자 개개인에 따라 위험의 유형과 정도에 따라 달라질 수 있으며(신문식 외, 2012; 신민경 외, 2004), 일반적으로 인터넷 환경의 경우 개인 사용자의 정보를 더 많이 수집하고 그러한 정보를 보다 장기적으로 축적하고 있을수록, 그리고 사용자가 가지고 있는 고유정보 또는 개인정보를 더 많이 활용할수록 사용자의 사적인 온라인 활동이 기업에 의해 침해될 위험성이 높아진다(이준기 외, 2007; 김재휘 외, 2010). 개인정보가 네트워크상에서 유통되는 과정에서 해킹되거나 도용됨으로써 유출될 위험이 있기 때문에 인터넷의 이용이 급증함에 따라 개인정보가 악용될 위험성 또한 증가하고 있다(남지연・나종연, 2009).

4. 정보프라이버시 염려(Information Privacy Concerns)

인터넷을 통한 커뮤니케이션, 사물인터넷, 온라인 거래 및 전자상거래가 발전됨에 따라 사용자들은 개인정보를 자신도 모르게 인터넷상에 제공하게 되며, 이에 따라 인터넷사용자의 프라이버시 염려는 증가한다.

Malhotra 등(2004)은 프라이버시 염려 모델을 기초로 온라인 환경에서 인터넷 사용자의 정보프라이버시 염려를 파악할 수 있는 IUIPC모델을 제안하였다. IUIPC는 정보프라이버시 염려(수집(collection), 통제(control), 인식(awareness))를 3변인으로 구성하였다. IUIPC는 Smith 등(1996)와 Stewart와 Segars(2002)의 연구를 더욱 발전시킨 모델로 '정보에 대한 자기결정권의 개념이 증가한 것이다. 본 연구에서는 개인정보과잉과 정보프라이버시 염려를 기본으로 모델을 설정함에 따라 개인정보과잉과 정보 프라이버시 염려를 실증적으로 측정할 수 있는 IUIPC모델을 사용하였다. 박천웅・김준우(2016)는 사물인터넷시대의 정보프라이버시 염려에 대한 연구에서 정보프라이버시 중에 정보프라이버시 위험이 정보프라이버시 염려에 영향을 미친다고 했다. 사용자 스스로가 자신의 개인정보를 선택하고 결정할 수 있는 여지가 낮을수록 사용자의 심리적 저항이 강해 정보프라이버시 위험을 느끼게 된다(남지연・나종연, 2009; 김재휘 외, 2010; 정철화・남수현, 2011).

5. 정보프라이버시 보호반응 (Information Privacy Protective Response)

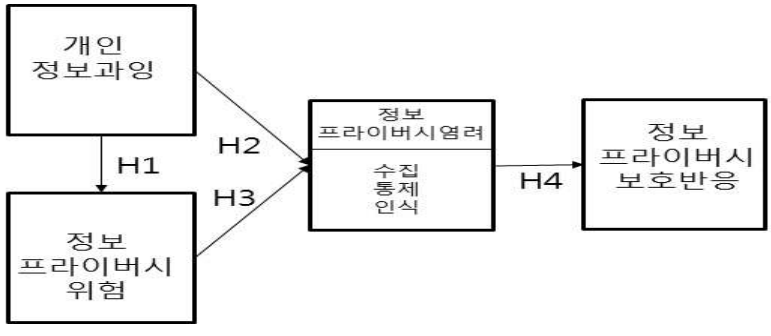
정보프라이버시 보호반응은 사용자의 불평행동에서부터 발생하는 것으로, 사용과정에서 불만족이나 문제 상황을 경험하고 그로 인한 피해를 받았을 경우 사용자들이 그 문제 상황의 해결을 위해 주변의 사람들이나 온라인 기업, 혹은 사용자단체 등에 자신의 의견과 정보를 전달하는 것으로 정의할 수 있다(성승현, 2001). 정보프라이버시 보호반응에서 개인의 특성은 심리적으로 자신행동이나 의도에 영향을 미친다. 이를 바탕으로 불평행동과 관련된 보호반응 연구들은 사용자 개인의 개별특성 성향이 불평행동을 설명하는 주요 요인으로 제기하였다(Mowen와 Speers, 1999). 사용자들은 자신과 관련된 정보가 상업적으로 활용될 수 있는 위험성에 매우 민감하게 반응하는 경향을 가지고 있으며, 이때의 사용자 반응은 불쾌, 불안, 두려움 등과 같은 부정적인 감정반응을 동반하게 된다(김재휘 외, 2010; Sheehan와 Hoy, 2000).

정보프라이버시 보호반응의 첫 번째 심리적 요인은 위험회피(Risk-aversion)성향이다. 위험회피성향이란 불확실하거나 애매모호한 상황에 대해 위험을 느끼거나 이러한 상황을 피하려는 심리적 경향을 의미하는 것으로 위험회피성향이 높은 사용자는 위험과 불확실한 상황을 위험으로 느끼는 성향이 있다(Hofstede, 2001). 두 번째 심리적 요인은 자기주장성향(Assertiveness)이다. 자기주장성향이란 개인의 최적의 이익을 위해 자신의 뜻을 표현하는 것을 말하며, 자기주장성향이 강한 사용자의 경우 자신이 믿는 신념에 따라 행동하며 자신의 미래나 운명을 스스로 결정할 수 있다고 생각 한다(Richins, 1983). 이처럼 사용자들의 심리적 요인은 다양하게 나타나며, 개인의 서로 다른 심리적 요인은 정보 프라이버시 보호반응에도 중요한 영향을 미치게 된다(Morel 등, 1997). 이동주 외(2010)는 개인정보의 제공에 따른 피해경험을 파악하고, 피해경험이 개인정보 보호반응에 어떠한 영향을 미치는가를 분석하였다. 분석결과, 개인정보보호반응은 개인정보 보호 필요성에 대한 인지도가 높을수록 높은 영향을 받는 것으로 분석되었다.

Ⅲ. 연구의 설계

1. 연구의 모형

본 연구에서는 사물인터넷 사용에 따른 개인정보과잉이 정보프라이버시 위험, 정보프라이버시 염려(수집, 통제, 인식)를 매개로 정보프라이버시 보호반응에 어떠한 영향을 미치는지를 알아보는데 목적이 있다. 사물인터넷을 사용하는 과정에서 정보프라이버시 보호반응을 알아보고자 한다. 기존의 선행연구를 바탕으로 설계되어진 연구모형을 제시하면 <그림 1>과 같다.



<그림 1> 연구모형

2. 연구의 가설

2.1 개인정보과잉, 정보프라이버시 위험과 염려에 관한 가설

이환수 외(2013)는 빅데이터 시대의 개인정보과잉과 사용자 저항에 대한 연구에서 개인정보과잉이 정보프라이버시 위험에 영향을 미친다고 하였다. 박현선・김상현(2016)은 소셜네트워크의 피로감연구에서 정보과잉이 SNS 피로감에 영향을 미친다고 하였다. 곽관훈(2014)은 기업의 빅데이터의 활용에서 정보과잉으로 인한 정보위험으로부터 개인정보가 보호되어야하며, 개인보호

를 위한 법제도의 정비가 필요하다고 했다.

가설 1: 개인정보과잉은 정보프라이버시 위험에 유의한 영향을 미칠 것이다.

가설 2: 개인정보과잉은 정보프라이버시 염려에 유의한 영향을 미칠 것이다.

가설 2-1: 개인정보과잉은 정보프라이버시 염려 중 수집에 유의한 영향을 미칠 것이다.

가설 2-2: 개인정보과잉은 정보프라이버시 염려 중 통제에 유의한 영향을 미칠 것이다.

가설 2-3: 개인정보과잉은 정보프라이버시 염려 중 인식에 유의한 영향을 미칠 것이다.

2.2 정보프라이버시 위험과 정보프라이버시 염려에 관한 가설

박천웅・김준우(2016)는 사물인터넷시대에서 정보프라이버시 위험이 정보프라이버시 염려에 영향을 미친다고 했다. 채수연(2016)은 사물인터넷의 환경에서 지각된 정보프라이버시 위험은 정보프라이버시 염려에 영향을 미친다고 했다. 사용자의 개인정보에 대한 통제권 및 선택권 상실로 인해 자신의 개인정보 노출에 대한 심리적 불안감, 즉 정보프라이버시 위험을 느끼게 되며, 자신의 개인정보 제공에 대한 정보프라이버시 염려에 영향을 미치는 것으로 나타났다(최혁준・전기홍, 2012; Awad와 Krishnan, 2006). Van Slyke 등(2006)은 정보프라이버시 염려 모델을 이용하여 지각된 위험과 정보프라이버시 염려의 관계를 알아보고자 하였다. 따라서 다음과 같은 가설을 설정하였다.

가설 3: 정보프라이버시 위험은 정보프라이버시 염려에 유의한 영향을 미칠 것이다.

가설 3-1: 정보프라이버시 위험은 정보프라이버시 염려 중 수집에 유의한 영향을 미칠 것이다.

가설 3-2: 정보프라이버시 위험은 정보프라이버시 염려 중 통제에 유의한 영향을 미칠 것이다.

가설 3-3: 정보프라이버시 위험은 정 프라이버시 염려 중 인식에 유의한 영향을 미칠 것이다.

2.3 정보프라이버시 염려와 정보프라이버시 보호반응에 관한 가설

사용자들은 자신의 정보가 상업적인 목적으로 활용된다는 것에 대해 부정적으로 반응하며 자신의 개인적인 정보를 공개하려고 하지 않는다(김윤환・최영, 2009). 박정훈・이숙현(2007)은 개인정보프라이버시 염려에도 불구하고 다양한 상황에서 개인정보를 제공하는 모순된 행태를 보이지만, 정보프라이버시 염려는 정보프라이버시 보호행동에 영향을 주는 것으로 나타났다. Son과 Kim(2008)은 정보프라이버시 염려에 대한 연구에서 온라인 회사의 개인정보의 잘못된 사용은 상당한 손실을 발생시킬 수 있으므로 프라이버시 보호반응 행동을 갖는다고 설명하였다. 따라서 다음과 같은 가설을 설정하였다.

가설 4: 정보프라이버시 염려는 정보프라이버시 보호반응에 유의한의 영향을 미칠 것이다.

가설 4-1: 정보프라이버시 염려 중 수집은 정보프라이버시 보호반응에 유의한 영향을 미칠 것이다.

가설 4-2: 정보프라이버시 염려 중 통제는 정

보프라이버시 보호반응에 유의한 영향을 미칠 것이다.

가설 4-3: 정보프라이버시 염려 중 인식은 정보프라이버시 보호반응에 유의한 영향을 미칠 것이다.

3. 변수의 조작적 정의

연구모형을 측정하기위해 변수 및 조작적 정의 및 설문은 <표 1>과 같다.

<표 1> 조작적 정의 및 설문사항

변수명	조작적 정의	세부사항	참고문헌
개인정보과잉	정보의 양이 처리 가능한 범위를 벗어난 정도	-정보의 양이 많음 -정보를 찾는 시간이 길고 많음 -많은 정보에 대한 불안감	Grise와 Gallupe(2000) Schultz와 Vandenbosch(1998) Shenk(1997)
정보 프라이버시 위험	개인정보가 알려짐으로 정보노출 범죄 및 사생활 추적의 가능성	-정보노출이 범죄에 이용 -사생활 추적의 가능성 -불특정 사람에게 정보노출	안주아(2008) 전성률・박현진(2003)
정보 프라이버시 염려(수집)	개인을 식별할 수 있는 정보를 너무 많이 수집하고 저장하는 것에 대한 염려	-개인정보 요구의 귀찮음 -개인정보 유출에 대한 걱정 -지나친 개인정보 요구	Malhotra 등(2004) Stewart와 Segars(2002)
정보 프라이버시 염려(통제)	제공된 개인정보가 개인의 의사에 반하는 경우, 이를 변화시킬 수 있는 영향력 및 통제력을 상실	-개인정보에 대해 자율성 -개인정보 통제력 상실 -개인정보의 사생활 침해	Malhotra 등(2004) Stewart와 Segars (2002)
정보 프라이버시 염려(인식)	조직의 정보 프라이버시 정책에 대해 개인이 충분히 인지하고 있는지에 대한 염려	-개인정보에 대한 명확한 인식 -개인정보정책의 명확한 이해 -개인정보사용의 정확한 인지	Malhotra 등(2004) Stewart와 Segars (2002)
정보 프라이버시 보호반응	개인정보 노출로 인해 생기는 불만족을 공개적으로 표현	-정보제공 거부 -정보에 대한 허위표시 -정보노출의 직접적 항의	Richins(1983) Morel 등(1997)

Ⅳ. 실증분석 및 결과

1. 자료수집 및 표본의 특성

본 연구에서는 개인정보과잉과 정보프라이버시 염려에 대해 인지하고 사물인터넷을 활용하고 있는 사용자를 대상으로 설문조사를 진행하였다. 설문조사는 2016년 7월 15일부터 30일간 실시하였으며 290부를 배부하고 287부를 회수하였다. 현재 사물인터넷 환경에서 스마트기기를 활용하는 20에서 30대를 주로 설문지를 배부하였다. 설문지는 가정의 시큐리티(스마트폰과 연결된 CCTV, 스마트락), 스마트폰을 이용한 주변 환경 정보 제공, 건강관리 및 휘트니스 등을 위한 웨어러블 제품(갤럭시 기어, 나이키 퓨얼밴드, 스마트 체중계) 등을 사용자를 대상으로 설문조사하였다. 회수된 설문지 중에서 불성실한 응답 설문지 15부를 제외한 272부가 설문용으로 사용되었다.

<표 2> 인구통계학적 특성(n=272)

항목		빈도수	비율(%)	항목		빈도수	비율(%)
성별	남	123	45.2	학력	고교졸업	43	15.8
	여	149	54.8		대학교 졸업	87	31.98
연령	20대	208	46.2		대학교 재학	107	39.33
					대학원 재학	16	5.88
	30대	37	26.6		대학원 졸업	17	6.25
	40대	18	13.6		기타	2	0.73
직업	전문직	15	6	1일 사물인터넷 활용 횟수	매일 사용안함	32	0.12
	자영업	36	13		1-3	75	0.28
	사무직	73	27		4-6	71	0.26
	학생	130	48		7-9	42	0.16
	기타	18	7		10회 이상	52	0.19

2. 자료의 분석방법

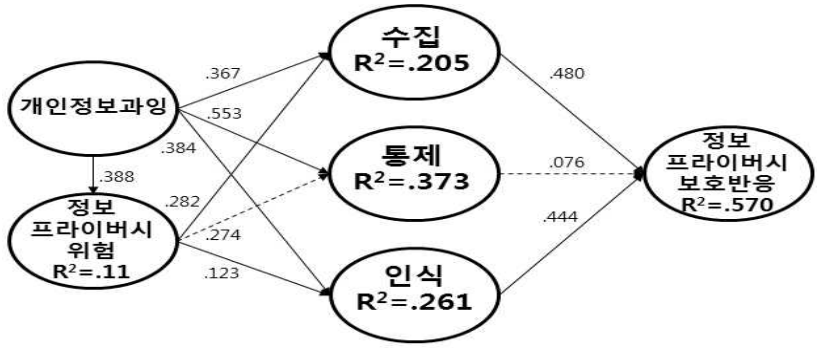
본 연구에서 신뢰성 및 타당성을 측정하기위해 신뢰성 분석과 타당성 분석을 실시하였다. 측정항목간의 내적 일관성을 검증하는 Cronbach's α계수, 합성 신뢰성(CR; Composite Reliability) 그리고 평균분산추출(AVE) 값을 통해 확인하였다. Cronbach's α계수는 0.7이상, CR 값은 0.7이상, AVE값은 0.5이상이면 측정변수들의 신뢰성이 인정된다. 판별 타당성 검정을 위해 <표 4>과 같이 상관계수와 AVE를 비교해 본 결과 대각선으로 표시된 AVE가 각 요인의 상관계수보다 커서 연구 요인들 사이에 존재하는 판별타당성이 확보되었다.

<표 3> 신뢰도 및 타당성 분석결과

변수명		요인적재량	C.R	AVE	Cronbach's α	변수명		요인적재량	C.R	AVE	Cronbach's α
개인정보 과잉	A1	0.835	0.911	0.774	0.854	통제	D1	0.960	0.936	0.836	0.966
	A2	0.916					D2	0.975			
	A3	0.887					D3	0.966			
정보 프라이버시 위험	B1	0.971	0.960	0.889	0.938	인식	Y1	0.977	0.974	0.826	0.960
	B2	0.900					Y2	0.952			
	B3	0.955					Y3	0.956			
수집	C1	0.866	0.908	0.766	0.848	정보프라이버시 보호반응	Z1	0.865	0.915	0.782	0.861
	C2	0.891					Z2	0.881			
	C3	0.869					Z3	0.970			

<표 4> 판별타당성 분석 결과

변수	AVE	개인정보 과잉	정보프라이버시 위험	수집	통제	인식	정보프라이버시 보호반응
개인정보과잉	0.774	**0.880**					
정보프라이버시 위험	0.889	0.338	**0.942**				
수집	0.766	0.367	0.373	**0.875**			
통제	0.836	0.553	0.430	0.480	**0.914**		
인식	0.826	0.498	0.278	0.510	0.400	**0.908**	
정보프라이버시 보호반응	0.782	0.425	0.457	0.655	0.644	0.346	**0.884**



<그림 2> 구조모형 분석 결과

<표 5> 연구모형의 가설 검증 결과

가설	원인변수	결과변수	경로계수	t-값	결과
H1	개인정보과잉	정보프라이버시위험	0.338	3.078**	채택
H2-1	개인정보과잉	수집	0.367	2.522**	채택
H2-2	개인정보과잉	통제	0.553	4.953***	채택
H2-3	개인정보과잉	인식	0.384	5.434***	채택
H3-1	정보프라이버시위험	수집	0.282	2.838**	채택
H3-2	정보프라이버시위험	통제	0.274	1.484	기각
H3-3	정보프라이버시위험	인식	0.124	3.160**	채택
H4-1	수집	정보프라이버시보호반응	0.480	4.670***	채택
H4-2	통제	정보프라이버시보호반응	0.076	0.872	기각
H4-3	인식	정보프라이버시보호반응	0.444	4.449***	채택

$t=1.960^{**}$ ($p<0.05$) $t=3.30^{***}$ ($p<0.001$)

3. 구조모형의 검증

구조모형 분석은 편미분방식인 Smart PLS 2.0을 사용하였으며 경로계수, 가설검정과 내생변수에 대한 결정계수(R^2)값을 도출하였다. R^2값이 0.26이상이면 적합도를 '상'으로 0.26~0.13이면 '중'으로 0.13이하는 적합도를 '하'로 표시할 수 있다(Cohen, 1988). 구성요소 값이 정보프라이버시 위험은 '하', 정보프라이버시 염려(수집)은 '중', 정보프라이버시 염려(통제), 정보프라이버시 염려(인식), 정보프라이버시 보호반응은 각각에 대해 '상'으로 평가할 수 있다.

H1은 개인정보과잉과 정보프라이버시 위험의 관계를 규명하기 위한 것이다. 개인정보과잉은 정보프라이버시 위험에 유의한 영향을 미치는 것으로 나타났다. 이는 기존의 연구(이환수 외, 2013)와 동일하다. 개인정보과잉으로 인해 정보프라이버시의 위험을 느낀다는 것이다. H1은 채택되었다.

H2은 개인정보와 정보프라이버시 염려의 관계를 규명하기 위한 것이다. 정보프라이버시 염려의 수집, 통제 및 인식에 유의한 영향을 미치는 것으로 나타났다. 이는 기존의 연구(이환수 외, 2013)와 동일하다. 개인정보과잉으로 인해 정보프라이버시의 염려를 느낀다는 것이다. H2은 채택되었다.

H3은 정보프라이버시 위험과 정보프라이버시 염려의 관계를 규명하기 위한 것이다. 정보프라이버시 염려(수집, 인식)에 유의한 영향을 미치는 것으로 나타났으나, 정보프라이버시 염려(통제)는 유의한 영향을 미치지 않는 것으로 나타났다. H3에서 H3-1, H3-3는 채택되었고 H3-2는 기각되었다. 이러한 결과는 정보기술이 발전함에 따라 개인정보과잉으로 인한 개인정보가 잘못된 방향으로 사용될 수 있다는 위험을 인지하고 있음을 알 수 있다. 개인정보사용자들이 자신의 정보에 대한 통제는 본인이 할 수 없다는 것으로 판단하여, 정보프라이버시 염려 중 통제에는 유의한 영향을 미치지 못한다는 것이다.

H4는 정보프라이버시 염려와 정보프라이버시 보호반응의 관계를 규명했다. 정보프라이버시 염려(수집, 인식)는 정보프라이버시 보호반응에 유의한 영향을 미치는 것으로 나타난 반면, 통제는 유의한 영향을 미치지 않는다. H4에서 H4-1, H4-3는 채택되었고 H4-2는 기각되었다. 분석결과를 통해 개인정보사용자는 개인정보과잉으로 인해 정보프라이버시 침해를 염려하고 있음을 알 수 있다. 따라서 개인정보를 지키고자 하는 보호능력이 증가함을 알 수 있다. 이는 사용자의 정보를 관리할 수 있는 정보통제의 영향력은 관리자중심으로 이루어지고 있음을 알 수 있다. H4-2는 기각되었다.

<그림 2>와 <표 5>에서 가설검정의 결과를 보여준다.

Ⅴ. 결 론

본 연구는 사물인터넷 시대를 맞이하여 개인의 의지와는 상관없이 데이터가 수집되고 정보가 처리되는 개인정보과잉에서 정보프라이버시 위험, 정보프라이버시 염려와 정보프라이버시 보호에 관련된 모형을 제시하고 실증분석을 하였다. 연구결과로부터 개인정보과잉이 정보프라이버시 보호에 대해 쉽게 접근하고자 하며, 정보의 과잉시대에서 정보생산자(정보사용자)도 자신의 정보의 사용에 대해 정확하게 인지하고 보호할 필요성이 있다.

본 연구의 주요결과를 요약하면 다음과 같다. 첫째, 개인정보과잉은 정보프라이버시 위험에 유의한 영향을 미치는 것으로 나타났다. 개인정보과잉으로 인해 정보프라이버시의 위험을 느낀다는 것이다. 둘째, 개인정보과잉이 정보프라이버

시 염려(수집, 통제, 인식)에 유의한 영향을 미치는 것으로 나타났다. 개인정보과잉으로 인해 정보프라이버시의 염려를 느낀다는 것이다. 셋째, 정보프라이버시 위험이 정보프라이버시 염려의 수집, 인식에 유의한 영향을 미치는 것으로 나타났으나, 통제는 유의한 영향을 미치지 않는 것으로 나타났다. 이러한 결과는 정보기술이 발전함에 따라 정보과잉으로 인한 개인정보의 사용이 잘못된 방향으로 사용된다는 위험을 항상 수집하고 인지하고 있음을 알 수 있다. 사용자들이 자신의 정보에 대한 통제는 본인이 할 수 없다는 것으로 판단하여, 정보프라이버시 염려 중 통제에는 유의한 영향을 미치지 않는 것으로 설명된다. 넷째, 정보프라이버시 염려(수집, 인식)은 정보프라이버시 보호반응에 유의한 영향을 미치지만, 통제는 유의한 영향을 미치지 않는다. 이러한 결과를 통해 개인정보과잉이 정보프라이버시의 침해를 줄 수 있으며 이에 따른 개인정보를 지키고자 하는 정보사용자들의 보호능력이 증가함을 알 수 있다. 실질적으로 과잉된 개인의 정보를 관리할 수 있는 기관에서의 권한 및 통제의 영향력은 개인사용자보다 강하여 개인사용자보다는 중보의 중심이 관리자로 부터 이루어진다고 생각하기 때문이다. 기존연구에서 대부분이 정보프라이버시 염려를 하나의 변수로 인식하고 있으나 보다 세분화할 필요가 있다. 따라서 정보보호에 대한 정보프라이버시의 세부변수까지 정확하게 파악할 필요가 있다. 따라서 본 연구모형을 통해 정보프라이버시 염려를 세분화하였으며, 정보프라이버시 염려의 기존 연구의 한계를 극복할 수 있는 연구결과를 제시하였다고 판단된다.

사물인터넷, 빅데이터 등의 정보기기의 발달과 데이터사용량의 증가로 개인정보 프라이버시에 대한 불안이 증가해지고 있는 현재, 개인정보과잉이 정보프라이버시 위험, 정보프라이버시 염려 및 정보프라이버시 보호반응에 영향을 미치는지를 확인해 보았다는 점에서 논문의 의의가 있다.

참고문헌

1. 강석주 · 김창태(2000), “전자상거래상에서의 정보보호 위협요소 분석에 관한 연구,” *경영과 정보연구,* 4, 1-28.
2. 곽관훈(2014), “개인정보 보호와 이용자 권리: 기업의 빅 데이터 활용과 개인정보의 보호의 조화,” *일감법학*, 27(0), 125-153.
3. 김윤환 · 최영(2009), “IPTV 확산의 심리적 저항요인에 관한 연구: 변형된 혁신저항모형을 중심으로,” *방송통신연구*, 69, 163-191.
4. 김영석(2002). *디지털미디어와 사회*, 서울: 나남출판사.
5. 김재휘 · 성보경 · 부수현(2010), “온라인 맞춤형 광고의 유용성, 편의성, 프라이버시 침해 위험성이 광고 수용의도에 미치는 영향: 소비자의 심리적 반응과 지각된 통제감을 중심으로,” *광고연구*, 87, 263-302.
6. 남지연 · 나종연(2009), “소비자의 위치정보 프라이버시 침해에 대한 우려와 위치기반서비스 사용에 관한 연구,” *소비자정책교육연구*, 5(2), 81-102.
7. 박영태(2015), “국내외 물류산업의 사물인터넷(IoT) 현황과 발전방향에 관한 연구,” *경영과 정보연구,* 34(3), 1-20.
8. 박정훈 · 이숙현(2007), “정보 프라이버시와 관련한 개인의 태도 및 행동 경로분석,” *행정논총*, 45(1), 281-307.
9. 박천웅 · 김준수(2016), “사물인터넷 시대의 정보프라이버시 염려에 대한 실증연구,” *디지털융복합연구*, 14(2). 65-72.
10. 박현선 · 김상현(2016), “SNS 피로감의 선행

요인과 결과요인에 관한 연구- 습관의 조절 효과," *연세경영연구,* 53(1), 43-73.
11. 성승현(2001), "전자상거래에서의 소비자문제와 소비자의 대응행동에 관한 연구," *이화여자대학교대학원 석사학위논문.*
12. 신문식・한상설・김효정(2012), "인지된 위험, 사이트 품질, 사용자 개인성향이 지속적 사용의도에 미치는 영향: 소셜 커머스 사이트를 중심으로," *한국경영교육학회지*, 71, 1-23.
13. 신민경・정순희・여윤경(2004), "인터넷 쇼핑몰에서의 소비자의 위험지각과 정보탐색에 관한 연구," *대한가정학회지*, 42(9), 195-212.
14. 안주아(2008), "인터넷 쇼핑몰 브랜드 소비자의 구매경험에 따른 지각된 위험과 정보탐색 및 구매의도에 미치는 영향," *언론과학연구*, 8(1), 161-194.
15. 이동주・박영석・배윤수(2010, "온라인상의 개인 정보 제공에 있어서 정보 투명성의 역할: 프라이버시 계산 모형을 중심으로," *정보화정책*, 17(2), 68-85.
16. 이준기・최희재・최선아(2007), "서비스의 유용성과 프라이버시 염려도가 개인화 된 서비스 수용성에 미치는 영향에 관한 연구," *한국전자상거래학회지*, 12(4), 37-51.
17. 이환수・임동원・조항정(2013). "빅데이터 시대의 개인정보 과잉이 사용자 저항에 미치는 영향," *지능정보연구*, 14(2). 65-72.
18. 전성률・박현진(2003), "부정적 구전정보의 유형에 따른 구전효과의 차이에 관한 연구," *소비자학연구*, 14(4), 21-44.
19. 정철호・남수현(2011), "SNS 이용자의 프라이버시 염려도와 수용후 행동 간의 구조적 관계에 관한 연구," *경영과 정보연구*, 30(3), 85-105.
20. 채수연・이윤구・정윤혁・최세정(2016), "프라이버시 계산모형 관점에서 스마트 웨어러블기기 사용의도에 관한 연구," *한국정보사회학회*, 17(2), 99-108.
21. 최혁준・전기홍(2012). "인터넷쇼핑몰 브랜드 Identity가 전환 비용 및 브랜드 몰입에 미치는 영향," *e-비즈니스연구*, 13(4), 77-94.
22. Awad, N. F. and M. S. Krishnan(2006). "The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to be Profiled Online for Personalization," *MIS Quarterly*, 30(1), 13-28.
23. Beaudoin, C. E.(2008). "Explaining the relationship between Internet use and interpersonal trust: Taking into account motivation and information overload," *J. of Computer-Mediated Communication*, 13(3) 550-568.
24. Cohen, J.(1998), *Statistical Power Analysis for the Behavioral Science(2nd ed)*, Hillside, Newjersey: Lawrence Erlbaum.
25. Hofstede, G.(2001), "Culture's Consequences: Comparing Values, Behaviors," *Institutions and Organizations across Nations(2nd ed.)*, Sage, Thousand Oaks, CA.
26. Grise M. and R. B. Gallupe(2000), "Information overload: Addressing the productivity paradox in face-to-face electronic meetings," *Journal of Management Information Systems*, 16(3), 157-185.
27. Malhotra, N. K., S. S. Kim, and J. Agarwal(2004), "Internet Users Information Privacy Concerns(IUIPC)," The Construct, The Scale, and a Causal Model, *Information Systems Research*, 15(4), 336-355.
28. Morel, K. P. N., T. Poiesz, and H. Wilke(1997), Motivation, "Capacity and

Opportunity to Complaint Towards a Comprehensive Model of Consumer Complaining Behaviour," *Advances in Consumer Research*, 24, 464-469.

29. Mowen, J. C. and N. Spears(1999), "Understanding Compulsive Buying among College Students: A Hierarchical Approach," *Journal of Consumer Psychology*, 8(4), 407-430.
30. Richins, M. L.(1983), "An Analysis of Consumer Interaction Styles in the Marketplace," *Journal of Consumer Research*, 10(1), 73-82.
31. Schults, U. and Vodenbosch, B.(1998), "Information overload in groupware environment: Now you see it, now you don't," *J. of Organizational Computing and Electronic Commerce*, 8(2), 127-148.
32. Sheehan, K. B and M. G. Hoy(2000), "Dimensions of Privacy Concern among Online Consumers," *Journal of Public Policy & Marketing*, 19(1), 62-73.
33. Shenk, D.(1997). *Sata Smog: Surviving the information glut*, Harperedge: New York.
34. Simth, H. J., S. J. Milberg, and S. J. Burke(1996), "Information Privacy: Measuring Individuals Concerns about Organizational Practices," *MIS Quarterly*, 20(2), 167-196.
35. Son, J. Y. and S. S. Kim(2008), "Internet Users Information Privacy-Protective Response: A Taxonomy and a Nomological Model," *MIS Quarterly*, 32(3), 503-529.
36. Stewart, K. A. and A. H. Segars(2002). "An Empirical Examination of the Concern for Information Privacy Instrument," *Information Systems Research*, 13(1), 36-49.
37. Van Slyke, C., J. T. Shim, R. Johnson, and J. J. Jiang(2006), "Concern for Information Privacy and Online Consumer Purchasing," *Information Systems Research*, 7(6), 415-438.

Abstract

Effects of Information Overload to Information Privacy Protective Response in Internet of Things(Iot)

So, Won-Geun* · Kim, Ha-Kyun**

In the age of information overload such as Internet of Things(IoT), big data, and cloud computing, Data and informations are collected to processed regardless of the individual's will. The purpose of this paper presents a model related to personal information overlord, information privacy risk, information privacy concern (collection, control, awareness) and personal information privacy protective response.

The results of this study is summarized as follows. First, personal information overload significantly affects information privacy risk. Second, personal information overload significantly affects information privacy concern(collection, control, awareness) Third, information privacy risk significantly affects collection and awareness among information privacy concern, but control does not significantly affects. This results shows that users are cognitively aware the information risk through collection and awareness of information. Users can not control information by self, control of information does not affects. Last, information privacy concern(collection and awareness significantly affect information privacy protective response, but information privacy concern (control) does not affect.

Personal information users are concerned about information infringement due to excessive personal information, ability to protect private information became strong.

Key Words: Information of Things(IoT), Information Overload, Information Privacy Risks, Information Privacy Protective Response

* Assistant Professor, Division of Business Administration, Suwon University, s76412@hotmail.com
** Professor, Division of Business Administration, Pukyoung National University, kimhk@pknu.ac.kr