

전자상거래의 프라이버시 정책 인식이 개인정보제공의도에 미치는 영향

The Effect of Privacy Policy Awareness on the Willingness to Provide Personal Information in Electronic Commerce

김 종 기 (Jongki Kim) 부산대학교 경영학과 교수
오 다 운 (Dawoon Oh) 부산대학교 경영학과 박사과정, 교신저자

요 약

본 연구에서는 전자상거래 웹사이트와 인터넷 사용자 간의 신뢰를 높이고 인지된 위험을 완화하는 방법인 프라이버시 정책을 실증적으로 연구하고자 한다. 공정한 정보규정(FIP; Fair Information Practices)의 다섯 가지 요인인 공지, 접근, 선택, 보안, 시행을 통해 프라이버시 정책에 대한 인식을 측정하고 개인정보제공의도에 미치는 영향을 분석하였다. 또한 정책의 인식과 개인정보제공의도 간의 관계에 있어서 인지된 프라이버시 신뢰, 프라이버시 위험의 매개효과를 검증하였고, 개인의 신뢰성향을 프라이버시 정책의 인식과 프라이버시 신뢰 간 관계를 강화하는 요인으로 설정하여 조절효과를 확인하였다. 연구의 결과, 프라이버시 정책 인식과 개인정보제공의도 관계에서 인지된 프라이버시 신뢰와 위험이 통계적으로 유의한 영향을 미치는 것을 확인하였다. 또한 조절변수로 사용된 신뢰성향이 프라이버시 정책의 인식과 프라이버시 신뢰 관계를 강화하는 것으로 나타났다. 본 연구는 공정한 정보규정을 기반으로 프라이버시 정책에 대한 개인의 인식을 측정하여 실증적으로 분석했다는 점에서 의의가 있으며, 연구의 결과가 프라이버시 정책의 향후 연구에 시사점을 제시한다.

키워드 : 정보 프라이버시, 프라이버시 정책, 공정한 정보규정, 프라이버시 신뢰, 프라이버시 위험

I. 서 론

온라인 환경과 새로운 기술이 발달하면서 기하급수적으로 늘어난 전자상거래 시장은 현재까지 많은 사람들이 이용하고 있다. 과거의 전통적인 거래 환경과 달리 원하는 제품이나 서비스 정보에 대한 접근이 쉬워지고 시간과 장소의 경계

가 사라짐으로써 전자상거래는 정보화 사회에서 인터넷을 활용한 유용한 거래수단으로 자리 잡았다. 인터넷 사용자는 전자상거래 웹사이트를 통해 풍부한 정보와 높은 수준의 편의성, 개인화된 서비스를 받기 위해 상당한 개인정보를 제공하고 있다. 그러나 동시에 개인정보 침해, 남용과 같은 부작용에 잠재적으로 노출되며 실제로 이에 대한 문

제가 급증하고 있어 온라인 환경의 프라이버시 문제에 대한 실질적인 개선이 필요하다(Awad and Krishnan, 2006; Bansal *et al.*, 2016; Li *et al.*, 2011).

온라인 환경은 물리적 확실성이 부족하고 디지털화된 정보에 의존하는 상황이므로 불확실성이 높다(민진영, 김병수, 2013). 개인정보를 활용한 서비스가 확대되면서 사용자들은 정보 활용의 투명성을 요구하였으며 이러한 문제점을 해결하고자 기관에서 마련한 대책이 프라이버시 정책이다(Awad and Krishnan, 2006). 프라이버시 정책은 전자상거래 사용자에게 개인정보 수집 및 사용에 대한 공지와 선택권을 제공함으로써 프라이버시 위험을 완화하는 대표 수단이며, 개인의 프라이버시를 보호하기 위해 권고되는 방법 중 가장 보편적이다(Earp *et al.*, 2005).

최근 정보시스템 분야는 프라이버시 정책의 효과가 개인의 태도, 행동에 미치는 영향을 검증하고 개인의 프라이버시 보장 수준을 평가하는 도구로써 프라이버시 실(Privacy Seal)이나 정책을 이용한 연구가 증가하였다. 본 연구에서는 프라이버시 정책의 인식을 실증적으로 측정하여 프라이버시 정책의 효과를 명확히 이해하고자 하였다.

본 연구는 OECD 개인정보보호 가이드라인을 기반으로 개발된 공정한 정보규정(FIP; Fair Information Practices)을 적용하여 프라이버시 정책에 대한 인식을 측정하고, 정책의 인식이 전자상거래 웹사이트의 개인정보 제공의도에 미치는 영향을 규명하고자 한다. 프라이버시 정책의 인식은 공지, 접근, 선택, 보안, 시행 다섯 가지 요인의 2차 요인(Second Order Factor)으로 설정하였다. 또한 프라이버시에 대한 개인의 행동을 설명하기 위해 신뢰-위험 모델을 사용하여 웹사이트가 개인정보를 올바르게 다룰 것이라는 신념을 프라이버시 신뢰, 개인정보를 제공함으로써 나타나는 잠재적 손실을 인지하는 정도를 프라이버시 위험으로 정의한다. 그리고 프라이버시의 선행연구에

의하면 개인은 그들의 신뢰성향에 의존하여 프라이버시 관련 의사결정을 한다. 그러므로 프라이버시 정책의 인식과 개인의 프라이버시 신뢰 간의 관계에서 신뢰성향의 정도가 관계의 강도를 조절하는지 살펴보고자 한다.

본 연구는 전자상거래를 이용하면서 쌓인 프라이버시 정책에 대한 인식을 바탕으로 향후 새로운 전자상거래 웹사이트 회원가입 시 개인정보 제공의도에 미치는 영향을 연구하고자 한다. 평소에 전자상거래 웹사이트가 나의 개인정보를 다루는데 있어서 개인정보수집 동의절차, 처리방침 고지, 보안과 규정에 대한 명시에 대해 인식하는 정도를 측정하여 향후 전자상거래 웹사이트의 개인정보제공의도에 어떠한 영향을 미치는지 설명할 것이다.

II. 이론적 배경

2.1 정보 프라이버시

프라이버시는 사회과학의 학문 분야에서 철학적, 정신적, 사회적, 법적 개념으로 100년 이상 연구되었다. Smith *et al.*(2011)의 연구에서 프라이버시를 가치기반 정의와 인지기반 정의로 분류하였다. 가치기반 정의는 권리로서 프라이버시와 상품으로서 프라이버시, 동일어원 기반 정의는 상태로써 프라이버시와 통제로서 프라이버시로 구분하였으며 <표 1>과 같이 요약하였다.

정보 프라이버시는 프라이버시의 복잡한 특성을 가지며 개인마다 상황이나 인생 경험이 다르므로 다차원 개념이다(Xu *et al.*, 2008). Westin (2003)은 개인정보 공개를 결정하는 개인의 권한으로 정의하였으며, Solove(2006)는 조직이 개인정보를 처리하는 동안 일어나는 문제들의 집합으로 정의하였다. Clarke(1999)는 프라이버시를 도덕적 권리 또는 법적 권리로 보았으며, 많은 연구자들이 자신의 정보를 통제하는 개인의 능력으로 설명하였다.

〈표 1〉 프라이버시 정의(Smith *et al.*, 2011)

가치 기반	권리로서 프라이버시	<ul style="list-style-type: none"> • 프라이버시란 사회의 도덕 가치 시스템에 필수적인 인간의 권리 • Warren and Brandeis(1890)가 프라이버시를 “혼자 있을 권리”로 정의한 후 미국 법에서 하나의 독립된 권리로 인정
	상품으로서 프라이버시	<ul style="list-style-type: none"> • 프라이버시는 절대적인 권리가 아니지만 비용-이익 분석과 상충관계에 있어서 경제학의 대상 • 경제적 주체인 개인이 자발적으로 그들의 데이터 수집에 협조하는 이유는 프라이버시를 개인의 권리에서 인지된 이익을 위해 교환할 수 있는 상품으로 재 개념화 했기 때문
동일 어원 기반	상태로서 프라이버시	<ul style="list-style-type: none"> • 익명성, 고독, 신중함, 친밀함 네 가지 하위 상태로 구별(Westin, 2003) • 개인에게 제한된 접근상태(Schoeman, 1984) • 다른 사람으로부터 분리된 상태(Weinstein, 1971)
	통제로서 프라이버시	<ul style="list-style-type: none"> • 자신에 대한 접근을 선택적으로 통제(Altman, 1975) • 개인과 타인 간 거래의 통제는 자율성을 향상시키고 취약점을 최소화 하는 것이 궁극적인 목표

정보 프라이버시는 정보시스템뿐만 아니라 마케팅, 법, 경영학, 심리학 분야에서 연구되어온 전체 프라이버시 개념의 부분집합이다(Belanger and Crossler, 2011). 정보화 사회에서 개인의 프라이

버시 염려가 중요한 요인으로 부상하였고 이와 관련된 개인의 행동의도를 설명하는 연구가 증가하였다. <표 2>에는 정보 프라이버시 선행연구를 요약하였다.

〈표 2〉 정보 프라이버시 선행연구

연구자	선행요인	매개요인	결과요인
Malhotra <i>et al.</i> (2004)	<ul style="list-style-type: none"> • 인터넷 사용자의 정보 프라이버시 염려 	<ul style="list-style-type: none"> • 신뢰신념 • 위험신념 	<ul style="list-style-type: none"> • 행동의도
Dinev and Hart(2006)	<ul style="list-style-type: none"> • 인지된 프라이버시 위험 • 개인적 인터넷 흥미 	<ul style="list-style-type: none"> • 프라이버시 염려 • 인터넷 신뢰 	<ul style="list-style-type: none"> • 인터넷 거래를 위한 개인정보제공의도
Van slyke <i>et al.</i> (2006)	<ul style="list-style-type: none"> • 프라이버시 염려(CFIP) • 친밀성 	<ul style="list-style-type: none"> • 신뢰 • 위험인식 	<ul style="list-style-type: none"> • 거래의도
Kumar <i>et al.</i> (2008)	<ul style="list-style-type: none"> • 정보 프라이버시 염려 • 보안대책 인식 • 컴퓨터 불안 	<ul style="list-style-type: none"> • 인지된 유용성 • 태도 • 인지된 용이성 	<ul style="list-style-type: none"> • 방화벽 사용의도
Li <i>et al.</i> (2010)	<ul style="list-style-type: none"> • 인지된 관련성 • 인지된 유용성 • 금전적 보상 	<ul style="list-style-type: none"> • 프라이버시 보호신념 • 프라이버시 위험신념 	<ul style="list-style-type: none"> • 행동의도
Liao <i>et al.</i> (2011)	<ul style="list-style-type: none"> • 인터넷 능력 • 사회적 실재감 • 인지된 위험 • 신뢰성향 	<ul style="list-style-type: none"> • 프라이버시 염려 • 신뢰 	<ul style="list-style-type: none"> • 거래의도 • 정보검색의도
Xu <i>et al.</i> (2012)	<ul style="list-style-type: none"> • 산업 자체 규정 • 정부 법 	<ul style="list-style-type: none"> • 개인정보에 대한 인지된 통제 	<ul style="list-style-type: none"> • 정보 프라이버시에 대한 특정 염려

〈표 2〉 정보 프라이버시 선행연구(계속)

연구자	선행요인	매개요인	결과요인
Li(2014)	<ul style="list-style-type: none"> • 프라이버시 경험 • 웹사이트 명성 • 웹사이트 친밀성 	<ul style="list-style-type: none"> • 프라이버시 성향 • 웹사이트에 대한 프라이버시 염려 	<ul style="list-style-type: none"> • 행동의도
Osatuyi(2015)	<ul style="list-style-type: none"> • 외향성 • 상냥함 • 성실성 • 신경증적 • 지적 	<ul style="list-style-type: none"> • 프라이버시 염려 • 컴퓨터 불안 	<ul style="list-style-type: none"> • 행동의도
Choi <i>et al.</i> (2015)	<ul style="list-style-type: none"> • 정보보급 • 네트워크 공용성 	<ul style="list-style-type: none"> • 인지된 프라이버시 침해 • 인지된 유대관계 	<ul style="list-style-type: none"> • 무행동 • 거래 회피 • 대인 관계 회피 • 접근
Bansal <i>et al.</i> (2016)	<ul style="list-style-type: none"> • 프라이버시 침해 • 경험 • 외향성 • 상냥함 • 감정적 안전성 	<ul style="list-style-type: none"> • 프라이버시 염려 • 신뢰 	<ul style="list-style-type: none"> • 공개의도

2.2 프라이버시 정책

온라인에 개인정보를 제공하는 인터넷 사용자는 데이터베이스의 증가와 함께 수집된 많은 양의 개인 데이터에 대해 우려하였고, 개인정보를 수집하고 처리하는 동안 개인의 통제력 상실에 대한 불안이 증가하였다(Culnan, 1993). 기업과 개인 간 정보가 공유되는 동안 발생하는 부당한 상황을 해결하기 위한 기준이 필요했다(최보미 등, 2015). 여러 국가에서 인터넷 사용자의 불안을 완화하기 위해 온라인 프라이버시 정책을 채택하였으며 온라인 회사는 프라이버시 정책을 통해 고객과의 신뢰를 구축하였다(Wu *et al.*, 2012).

1970년 미국의회에서 정보의 투명성, 이용제한, 접근과 수정, 데이터 질, 보안 등을 포함하는 공정한 정보규정원칙을 채택하였으며, 1980년 OECD가 ‘프라이버시 보호 및 개인 데이터의 국경 간 유통에 관한 경제협력개발기구 지침’을 채택하였다. OECD 개인정보보호 8가지 지침은 수집 제한의 원칙, 정보 정확성의 원칙, 목적 명확

화의 원칙, 이용 제한의 원칙, 안전성 보호의 원칙, 공개의 원칙, 개인참여의 원칙, 책임의 원칙으로 구성된다(OECD, 2013).

1998년 연방통상위원회에서 공지/인식, 선택/동의, 접근/참여, 무결성/보안, 시행/시정을 포함하는 ‘공정한 정보규정’ 다섯 가지 핵심원칙을 개발하였다. 이 원칙은 OECD 개인정보보호 8가지 지침을 기반으로 개발되었고(Culnan and Bies, 2003), 이를 통해 형성된 프라이버시 정책은 정보 수집 절차의 투명성을 증가시킨다. 또한 웹사이트의 프라이버시 보호수준을 평가하도록 도와주므로 고객의 정보제공에 대한 여부를 결정한다(Li *et al.*, 2011).

OECD 개인정보보호 가이드라인을 기반으로 국내에서 제정된 법이 개인정보보호법이다(박경신, 2011). 2012년 3월부터 시행된 이 법은 공정한 정보규정에 제시된 개인정보 수집, 사용에 대한 공지, 선택(동의), 접근, 보안, 시행 등의 내용을 포함한다. 국내의 전자상거래 웹사이트는 개인정보보호법을 기반으로 프라이버시 정책을 제정해야 하며, 웹사이트마다 정책을 제공하는 방법은

<표 3> 공정한 정보규정 다섯 가지 핵심원칙

원칙	내용
공지 (Notice)	가장 기본적인 원칙으로 조직이 개인정보를 수집하기 전에 개인정보에 대한 수집, 사용 및 처리와 관련한 사항을 정보 제공자에게 알린다.
접근 (Access)	수집된 개인정보가 정확하고 안전한지 확인할 수 있도록 정보 제공자에게 정보에 대한 접근을 제공한다.
선택 (Choice)	조직이 개인정보 요구 시 개인정보에 대한 사용이나 공개와 관련하여 정보 제공자에게 선택권을 제공하고 그들에게 동의를 구한다.
보안 (Security)	비 허가된 접근으로부터 개인정보를 보호하기 위해 조직이 갖춘 체계 또는 시스템을 말한다.
시행 (Enforcement)	조직이 개인정보와 관련된 법률이나 규정에 따라 개인정보를 다루며 프라이버시 위반에 관한 법적 규정을 명시한다.

다를 수 있으나, 개인정보보호법을 기반으로 제정되어야 하는 기본요소는 같으며 이 요소는 공정한 정보규정의 다섯 가지 핵심원칙에 대한 내용을 포함한다. 공정한 정보규정의 다섯 가지 핵심원칙은 <표 3>과 같다.

공정한 정보규정은 개인의 권리와 조직의 책

임을 가이드라인으로 제시함으로써 프라이버시 관련 문제를 고려한 데이터 보호규정이다. 개인과 조직 간의 약속을 이행하고 조직의 책임을 평가하는 도구이므로 선행연구에서 개인적, 조직적 차원으로 다양하게 연구하였다. 프라이버시 정책과 관련한 연구는 <표 4>와 같다.

<표 4> 프라이버시 정책의 선행연구

연구자	선행요인	매개요인	결과요인
Li et al.(2011)	<ul style="list-style-type: none"> • 인지된 정보 관련성 • 프라이버시 정책의 인지 • 기쁨 • 두려움 	<ul style="list-style-type: none"> • 프라이버시 보호신념 • 프라이버시 위험신념 	<ul style="list-style-type: none"> • 행동의도
Wu et al.(2012)	프라이버시 정책	<ul style="list-style-type: none"> • 프라이버시 염려 • 신뢰 	<ul style="list-style-type: none"> • 개인정보 제공의도
Awad and Krishnan(2006)	<ul style="list-style-type: none"> • 이전의 온라인 프라이버시 침해 • 프라이버시 염려 • 프라이버시 정책의 중요성 	<ul style="list-style-type: none"> • 정보 투명성의 중요성 	<ul style="list-style-type: none"> • 개인화 서비스를 위한 온라인 프로필 의도 • 개인화광고를 위한 온라인 프로필 의도
Xu et al.(2011)	<ul style="list-style-type: none"> • 프라이버시 정책의 효과 • 산업 자체규정의 인지된 효과 	<ul style="list-style-type: none"> • 프라이버시 통제 • 프라이버시 위협 	<ul style="list-style-type: none"> • 프라이버시 염려
Liu et al.(2005)	<ul style="list-style-type: none"> • 프라이버시 (공지, 접근, 선택, 보안) 	<ul style="list-style-type: none"> • 신뢰 	<ul style="list-style-type: none"> • 행동의도
Lauer and Deng(2007)	<ul style="list-style-type: none"> • 프라이버시 정책 	<ul style="list-style-type: none"> • 무결성 • 호혜성 • 능력 • 신뢰 	<ul style="list-style-type: none"> • 고객 신뢰 • 고객 로열티
Zhao et al. (2012)	<ul style="list-style-type: none"> • 프라이버시 정책 • 프라이버시 통제 	<ul style="list-style-type: none"> • 프라이버시 염려 	<ul style="list-style-type: none"> • 위치기반 정보제공의도

2.3 프라이버시 신뢰

온라인 웹사이트에 개인정보를 제공하는 것은 상품과 서비스를 구매하는 경제적 교환뿐만 아니라 관계를 구축하는 사회적 교환을 포함한다. 사회계약을 통해 구성원의 의무나 사회적 규범을 이해함으로써 개인정보를 남용하는 기회주의적 행동으로부터 보호한다(Li, 2012).

신뢰의 개념은 매우 광범위하다. 사회의 법이나 전자상거래 기술과 같은 제도에서 개인의 신뢰인 제도적 신뢰(Institutional Trust), 특정 구성원 또는 제3자에 대한 신뢰인 대인 관계적 신뢰(Interpersonal Trust), 심리학 분야의 연구를 기반으로 다른 사람을 신뢰하는 개인의 태도를 의미하는 신뢰성향(Disposition to Trust) 등이 있다(McKnight and Chervany, 2002). 프라이버시 신뢰란 특정 사람에게 직접적으로 가지는 신념으로 대인 관계적 신뢰로 분류되며 인지적-감정적 반응과 사람 간의 관계에서 상호작용 함으로써 행동을 결정한다. 또한 상대방의 완전성, 호혜성, 일관성을 반영하여 신뢰할 것인지 주관적인 가능성과 의도를 포함한다(McKnight and Chervany, 2002). 본 연구에서 제시하는 프라이버시 신뢰란 나의 개인정보를 다루는 서비스 제공자에 대한 신뢰로서 나의 개인정보를 제공받는 상대방에 대한 신뢰이다. 서비스 제공자가 나의 개인정보를 정직하고 성실하게 다룰 것이라는 인지된 믿음이다. Malhotra *et al.*(2004)에 따르면 신뢰신념이란 회사가 고객의 정보를 보호해준다고 개인이 믿는 정도이며 Li *et al.*(2011)는 프라이버시 보호신념이란 온라인 판매자가 나의 개인정보를 보호해 줄 것이라고 믿는 고객의 신념으로 정의한다.

2.4 프라이버시 위협

온라인 쇼핑으로 제품이나 서비스를 구매하는 고객에게 위협은 일반적인 신념이다. 전통적인 쇼핑은 실제로 제품을 보고 만짐으로 인해 인지

된 위협을 완화할 수 있다. 그러나 온라인 쇼핑을 통한 구매는 고객의 주소, 전화번호, 심지어 신용카드 정보까지 포함된 상당한 개인정보를 웹사이트에 제공해야 한다. 필요한 정보를 제공한 후에 구매자는 거래절차가 온전하게 처리되어 제품이나 서비스를 전달받고 거래가 완전히 끝날 때까지 기다려야 한다. 그러므로 인터넷 사용자가 온라인 쇼핑에 대해 위협을 느끼는 것은 일반적인 일이며 위협은 온라인 구매를 결정하는 데 영향을 미친다(Kim *et al.*, 2008).

일반적으로 전자상거래 상황에서 위협이란 거래의 기록이 제3자에게 유출될 위험, 나의 개인정보가 내 허락없이 다른 사람에게 알려질 위험과 같은 외부적 위협을 의미한다(Dinev and Hart, 2006). 본 연구에서 프라이버시 위협이란 개인정보를 제공함으로써 초래되는 기술적, 외부적 환경에 의한 잠재적 손실을 인지하는 정도이다. Kim *et al.*(2008)에 따르면 인지된 위협이란 온라인 구매를 함으로써 초래되는 부정적인 결과의 불확실성을 말하며, Li *et al.*(2011)은 프라이버시 위협신념이란 특정 회사에 개인정보를 제공함으로써 기대되는 잠재적 손실이라고 정의한다.

2.5 신뢰성향

신뢰성향은 심리학에서 유래된 개념으로서 특정한 상황이나 사람의 범위를 넘어 다른 사람을 신뢰하며, 인간에 대한 신뢰를 가지는 나의 개인적인 성향을 의미한다(Gefen, 2000). 특정 사람에 대한 지식이나 경험 없이 개인의 일생 경험에서 사회화된 결과이므로 일반적으로 다른 사람을 의존하는 정도이다(Kim *et al.*, 2008). 다른 사람은 선하고 믿을 수 있다는 개인의 신념을 기반으로 하며(Gefen *et al.*, 2003), 전자상거래와 같은 새로운 환경에서 고객은 그들의 일반적인 신뢰에 의존하므로 신뢰성향이 더욱 중요한 요인이다(Gefen *et al.*, 2003). 신뢰성향은 낮은 판매자나 새로운 환경에 영향을 미치며 상황을 반영한 제도

적 신뢰에 영향을 준다(McKnight *et al.*, 2002). 고객은 그들의 개인성향을 기반으로 다른 사람을 신뢰하며 이것은 판매자를 의존하는 성향과 관련이 있다(Joubert and Bell, 2013).

일반적으로 신뢰성향은 신뢰의 합리적인 평가와 일반적인 도덕성이므로 의사결정 과정에 포함되며 사회적 규칙, 규범의 영향을 받는다. Yang *et al.*(2009)의 연구에 따르면 전자상거래 웹사이트의 인지된 규범의 수행과 판매자에 대한 신뢰에 있어서 개인의 신뢰성향이 조절효과가 있다고 언급한다. 이와 같은 맥락에서 전자상거래 웹사이트의 프라이버시 정책에 대한 인식이 서비스 제공자에 대한 신뢰에 미치는 영향에 있어서 개인의 특정한 신뢰성향이 관계를 조절한다고 볼 수 있다.

III. 연구모형과 가설

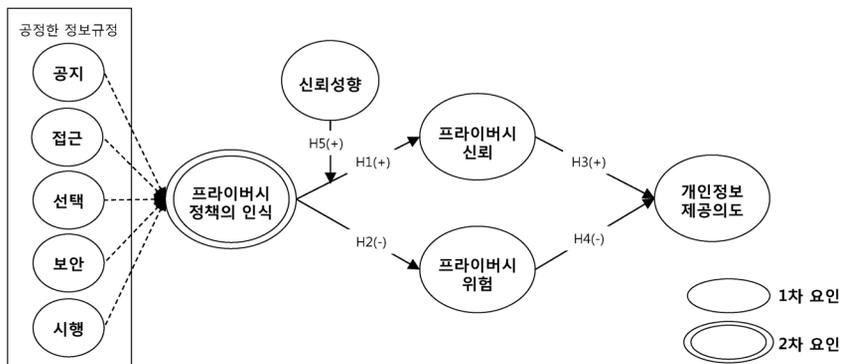
본 연구는 프라이버시 정책에 대한 인식이 개인정보제공의도에 미치는 영향을 실증적으로 분석하고자 <그림 1>과 같은 연구모형을 개발하였다. 본 연구에서 프라이버시 정책의 인식을 측정하기 위해 정책을 형성하는 공정한 정보규정의 다섯 가지 구성요소를 활용하여 2차 요인으로 설정하였다. 프라이버시 정책 인식과 개인정보제공의도 간의 관계에 있어서 프라이버시 신뢰와 프라이버

시 위협의 매개효과를 검증하고 신뢰성향을 통해 프라이버시 정책에 대한 인식과 프라이버시 신뢰 간 관계의 조절효과를 검증하고자 한다.

3.1 프라이버시 정책의 인식

프라이버시 정책의 인식은 전자상거래 웹사이트를 이용한 경험을 바탕으로 프라이버시 정책을 평가한 개인의 인식이다. Li *et al.*(2011)에 따르면 프라이버시 정책 인식은 프라이버시 정책의 평가와 수집된 정보의 특성, 프라이버시에 대한 개인의 신념을 포함한다. Earp *et al.*(2005)에 따르면 조직이 개인의 프라이버시를 보호하기 위한 공정한 절차를 보여주면 조직에 대한 신뢰가 증가하며 사용자의 요구와 프라이버시 염려를 고려한 프라이버시 정책과 규정은 고객과의 약속을 의미한다고 보았다.

인터넷 사용자들은 전자상거래를 이용하기 전에 웹사이트로부터 조직의 신뢰를 보장하는 신호들(Signals)을 찾으며, 이 신호는 조직이 제공받은 개인정보를 어떻게 사용할 것인지 웹사이트 방문자에게 공지하는 프라이버시 정책이나 게시된 성명을 포함한다. 구조적 보장이나 보안은 웹 페이지에 승인 표시, 프라이버시 정책 등이 있으며 보증, 규정과 같은 안전망을 통해 특정 상황을 평가하고 신뢰에 긍정적인 영향을 미친다(Gefen *et al.*, 2003).



<그림 1> 연구모형

프라이버시 정책은 인터넷 사용자에게 개인정보 수집 및 사용 내역과 개인정보 손실이나 남용으로 부터 보호하는 내용을 알리며 고객이 정확한 정보를 유지하도록 개인정보를 수정할 수 있다는 사실을 고지한다(Li *et al.*, 2011). 고객은 회사의 개인정보 수집에 대해 고지를 받고 발언권을 가질 때 공정하다고 인지한다(Culnan and Bies, 2003).

프라이버시 정책은 개인정보의 공개와 이차적 사용에 대한 통제권을 개인에게 보장하는 의미를 가진다. 공정한 정보규정을 기반으로 한 프라이버시 정책을 실행함으로써 온라인 회사는 개인정보를 보호할 책임을 가진다. 이것은 정보수집 절차의 투명성을 증가시키고 웹사이트에서 제공하는 프라이버시 보호수준을 평가하도록 도와주므로 공정한 정보규정을 기반으로 한 프라이버시 정책의 실행은 프라이버시에 대한 신뢰를 높인다(Li *et al.*, 2011). 따라서 프라이버시 정책의 인식이 프라이버시 신뢰에 영향을 미친다는 것을 추론할 수 있으며 다음과 같은 가설을 설정하였다.

H1: 프라이버시 정책에 대한 인식은 프라이버시 신뢰에 정(+)¹의 영향을 미칠 것이다.

Lauer and Deng(2007)은 회사가 프라이버시 정책이 없이 개인정보를 다룬다면 회사의 직원이나 부서에 의해 개인정보가 부적절하게 사용될 위험에 직면한다고 설명하였다. 조직은 개인정보를 수집하고 이차적으로 정보를 취득하는 것에 대한 책임이 필요하며 프라이버시 정책을 통해 고객과의 약속을 이행함으로써 책임을 완수할 수 있다(Liu and Arnett, 2002). 그러므로 조직은 전자상거래를 이용하는 고객이 느끼는 프라이버시 위험을 완화하기 위해 프라이버시 정책을 채택한다.

온라인 거래에서 약속, 보증, 계약상의 보호는 낮은 곳에서 느끼는 고객의 인지된 위험을 완화한다(Luo *et al.*, 2010). 즉, 개인의 프라이버시를 보호하는 수단으로 규정된 프라이버시 정책에 대한 인식은 개인의 인지된 위험에 영향을 미칠 것

으로 가정하여 다음과 같은 가설을 설정하였다.

H2: 프라이버시 정책에 대한 인식은 프라이버시 위험에 부(-)²의 영향을 미칠 것이다.

3.2 프라이버시 신뢰

웹사이트와 인터넷 사용자 간 신뢰관계의 발전은 인터넷 사용자가 웹사이트에 개인정보를 공유하도록 촉진한다. Luo *et al.*(2010)의 연구에서 신뢰/위험 신념은 사람의 행동의도에 영향을 주는 주요 결정요인으로 보았다. 예를 들어 은행을 신뢰하는 태도를 가진 고객은 모바일 banking 사용에 대한 행동의도에 긍정적인 영향을 미친다고 설명하였다.

신뢰가 고객과 비즈니스 간에 필수적인 역할을 하는 이유는 고객 만족을 비롯하여 조직과 계속된 비즈니스를 이어가는 데 상당한 기여를 하기 때문이다(Mayer *et al.*, 1995). Dinev and Hart(2006)에 따르면 인터넷 활동을 하는 동안 신뢰와 인터넷 사용자의 개인정보 제공의도는 강한 정의 관계를 가진다. 웹사이트가 신뢰할 수 있고 안전한 환경이라고 믿는 신념은 정보를 안전하게 다룬다고 생각하므로 개인정보 제공의도를 증가시키기 때문이다. 따라서 전자상거래 웹사이트에서 개인정보가 올바르게 다루어질 것이라고 믿는 프라이버시 신뢰는 개인정보제공의도에 영향을 미친다고 추론하여 다음과 같은 가설을 설정하였다.

H3: 프라이버시 신뢰는 개인정보제공의도에 정(+)³의 영향을 미칠 것이다.

3.3 프라이버시 위험

인터넷 사용자는 온라인 활동을 하는 동안 개인의 프라이버시를 보호받지 못한다는 염려를 가지며 개인정보가 남용되거나 온라인 거래를 하는 동안 예상치 못한 문제에 직면하는 것을 두려워

한다. 이러한 두려움은 웹사이트에 정보를 제공하지 않거나 잘못된 정보를 제공하는 결과로 이어진다.

Jarvenpaa and Tractinsky(1999)에 따르면 위험 인식은 책을 구매하는 온라인 구매자의 행동의도를 감소시킨다는 실증적 증거를 제시하였다. Van Slyke *et al.*(2006)에 따르면 온라인 거래에서 개인정보는 공공의 컴퓨터 네트워크로 전해지며 종종 판매자의 온라인 서버에 저장되어 개인정보가 불법적으로 공개될 가능성이 있으므로 프라이버시 위험은 거래의도에 영향을 준다고 설명하였다. 인터넷 환경에 대한 불확실성은 전자상거래에 필요한 개인정보를 제공하는 것을 망설이게 하며 위험인식이 높으면 개인정보를 제공하지 않는다(Dinev and Hart, 2006). 반면에 프라이버시 정책을 통해 프라이버시 위험을 완화하는 것은 인터넷 사용자의 개인정보 제공여부를 결정하도록 도와준다(Wu *et al.*, 2012). 인지된 프라이버시 위험과 개인정보제공의도 관계에 대한 선행연구를 바탕으로 다음과 같은 가설을 설정하였다.

H4: 프라이버시 위험은 개인정보 제공의도에 부(-)의 영향을 미칠 것이다.

3.4 신뢰성향

신뢰성향은 다른 사람을 신뢰하는 태도를 의미하며 신뢰와 관련된 행동에 영향을 미친다고 연구되었다. 개인은 다른 사람을 신뢰함으로써 더 나은 결과를 성취할 것이라고 믿기 때문에 신뢰성향을 가진다(McKnight *et al.*, 2002). Chen and Barnes(2007)에 따르면 고객이 낮은 상황에서 불충분한 정보를 가질 때 다른 사람을 신뢰하는 그들의 상태가 각기 다르므로 신뢰성향은 신뢰형성에 필수적이라는 사실을 확인하였다. Lee and Turban(2001)에 의하면 신뢰성향이란 신뢰의 속성을 조절하는 개인의 특성이며 고객들은 얼마나 신뢰할 것인지 신뢰정도를 결정하기 위한 신호를

찾는다. 그리고 보안 인프라 구조와 개인의 신뢰 간 관계를 조절하는 실증적인 연구를 제시하였다. 그러므로 신뢰성향이 제도적 구조와 개인의 신뢰 간의 관계를 조절한다는 것을 추론하여 다음과 같은 가설을 설정하였다.

H5: 신뢰성향은 프라이버시 정책에 대한 인식과 프라이버시 신뢰의 관계를 강화(+시킬) 것이다.

IV. 실증분석

4.1 변수의 조작적 정의 및 측정항목

본 연구는 전자상거래 웹사이트의 프라이버시 정책에 대한 인식이 개인정보 제공의도에 미치는 영향을 연구하고자 하였으며, 프라이버시 신뢰와 위험의 매개효과와 신뢰성향의 조절효과를 실증적으로 검증하고자 하였다. 연구모형의 구성개념을 구체적으로 표현하고 변수의 값을 측정하기 위해 변수의 조작적 정의를 내렸다. 프라이버시 정책의 인식을 형성하는 요인은 공지, 접근, 선택, 보안, 시행으로 구분하여 측정항목을 개발하였다. 각 구성개념의 측정항목은 리커트 7점 척도로 구성하여 “매우 동의하지 않음”에서 “매우 동의함”으로 개인의 인식과 의도를 측정하였다. 본 연구의 조작적 정의와 측정항목은 <표 5>와 같다.

4.2 자료수집 및 분석

본 연구는 실증분석을 위한 본 설문을 실시하기에 앞서 부산지역의 대학생들을 대상으로 예비조사를 2회 실시하여 설문지를 배포하였다. 예비조사를 통해 설문지의 문제점을 확인하고 연구에 적합한 설문 문항으로 수정하였다. 본 설문조사는 전자상거래를 이용하는 학생 중 직장이 있는 특수대학원 학생들을 대상으로 실시하였다. 총 220부의 설문지 중 불성실한 응답(전체 항목을 동일하

〈표 5〉 조작적 정의

연구변수	조작적 정의	측정항목	연구자	
프라이버시 정책	공지	개인정보와 관련 정책을 명확히 고지한다고 생각함	Culnan and Williams (2009), Earp <i>et al.</i> (2005), Wu <i>et al.</i> (2012)	
		개인정보 수집 및 이용에 대해 고지한다고 생각함		
		개인정보를 취급하는 방침을 고지한다고 생각함		
		개인정보를 처리하는 방침을 고지한다고 생각함		
	접근	개인정보에 접근할 수 있다는 인식		수집된 개인정보에 접근할 수 있다고 생각함
				부정확한 정보에 대해 수정할 수 있다고 생각함
				기록된 개인정보를 삭제할 수 있다고 생각함
				수집된 나의 개인정보를 관리할 수 있다고 생각함
	선택	개인정보 요구 시 선택권을 주거나 동의를 구한다는 인식		개인정보 요구 시 나의 동의를 구한다고 생각함
				개인정보를 수집하기에 앞서 나의 동의를 구한다고 생각함
				개인정보를 이용하기에 앞서 나의 동의를 구한다고 생각함
				개인정보를 처리하기에 앞서 나의 동의를 구한다고 생각함
	보안	개인정보를 안전하게 다루는 시스템을 가진다는 인식		개인정보를 보호하는 보안기술을 사용한다고 생각함
				개인정보를 보호하는 암호화기술을 사용한다고 생각함
				개인정보를 확인하는 본인인증시스템을 사용한다고 생각함
				개인정보 접근을 관리하는 시스템을 사용한다고 생각함
	시행	개인정보와 관련된 법률이나 규정에 따라 개인정보를 다룬다는 인식		불법적인 침입을 탐지하는 시스템을 사용한다고 생각함
				개인정보를 보호하는 규정이 존재한다고 생각함
				개인정보보호정책을 위반하는 사람들을 처벌하는 규정이 있다고 생각함
				타인의 개인정보를 오·남용 할 경우 이를 처벌하는 규정이 있다고 생각함
프라이버시 신뢰	개인정보가 서비스 제공자에 의해 올바르게 다루어진다고 믿는 정도	타인의 개인정보를 도용할 경우 이를 처벌하는 규정이 있다고 생각함		
		개인정보와 관련된 법률에 따라 개인정보를 다룬다고 생각함		
		개인정보를 다룰 때 정직하게 행동할 것이라고 믿음		
		개인정보를 다룰 때 진실하게 행동할 것이라고 믿음		
프라이버시 위험	개인정보를 제공함으로써 외부적 환경에 의해 초래되는 잠재적 손실을 인지하는 정도	개인정보를 다룰 때 성실히 행할 것이라고 믿음		
		개인정보를 일관되게 다룰 것이라고 믿음		
		개인정보를 예측 가능하게 다룰 것이라고 믿음		
		개인정보를 제공하는 것은 위험하다고 생각함		
신뢰성향	다른 사람을 신뢰하는 정도	개인정보를 제공하는 것은 손실 가능성이 높다고 생각함		
		개인정보를 제공하는 것은 불확실성이 많다고 생각함		
		개인정보를 제공하는 것은 안전하지 못하다고 생각함		
		개인정보를 제공하는 것은 예상치 못한 문제들을 수반한다고 생각함		
개인정보 제공의도	웹사이트에 개인정보를 제공하고 자 하는 정도	나는 다른 사람을 신뢰한다고 생각함		
		나는 인간에 대한 신뢰를 가지고 있다고 생각함		
		나는 사람을 신뢰할 수 있다고 생각함		
		나는 내가 신뢰를 주면 상대방도 나를 신뢰할 것이라고 생각함		
개인정보 제공의도	웹사이트에 개인정보를 제공하고 자 하는 정도	나는 내가 신뢰를 주면 상대방도 나를 신뢰할 것이라고 생각함		
		개인정보를 기꺼이 제공할 것임		
		개인정보를 제공할 의향이 있음		
		개인정보를 흔쾌히 제공할 것임		
개인정보 제공의도	웹사이트에 개인정보를 제공하고 자 하는 정도	개인정보를 제공할 의도가 있음		
		개인정보 요구 시 제공할 의도가 있음		

게 응답하거나 중간 값으로 응답)이나 결측치를 포함하는 응답을 제외한 203부의 설문지를 최종 분석 데이터로 사용하였다. SPSS Statistics 21을 사용하여 기초적인 분석을 실시하였으며 연구모형을 분석하기 위한 분석 도구로 SmartPLS 2.0을 사용하였다.

설문대상의 전체 응답자 203명 중 남성이 111명(54.7%)으로 여성보다 비율이 높았으며, 나이

<표 6> 표본의 특성

변수	구분	빈도(명)	비율(%)
성별	남성	111	54.7
	여성	92	45.3
	계	203	100.0
나이	20~25세	14	6.9
	26~30세	27	13.3
	31~40세	56	27.6
	41~50세	77	37.9
	51세 이상	29	14.3
	계	203	100.0
직업	학생	23	11.3
	회사원	117	57.6
	교직원	11	5.4
	공무원	9	4.4
	자영업	16	7.9
	기타	27	13.3
	계	203	100.0
개인정보 수집 및 이용 방침 읽는 정도	읽지 않는다.	106	52.2
	가끔 읽는다.	87	42.9
	항상 읽는다.	10	4.9
	계	203	100.0
선택적 제공항목에 정보제공 정도	하지 않는다.	30	14.8
	가끔 한다.	81	39.9
	거의 매번 한다.	62	30.5
	매번 한다.	30	14.8
	계	203	100.0
프라이버시 침해경험	없다.	24	11.8
	소극적 경험	114	56.2
	적극적 경험	49	24.1
	주변인의 경험	16	7.9
	계	203	100.0

는 41~50세가 77명(37.9%)으로 가장 높았다. 직업은 회사원이 117명(57.6%)명으로 가장 높은 비율을 차지했으며, 개인정보 수집 및 이용 방침을 읽는 정도를 조사한 결과 읽지 않는다는 응답이 106명(52.2%)으로 가장 높았다. 선택적 제공항목에 정보를 제공하는 정도를 조사한 결과 가끔 한다는 응답이 81명(39.9%)으로 가장 높았으며 프라이버시 침해 경험에 대한 응답비율은 스패 전화, 문자와 같은 소극적 경험이 114명(56.2%)으로 가장 높았다. 표본의 특성은 <표 6>과 같다.

4.3 측정모형의 평가

4.3.1 1차 요인 분석

측정모형의 경로를 분석하기에 앞서 구성개념에 대한 변수의 신뢰성과 타당성을 평가하였다. 신뢰성과 집중 타당성을 평가하기 위해서 Cronbach's α 와 합성 신뢰도(CR; Composite Reliability), 표준 요인적재량(Factor Loading)과 평균분산추출(AVE; Average Variance Extracted)로 평가한다. 신뢰도와 집중 타당성은 Cronbach's α 와 합성 신뢰도 값이 0.7 이상, 구성개념과 각 항목 간의 관계 정도에 대한 지표인 요인적재량 값이 0.7 이상이며, 각 요인에 대한 평균분산추출 값이 0.5 이상으로 신뢰성과 타당성을 판단한다(Kim *et al.*, 2004). 또한 판별 타당성은 구성개념의 평균분산추출 제곱근이 구성개념들 간의 상관계수보다 크며 0.7 이상이어야 판별 타당성이 있다고 판단한다(김계수, 2013). 본 연구에서 1차 요인의 신뢰성과 집중 타당성을 평가한 결과는 <표 7>과 같다.

프라이버시 정책을 형성하는 공지, 접근, 선택, 보안, 시행의 측정변수와 프라이버시 신뢰, 프라이버시 위험, 신뢰성향, 개인정보 제공의도 측정변수의 신뢰성을 평가함에 따라 Cronbach's α 와 합성 신뢰도 값을 도출한 결과 권장수준 0.7 이상으로 나타났으며, 집중 타당성은 권장되는 기준 요인적재량인 0.7 이상, 평균분산추출 값이 0.5 이상으로 나타나 집중타당성이 있다고 판단된다. 1

〈표 7〉 1차 요인의 신뢰성과 집중 타당성 분석

잠재변수		측정변수	요인적재량	t값	AVE	CR	Cronbach's α
프라이버시 정책	공지	공지1	0.919	51.125	0.879	0.967	0.954
		공지2	0.924	51.533			
		공지3	0.950	84.605			
		공지4	0.957	114.753			
	접근	접근1	0.779	14.325	0.716	0.909	0.876
		접근2	0.784	15.797			
		접근3	0.895	51.049			
		접근4	0.918	67.012			
	선택	선택1	0.813	20.144	0.787	0.936	0.911
		선택2	0.870	24.213			
		선택3	0.937	94.307			
		선택4	0.921	78.033			
	보안	보안1	0.941	102.723	0.831	0.961	0.949
		보안2	0.942	90.962			
		보안3	0.892	51.607			
		보안4	0.925	68.149			
		보안5	0.856	31.338			
	시행	시행1	0.811	19.580	0.774	0.945	0.927
		시행2	0.905	47.520			
		시행3	0.904	48.733			
시행4		0.919	51.900				
시행5		0.856	36.134				
프라이버시 신뢰	신뢰1	0.924	63.672	0.871	0.971	0.963	
	신뢰2	0.949	84.588				
	신뢰3	0.948	124.347				
	신뢰4	0.931	74.614				
	신뢰5	0.915	64.681				
프라이버시 위협	위협1	0.935	82.044	0.878	0.973	0.965	
	위협2	0.944	117.011				
	위협3	0.923	55.018				
	위협4	0.943	84.250				
	위협5	0.940	81.317				
신뢰성향	성향1	0.920	35.156	0.841	0.955	0.937	
	성향2	0.960	64.963				
	성향3	0.943	52.153				
	성향4	0.842	17.401				
개인정보 제공의도	의도1	0.936	81.351	0.890	0.970	0.959	
	의도2	0.953	115.649				
	의도3	0.947	106.000				
	의도4	0.937	81.535				

〈표 8〉 1차 요인의 판별 타당성 분석

	공지	접근	선택	보안	시행	신뢰	위협	성향	의도
AVE 제공근	0.937	0.938	0.885	0.911	0.879	0.933	0.937	0.916	0.943
공지	1.000								
접근	0.490	1.000							
선택	0.510	0.502	1.000						
보안	0.514	0.434	0.513	1.000					
시행	0.479	0.407	0.403	0.538	1.000				
신뢰	0.415	0.445	0.532	0.580	0.552	1.000			
위협	-0.147	-0.283	-0.312	-0.313	-0.232	-0.477	1.000		
성향	0.330	0.203	0.183	0.192	0.345	0.217	-0.055	1.000	
의도	0.407	0.429	0.429	0.411	0.480	0.603	-0.409	0.418	1.000

〈표 9〉 2차 요인 형성지표의 다중공선성 분석

잠재변수	측정변수	가중치	t값	공차	VIF	상태지수
프라이버시 정책	공지	-0.137	1.152	0.582	1.717	8.577
	접근	0.173	1.530	0.657	1.521	9.554
	선택	0.384	3.046	0.592	1.690	10.214
	보안	0.462	3.966	0.571	1.751	11.099
	시행	0.358	2.963	0.647	1.546	11.635

차 요인의 판별 타당성 분석에 대한 결과는 <표 8>과 같으며 평균분산추출 제공근 값이 각 구성개념들 간의 상관관계수보다 크게 나타났으므로 판별 타당성이 있는 것을 확인하였다.

4.3.2 2차 요인의 다중공선성 분석

프라이버시 정책은 구성개념과 측정변수와의 관계를 형성지표로 설정하여 가중 값을 제시하였다. 형성지표의 측정변수들은 서로 독립적이고 낮은 상호 상관관계를 가지므로 구성개념의 내부 상관관계와 개념 간 상관관계에 대한 규칙이 존재하지 않기 때문에 반영지표에서 측정되는 내적 일관성에 대한 기준을 적용하지 않는다(김종기, 김상희, 2012).

일부 측정변수의 가중 값이 유의하지 않을 때 다중공선성 분석을 실시한다. 형성지표들 간의 높은 상관성이 있을 때 공선성이라고 부르며 2개 이상의 형성지표들이 포함될 경우 다중공선성

(Multicollinearity)이라고 한다. 이에 대한 판별은 공차 값이 0.1보다 작고 VIF값이 10보다 크며 상태지수가 30을 초과하면 측정변수들 간에 다중공선성이 있다고 본다(Chin, 1998). 본 연구에서 다중공선성 분석을 실시한 결과는 <표 9>와 같으며 공지, 접근, 선택, 보안, 시행에 대한 공차 값이 0.1보다 크며 VIF값이 10보다 작고, 상태지수가 30을 넘지 않았기 때문에 다중공선성에 문제가 없다고 판단하여 신뢰성이 있는 것을 확인하였다.

4.4 구조모형의 평가

구조모형의 적합도는 중복성(Redundancy)과 잠재변수의 R²값, 전체 적합도(Goodness of Fit)로 평가한다. 중복 값이 양수이고, 잠재변수의 R²값이 0.26 이상이면 적합도를 ‘상’으로, 0.13 이상 0.26 미만이면 ‘중’, 0.02 이상 0.13 미만이면 ‘하’

로 평가한다(Cohen, 1988). 공통성(Communality)은 표준화된 측정항목의 요인 적재치를 제공하여 합한 것으로 한 항목에서 얼마나 많은 분산이 공통요인들에 의해 설명되는지 나타내며 항목으로부터 추출된 분산으로 표현한다. <표 10>과 같이 본 연구의 공통성은 0.5 이상의 값을 나타내며 유의하다는 것을 확인하였다. 또한 연구 모형의 전체 적합도는 0.511로 높다고 판단된다.

<표 10> 모형의 적합도 분석

변수	R ²	중복성	공통성
프라이버시 정책	-	-	0.526
프라이버시 신뢰	0.475	0.008	0.871
프라이버시 위험	0.132	0.115	0.878
개인정보제공의도	0.383	0.091	0.890
평균값	0.330	0.071	0.791
모형 적합도	$\sqrt{0.330 \times 0.791} = 0.511$		

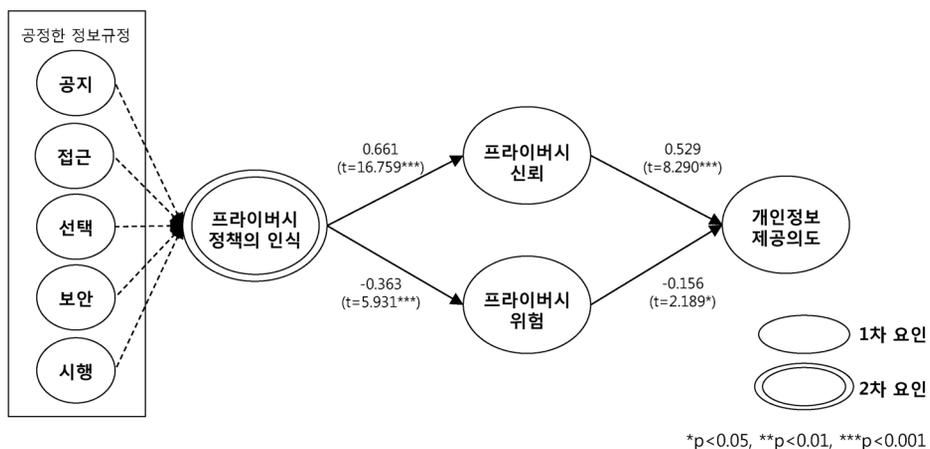
4.5 연구 가설 검증

본 연구모형의 독립변수와 매개변수, 종속변수 간의 관계를 분석하기 위해 구조방정식을 실시하였다. 앞서 연구한 측정모형의 신뢰성, 타당성, 적합도에 대한 검증을 바탕으로 전체 연구모형의 구

성개념 간의 관계를 추정하였다. 본 연구에 제시된 연구모형을 분석한 결과는 <그림 2>와 같다.

프라이버시 정책의 인식과 프라이버시 신뢰 간의 경로계수가 0.661, t값이 16.759로 유의수준 0.001에서 통계적으로 유의한 영향을 미치는 것으로 나타나 H1은 채택되었다. 프라이버시 정책에 대한 인식의 정도에 따라 개인의 프라이버시 신뢰에 영향을 미친다는 것을 확인하였다. 전자상거래가 나의 개인정보를 이용하기에 앞서 수집에 대한 동의나 처리방침 고지, 전자상거래의 보안 시스템, 법적인 규정에 대한 인식의 정도가 높을수록 전자상거래가 나의 개인정보를 안전하게 다룰 것이라는 믿음에 긍정적인 영향을 미친다고 볼 수 있다.

또한 프라이버시 정책의 인식과 프라이버시 위험 간의 경로계수가 -0.363, t값이 5.931로 유의수준 0.001에서 유의한 영향을 미치는 것으로 나타나 H2가 채택되었다. 프라이버시 신뢰가 전자상거래에 개인정보를 제공하는 의도에 긍정적인 영향을 미치는 것을 확인하였다. 전자상거래가 나의 개인정보를 다루는 것에 대한 신뢰가 높을수록 전자상거래는 안전하고 믿을 수 있는 환경이라고 인식함으로써 개인정보제공의도가 높아진다고 볼 수 있다.



<그림 2> 연구모형 분석결과

〈표 11〉 가설검정 결과

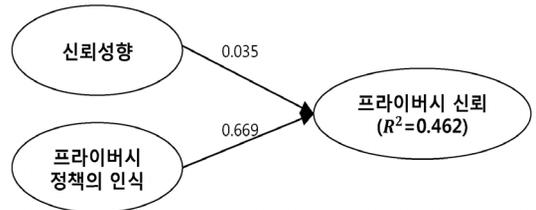
가설	경로	경로계수	t값	통계적 검정	채택여부
H1(+)	정책 → 신뢰	0.661	16.759	유의수준 $\alpha = 0.001$ 에서 유의함	채택
H2(-)	정책 → 위험	-0.363	5.931	유의수준 $\alpha = 0.001$ 에서 유의함	채택
H3(+)	신뢰 → 의도	0.529	8.290	유의수준 $\alpha = 0.001$ 에서 유의함	채택
H4(-)	위험 → 의도	-0.156	2.189	유의수준 $\alpha = 0.05$ 에서 유의함	채택

프라이버시 신뢰와 개인정보 제공의도 간의 경로계수가 0.529, t값이 8.290으로 유의수준 0.001에서 통계적으로 유의한 결과를 확인하여 H3이 채택되었다. 프라이버시 정책에 대한 인식이 낮을수록 프라이버시에 대한 위험이 증가하는 것을 확인하였다. 최근 마스크를 통해 전자상거래를 비롯한 다양한 개인정보 유출 문제의 영향을 받아 전자상거래 환경에 대한 불안과 염려가 반영된 결과로 해석할 수 있다.

프라이버시 위험과 개인정보 제공의도 간의 경로계수는 -0.156, t값은 2.189로 유의수준 0.05에서 유의한 결과를 확인하여 H4가 채택되었다. 프라이버시 위험이 전자상거래에 개인정보를 제공하는 의도에 부정적인 영향을 미치는 것을 확인하였다. 전자상거래에 개인정보를 제공함으로써 잠재적 손실을 초래할 수 있다는 인식은 전자상거래는 위험하며 안전하지 못한 환경으로 판단하여 개인정보를 제공하고자 하는 의도를 감소시키는 것으로 판단된다. 가설검정의 결과는 <표 11>에 제시하였다.

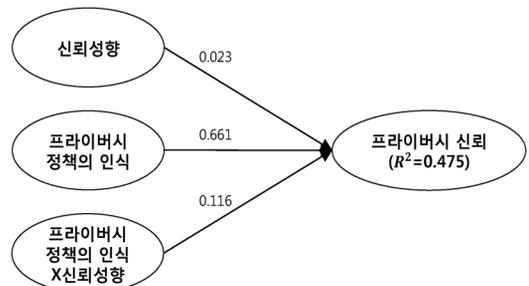
4.6 조절효과 분석

본 연구에서 프라이버시 정책의 인식과 프라이버시 신뢰의 관계에 있어서 신뢰성향의 조절효과를 유무를 확인하기 위해 Cohen(1988)이 제시한 효과크기를 사용하였다. Cohen(1988)의 효과크기 공식에 값을 대입하여 상호작용의 효과크기를 계산한 결과, 0.02에서 0.15의 값은 작은 효과크기를 나타내며 0.15에서 0.35의 값은 중간 효과크기, 0.35 이상은 큰 효과크기를 나타낸다.



〈그림 3〉 주 효과 모델 경로분석 결과

주 효과 모델의 경로를 분석한 결과는 <그림 3>과 같다. 프라이버시 신뢰에 대한 R²값은 0.462로 나타났으며 신뢰성향과 프라이버시 신뢰의 경로계수는 0.035, 프라이버시 정책의 인식과 프라이버시 신뢰의 경로계수는 0.669로 나타났다.



〈그림 4〉 상호작용 모델 경로분석 결과

상호작용 변수를 포함하는 조절효과를 분석한 결과는 <그림 4>와 같다. 프라이버시 신뢰의 R²값은 0.475로 나타났으며 신뢰성향과 프라이버시 신뢰의 경로계수는 0.023, 프라이버시 정책의 인식과 프라이버시 신뢰의 경로계수는 0.661, 프라이버시 정책의 인식과 신뢰성향의 상호작용 변수와 프라이버시 신뢰의 경로계수는 0.116으로 나타났다.

이는 신뢰성향이 프라이버시 정책에 0.023의 영향을 미치고 신뢰성향에 의해 프라이버시 정책인식의 경로계수는 0.661에서 프라이버시 정책인식과 신뢰성향 상호작용 변수의 경로계수인 0.116이 더해져 0.777까지 증가할 수 있다. 상호작용의 효과 크기를 계산한 결과 0.025의 값이 나와 작은 효과 크기가 있다고 판단된다.

그러나 본 논문에서 적용한 Cohen(1988)의 효과 크기는 조절효과의 유무에 대한 평가만 가능하며 가설이 유의한지에 대한 평가는 어렵다. 그러므로 F값 공식에 값을 대입하여 F값을 산출하고 그 값을 F분포표에 비교한 후 가설이 유의한지 평가하여 조절효과를 확인하였다. F값 공식은 식 (1)과 같다.

$$F_{(k_2 - k_1, n - k_2 - 1)} = \frac{(R_{Included}^2 - R_{Excluded}^2) / (k_2 - k_1)}{(1 - R_{Included}^2) / (n - k_2 - 1)} \quad (1)$$

$R^2_{Included}$ 는 상호작용 변수를 포함하는 모형의 R^2 를 의미하며 $R^2_{Excluded}$ 는 상호작용 변수를 포함하지 않는 모형의 R^2 를 의미한다. n은 표본의 개수를 말하며 k_2 는 독립변수와 종속변수, 상호작용 변수를 포함하는 변수의 개수, k_1 은 상호작용 변수를 포함하지 않는 변수의 개수를 말한다. 식 (1)의 공식에 값을 대입한 결과 F값은 4.903으로 나타났으며 F분포표를 비교해본 결과 유의수준 $\alpha = 0.05$ 에서 유의한 결과를 얻었으며 결과는 <표 12>과 같다.

<표 12> 조절효과 분석결과

	$R^2_{Included}$	$R^2_{Excluded}$	F값
신뢰성향	0.475	0.462	4.903

신뢰성향이 신뢰의 조절변수로 사용된 선행연구에 따르면 조절효과가 있다고 설명한다. 그러나 최근 일부 연구에서 온라인 환경이 변화하였고, 온라인 쇼핑에 대한 경험이 있을수록 신뢰성향은

더 이상 신뢰에 있어서 중요한 요인이 아니라고 설명한다(Jiang et al., 2008). 그러므로 본 연구에서 전자상거래 경험이 있는 사용자를 바탕으로 신뢰성향이 신뢰에 어떠한 영향을 미치는지 실증적으로 검증하고자 하였고, 연구결과 개인의 신뢰성향은 프라이버시 정책에 대한 인식과 서비스 제공자의 신뢰 관계를 강화시키는 역할을 한다는 것을 확인하였다. 그러므로 향후 신뢰연구에 있어서 개인의 성향이 중요한 요인으로 고려해야 한다는 점을 시사한다.

V. 결론

본 연구는 전자상거래의 프라이버시 정책 인식이 개인정보 제공의도에 미치는 영향을 살펴보고자 하였다. 전자상거래를 이용하면서 프라이버시 정책을 평가한 개인의 인식을 기반으로 프라이버시 신뢰와 프라이버시 위험 간의 관계를 규명하며, 인터넷 사용자는 전자상거래와 같은 불확실한 환경에서 신뢰성향에 의존한다는 선행연구를 바탕으로 프라이버시 정책 인식과 프라이버시 신뢰 관계의 조절효과를 확인하고자 모형을 설정하였다. 연구모형은 SmartPLS 2.0을 사용하여 실증적으로 분석하였다.

개인의 프라이버시 정책 인식을 2차 요인으로 설정하고 공지, 접근, 선택, 보안, 시행 측면에서 평가하는 지표를 생성하여 연구모형을 분석하였다. 또한 신뢰-위험 모델의 주요 요인을 프라이버시 신뢰와 프라이버시 위험으로 설정하여 개인의 프라이버시 관점에서 설명하고자 하였다.

본 연구의 분석 결과를 요약해보면 다섯 가지 가설 모두 채택되었다. 첫째, 프라이버시 정책의 인식을 평가하는 정도에 따라 웹사이트의 개인정보 사용에 대한 인지된 프라이버시 신뢰에 유의한 영향을 미친다는 사실을 확인하였다. 인터넷 사용자는 프라이버시 정책과 같은 제도적 신호를 기반으로 웹사이트의 정보 투명성을 평가할 수 있으며 개인의 신뢰형성에 영향을 미친다. 따라

서 전자상거래에서 프라이버시 정책을 높게 평가할수록 온라인 환경에 대한 제도적 신뢰가 형성되며 이를 통해 서비스 제공자가 개인정보가 올바르게 다룰 것이라는 프라이버시 신뢰가 높아진다. 반면에 정책에 대해 낮게 평가할수록 웹사이트가 개인정보를 원만히 다루지 못한다는 인식을 가지므로써 프라이버시 신뢰가 낮아진다. 이러한 결과는 정보가 상대적으로 부족한 거래수단에 대해 신뢰가 전반적으로 낮거나, 최근 개인정보유출이나 남용과 같은 문제가 부상함으로써 영향을 받은 결과라고 판단된다.

둘째, 전자상거래 웹사이트의 프라이버시 정책 인식을 평가하는 정도에 따라 인지된 위협에 유의한 영향을 미친다는 사실을 확인하였다. 프라이버시 정책의 인식이 높을수록 전자상거래 웹사이트에 개인정보를 제공함으로써 초래되는 위협을 인지하는 수준이 낮아진다. 프라이버시 정책은 웹사이트와 인터넷 사용자 간의 거래를 보장하는 규정으로서 개인정보가 프라이버시 정책에 따라 관리된다고 평가할수록 외부적인 위협으로부터의 위협에 대한 인식을 완화시킬 수 있다. 그러나 프라이버시 정책의 인식이 낮은 경우, 웹사이트에 개인정보를 제공함으로써 초래되는 부정적 결과에 대한 불안이 증폭되며, 프라이버시와 관련된 개인정보 유출이나 개인정보 오·남용과 같은 예상치 못한 문제를 수반할 것으로 생각하므로 인지된 프라이버시 위협이 높아지게 된다.

셋째, 프라이버시 신뢰는 전자상거래 웹사이트에 개인정보를 제공하고자 하는 의도에 유의한 영향을 미친다는 사실을 확인하였다. 웹사이트가 신뢰할 수 있는 환경이며 서비스 제공자가 개인정보를 안전하게 관리할 것이라는 신념이 성립되면 본인이 원하는 정보나 서비스를 받기 위해 개인정보를 제공하고자 하는 의도가 증가하는 것으로 나타났다.

넷째, 프라이버시 위협은 전자상거래 웹사이트에 개인정보를 제공하고자 하는 의도에 유의한 영향을 미친다는 사실을 확인하였다. 개인의 인

지된 위협인식은 행동의도에 영향을 준다. 특히 전자상거래 웹사이트에 제공된 정보는 공용 네트워크로 전송되고 판매자의 온라인 서버에 기록된다는 인식은 개인정보와 관련된 우려를 증가시킴으로써 잘못된 개인정보를 제공하거나 개인정보를 제공하지 않는 결과를 초래한다. 그러므로 인지된 위협이 높을수록 개인정보를 제공하고자 하는 의도가 낮아지는 것으로 나타났다.

다섯 째, 신뢰성향이 프라이버시 정책에 대한 인식과 프라이버시 신뢰의 정의 관계를 강화시키는 가설에 대해 유의수준 $\alpha = 0.05$ 에서 유의하다는 결과를 얻었다. 사람들은 직접 제품을 보고 만지는 일반적인 쇼핑방법과 달리 정보가 부족한 전자상거래 환경에서 신뢰성향에 의존하는 경향이 있다. 다른 사람을 신뢰하는 성향은 낮은 판매자나 새로운 환경에 영향을 미친다는 기존 연구를 기반으로 신뢰성향의 조절효과를 확인하였다. 일반적으로 신뢰성향이 높은 사람은 낮은 환경에도 불구하고 서비스 제공자를 신뢰할수록 더 나은 결과를 얻는다고 믿기 때문에 프라이버시 정책을 높게 평가할수록 개인정보가 올바르게 사용될 것이라는 인지된 프라이버시 신뢰와의 관계를 강화시킨다.

본 연구를 통해서 개인의 프라이버시 정책을 평가하는 정도에 따라 인지된 프라이버시 신념에 영향을 준다는 것을 알 수 있었다. 전자상거래 웹사이트는 프라이버시 정책을 형성하는 공지, 접근, 선택, 보안, 시행의 요소들을 더 보완하고 체계적으로 관리하여 인터넷 사용자가 개인정보를 보호받는다라는 인식이 향상되도록 노력할 필요가 있다. 인터넷 사용자의 개인정보 수집 및 사용내역에 관련된 공지 인식을 높이기 위해서 고지 내용이 다소 길고 복잡하여 읽기 힘든 부분을 보완할 필요가 있으며, 지속적인 보안 프로그램의 개발과 프라이버시 실 등을 게시함으로써 프라이버시 신뢰를 증가시키고 위협을 완화하는 방법을 꾸준히 모색해야 한다.

이전의 정보시스템 연구에서 프라이버시 정책

에 대한 중요성을 강조하거나 프라이버시의 위협을 낮추는 요인으로 프라이버시 정책을 언급하는 연구가 많다. 본 연구에서는 프라이버시 정책 인식을 공지, 접근, 선택, 보안, 시행으로 구분하여 실증적으로 분석했다는 점에서 의의가 있다. 또한 신뢰-위험 모델의 포괄적인 개념을 프라이버시 관점으로 접근하여 연구의 목적을 명확히 하였다.

본 연구에서 프라이버시 정책에 대한 인식을 공지, 접근, 선택, 보안, 시행으로 구분하여 측정하였다. 그러나 정책에 대한 인식을 더 세분화시키고 다양한 측면으로 개인의 인식을 측정한다면 향상된 연구가 될 수 있을 것이다. 직장이 있는 특수대학원생들을 대상으로 설문조사를 실시하였으나 표본의 대표성에 있어서 일반화시키는 데 다소 문제가 있을 수 있다. 그러므로 다양한 연령층을 설문대상으로 광범위한 표본을 통해 포괄적인 연구를 수행할 필요가 있다.

본 연구에서는 개인의 행동의도에 대한 연구를 실시하였으나 최근 정보시스템의 프라이버시 연구 분야에서는 행동의도와 실제 행동 간의 차이를 설명하는 프라이버시 역설에 대한 연구의 중요성을 언급하고 있다. 실제로 전자상거래에서 프라이버시 역설이 존재하며 진일보된 연구를 위해 개인의 태도와 행동의 관계를 규명하는 연구를 진행한다면 향후 연구에 더 큰 기여가 될 것이라 예상된다.

참 고 문 헌

- [1] 김계수, *SmartPLS 이용 쉬운 구조방정식모델* 청람, 2013.
- [2] 김종기, 김상희, “스마트폰 위치기반서비스에서 정보제공의도: 프라이버시 계산 관점을 중심으로”, *정보시스템연구*, 제21권, 제4호, 2012, pp. 55-79.
- [3] 민진영, 김병수, “프라이버시 계산 모형을 적용한 SNS 지속 사용 의도에 대한 연구: 페이스북과 카카오톡 사례 중심으로”, *Information Systems Review*, 제15권, 제1호, 2013, pp. 105-122.
- [4] 박경신, “사생활의 비밀의 절차적 보호규범으로서의 개인정보보호법리”, *공법연구*, 제40권, 제1호, 2011, pp. 129-162.
- [5] 최보미, 박민정, 채상미, “개인정보보호 기술 수용행동에 영향을 미치는 요인에 대한 연구”, *Information Systems Review*, 제17권, 제3호, 2015, pp. 77-94.
- [6] Altman, I., *The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding*, Books/Cole Publishing, Montrey, CA, 1975.
- [7] Awad, N. F. and M. S. Krishnan, “The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online for personalization”, *MIS Quarterly*, Vol.30, No.1, 2006, pp. 13-28.
- [8] Bansal, G., F. M. Zahedi, and D. Gefen, “Do context and personality matter? Trust and privacy concerns in disclosing private information online”, *Information & Management*, Vol.53, No.1, 2016, pp. 1-21.
- [9] Belanger, F. and R. E. Crossler, “Privacy in the digital age: A review of information privacy research in information systems”, *MIS Quarterly*, Vol.35, No.4, 2011, pp. 1017-1041.
- [10] Chen, Y. H. and S. Barnes, “Initial trust and online buyer behaviour”, *Industrial Management & Data Systems*, Vol.107, No.1, 2007, pp. 21-36.
- [11] Chin, W. W., “The partial least squares approach to structural equation modeling”, in G.A. Marcoulides (ed.), *Modern Methods for Business Research*, Lawrence Erlbaum Associates, New Jersey, 1998, pp. 195-336.
- [12] Choi, B. C., Z. Jiang, B. Xiao, and S. S. Kim, “Embarrassing exposures in online social networks: An integrated perspective of privacy invasion and relationship bonding”, *Information*

- Systems Research*, Vol.26, No.4, 2015, pp. 675-694.
- [13] Clarke, R., "Internet privacy concerns confirm the case for intervention", *Communications of the ACM*, Vol.42, No.2, 1999, pp. 60-67.
- [14] Cohen, J. O., *Statistical Power Analysis for the Behavioral Science* (2nd ed.), Hillsdale, New Jersey, Lawrence Erlbaum Associates, 1988.
- [15] Culnan, M. J. and R. J. Bies, "Consumer privacy: Balancing economic and justice considerations", *Journal of Social Issues*, Vol.59, No.2, 2003, pp. 323-342.
- [16] Culnan, M. J. and C. C. Williams, "How ethics can enhance organizational privacy: Lessons from the choicepoint and TJX data breaches", *MIS Quarterly*, Vol.33, No.4, 2009, pp. 673-687.
- [17] Culnan, M. J., "How did they get my name?: An Exploratory investigation of consumer attitudes toward secondary information use", *MIS Quarterly*, Vol.17, No.3, 1993, pp. 341-363.
- [18] Dinev, T. and P. Hart, "An extended privacy calculus model for e-commerce transactions", *Information Systems Research*, Vol.17, No.1, 2006, pp. 61-80.
- [19] Earp, J. B., A. Anton, L. Aiman-Smith, and W. H. Stufflebeam, "Examining internet privacy policies within the context of user privacy values", *Engineering Management IEEE Transactions on*, Vol.52, No.2, 2005, pp. 227-237.
- [20] Gefen, D., "E-Commerce: The role of familiarity and trust", *Omega*, Vol.28, No.5, 2000, pp. 725-737.
- [21] Gefen, D., E. Karahanna, and D. W. Straub, "Trust and TAM in online shopping: An integrated model", *MIS Quarterly*, Vol.27, No.1, 2003, pp. 51-90.
- [22] Jarvenpaa, S. L. and N. Tractinsky, "Consumer trust in an internet store: A cross-cultural validation", *Journal of Computer-Mediated Communication*, Vol.5, No.2, 1999, pp. 1-35.
- [23] Jiang, J. C., C. A. Chen, and C. C. Wang, "Knowledge and trust in e-consumers' online shopping behavior", in *Electronic Commerce and Security, 2008 International Symposium on IEEE*, 2008, pp. 652-656.
- [24] Joubert, J. and J. Van Belle, "The role of trust and risk in mobile commerce adoption within south africa", *International Journal of Business, Humanities and Technology*, Vol.3, No.2, 2013, pp. 27-38.
- [25] Kim, D. J., D. L. Ferrin, and H. R. Rao, "A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents", *Decision Support Systems*, Vol.44, No.2, 2008, pp. 544-564.
- [26] Kim, H. W., Y. Xu, and J. Koh, "A comparison of online trust building factors between potential customers and repeat customers", *Journal of the Association for Information Systems*, Vol.5, No.10, 2004, pp. 392-420.
- [27] Kumar, N., K. Mohan, and R. Holowczak, "Locking the door but leaving the computer vulnerable: Factors inhibiting home users' adoption of software firewalls", *Decision Support Systems*, Vol.46, No.1, 2008, pp. 254-264.
- [28] Lauer, T. W. and X. Deng, "Building online trust through privacy practices", *International Journal of Information Security*, Vol.6, No.5, 2007, pp. 323-331.
- [29] Lee, M. K. and E. Turban, "A trust model for consumer internet shopping", *International Journal of Electronic Commerce*, Vol.6, No.1, 2001, pp. 75-91.
- [30] Li, H., R. Sarathy, and H. Xu, "The role of affect and cognition on online consumers' decision to disclose personal information to unfamiliar online vendors", *Decision Support Systems*, Vol.41,

- No.3, 2011, pp. 434-445.
- [31] Li, H., R. Sarathy, and H. Xu, "Understanding situational online information disclosure as a privacy calculus", *Journal of Computer Information Systems*, Vol.51, No.1, 2010, pp. 62-71.
- [32] Li, Y., "A multi-level model of individual information privacy beliefs", *Electronic Commerce Research and Applications*, Vol.13, No.1, 2014, pp. 32-44.
- [33] Li, Y., "Theories in online information privacy research: A critical review and integrated framework", *Decision Support Systems*, Vol.54, No.1, 2012, pp. 471-481.
- [34] Liao, C., C. C. Liu, and K. Chen, "Examining the impact of privacy, trust, and risk perceptions beyond monetary transactions: An integrated model", *Electronic Commerce Research and Applications*, Vol.10, No.6, 2011, pp. 702-715.
- [35] Liu, C. and K. P. Arnett, "An examination of privacy policies in fortune 500 web sites", *American Journal of Business*, Vol.17, No.1, 2002, pp. 13-22.
- [36] Liu, C., J. T. Marchewka, J. Lu, and C. Yu, "Beyond concern-a privacy-trust-behavioral intention model of electronic commerce", *Information & Management*, Vol.42, No.2, 2005, pp. 289-304.
- [37] Luo, X., H. Li, J. Zhang, and J. P. Shim, "Examining multi-dimensional trust and multi-faceted risk in initial acceptance of emerging technologies: An empirical study of mobile banking services", *Decision Support Systems*, Vol.49, No.2, 2010, pp. 222-234.
- [38] Malhotra, N. K., S. S. Kim, and J. Agarwal, "Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model", *Information Systems Research*, Vol.15, No.4, 2004, pp. 336-355.
- [39] Mayer, R. C., J. H. Davis, and F. D. Schoorman, "An integrative model of organizational trust", *Academy of Management Review*, Vol.20, No.3, 1995, pp. 709-734.
- [40] McKnight, D. H. and N. L. Chervany, "What trust means in e-commerce customer relationships: And interdisciplinary conceptual typology", *International Journal of Electronic Commerce*, Vol.6, No.2, 2002, pp. 35-59.
- [41] McKnight, D. H., V. Choudhury, and C. Kacmar, "Developing and validating trust measures for e-commerce: An integrative typology", *Information Systems Research*, Vol.13, No.3, 2002, pp. 334-359.
- [42] OECD, *OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, 2013, Available: <http://www.oecd.org>.
- [43] Osatuyi, B., "Personal traits and information privacy concern on social media platforms", *Journal of Computer Information Systems*, Vol.55, No.4, 2015, pp. 11-19.
- [44] Scoeman, F. D., *Philosophical Dimensions of Privacy: An Anthology*, Cambridge University Press, Cambridge, UK, 1984.
- [45] Smith, H. J., T. Dinev, and H. Xu, "Information Privacy Research: An Interdisciplinary Review", *MIS Quarterly*, Vol.35, No.4, 2011, pp. 989-1015.
- [46] Solove, D. J., "A taxonomy of privacy", *University of Pennsylvania Law Review*, Vol.154, No.3, 2006, pp. 477-564.
- [47] Van Slyke, C., J. T. Shim, R. Johnson, and J. J. Jiang, "Concern for information privacy and online consumer purchasing", *Journal of the Association for Information Systems*, Vol.7, No.1, 2006, pp. 415-444.
- [48] Warren, S. D. and D. L. Brandeis, "The right to privacy", *Harvard Law Review*, Vol.4, No.5, 1890, pp. 193-220.

- [49] Weinstein, W. L., *The Private and the Free: A Conceptual Inquiry*, Privacy: Nomos XIII, 1971, pp. 624-692.
- [50] Westin, A. F., "Social and political dimensions of privacy", *Journal of Social Issue*, Vol.59, No.2, 2003, pp. 431-453.
- [51] Wu, K. W., S. Y. Huang, D. C. Yen, and I. Popova, "The effect of online privacy policy on consumer privacy concern and trust", *Computers in Human Behavior*, Vol.28, No.3, 2012, pp. 889-897.
- [52] Xu, H., T. Dinev, H. J. Smith, and P. Hart, "Examining the formation of individual's privacy concerns: Toward an integrative view", *ICIS 2008 Proceedings*, 2008, pp. 1-16.
- [53] Xu, H., T. Dinev, J. Smith, and P. Hart, "Information privacy concerns: Linking individual perceptions with institutional privacy assurances", *Journal of the Association for Information Systems*, Vol.12, No.12, 2011, pp. 798-824.
- [54] Xu, H., H. H. Teo, B. C. Tan, and R. Agarwal, "Research note-effects of individual self-protection, industry self-regulation, and government regulation on privacy concerns: A study of location-based services", *Information Systems Research*, Vol.23, No.4, 2012, pp. 1342-1363.
- [55] Yang, M. H., B. Lin, N. Chandlrees, and H. Y. Chao, "The effect of perceived ethical performance on shopping websites on consumer trust", *Journal of Computer Information Systems*, Vol.50, No.1, 2009, pp. 15-24.
- [56] Zhao, L., Y. Lu, and S. Gupta, "Disclosure intention of location-related information in location-based social network service", *International Journal of Electronic Commerce*, Vol.16, No.4, 2012, pp. 53-89.

The Effect of Privacy Policy Awareness on the Willingness to Provide Personal Information in Electronic Commerce

Jongki Kim* · Dawoon Oh**

Abstract

This study investigated the relationship between privacy policy awareness and willingness to provide personal information. Online privacy policies published on the Internet aim to build the trust of consumers and reduce their concerns about the provision of providing personal information.

This study uses FIP(FIP; Fair Information Practices) principles to measure awareness of privacy policy. The result of the survey indicates significant relationships among awareness of privacy policy of e-commerce websites, privacy trust, and privacy risk. Privacy policy aims to improve transparency of collection and use of personal information. A high level of privacy trust is related to a high level of willingness to provide personal information on an e-commerce website. A low level of privacy risk is related to a high level of willingness to provide personal information on an e-commerce website.

This study found that disposition to trust moderates the relationship between privacy policy awareness and privacy trust. This study contributes to further research on the relationships among privacy policy awareness, privacy trust, and privacy risk. The result of this study can be used by companies that aim to build privacy trust and reduce privacy risk.

Keywords: *Information Privacy, Privacy Policy, Fair Information Practices, E-Commerce, Privacy Trust, Privacy Risk*

* Professor, Dept. of Business Administration, Pusan National University

** Corresponding Author, Graduate Student, Dept. of Business Administration, Pusan National University

◎ 저 자 소 개 ◎



김 종 기 (jkkim1@pusan.ac.kr)

부산대학교 경영학과에서 학사를 마쳤으며, 미국 Arkansas State University에서 경영학 석사학위, Mississippi State University에서 경영학 박사학위를 취득하였다. 현재 부산대학교에서 경영학과 교수로 재직 중이며, 주요 관심분야는 정보보안관리, 프라이버시, 전자상거래, 기술경영 등이다.



오 다 운 (odw@pusan.ac.kr)

부산대학교 경영학과 경영정보전공 석사학위를 취득하였으며, 현재 동대학원 박사과정 재학 중이다. 주요 연구 관심분야는 개인정보보호, 프라이버시, 전자상거래, 보안 등이다.

논문접수일 : 2016년 02월 23일

1차 수정일 : 2016년 05월 25일

게재확정일 : 2016년 09월 13일

2차 수정일 : 2016년 09월 06일