「정보시스템연구」 제26권 제1호
한국정보시스템학회
2017년 3월, pp. 93～123

http://dx.doi.org/10.5859/KAIS.2017.26.1.93

개인정보 제공에 대한 인터넷 사용자의 경제적 행동에 관한 연구: Privacy Calculus, CPM 이론을 중심으로*

김 진 성** · 김 종 기***

〈목 차〉

Ⅰ. 연구의 필요성 및 목적
Ⅱ. 이론적 배경
2.1 이중 프로세스 이론
2.2 커뮤니케이션 프라이버시 관리 이론
2.3 프라이버시 계산 이론
Ⅲ. 연구모형 및 연구가설
3.1 연구모형
3.2 연구가설
Ⅳ. 연구방법
4.1 자료의 특성 및 분석 방법
Ⅴ. 연구결과
5.1 측정모형에 대한 신뢰성 분석
5.2 측정모형에 대한 타당성 분석
5.3 연구모형에 대한 평가
5.4 연구가설 검정
Ⅵ. 연구결론
6.1 연구결론
6.2 연구 시사점 및 한계점
참고문헌
<Abstract>

Ⅰ. 연구의 필요성 및 목적

전자상거래를 이용한 방식이 PC를 활용한 온라인 방식에서 스마트폰을 활용한 모바일 방식으로 확대되면서 전자상거래 시장 규모는 꾸준한 성장세를 보이고 있다. 통계청의 “2016년 8월 온라인쇼핑 동향” 보도자료에 따르면 온라인쇼핑 거래액(5조5,757억원)에서 모바일쇼핑 거래액(3조323억원)이 차지하는 비중이 54.4%로 지난 해 2015년 52.6%(2조278억원), 2014년 34.1%(1조3,254억원)와 비교해 볼 때 지속적인 증가 추세임을 알 수 있다.

이는 전자상거래 산업이 인터넷 은행(K뱅크, 카카오뱅크), 모바일 결제(삼성페이, 네이버페이, 카카오페이), O2O(online to offline)와 같은 금융 산업과 융합되어 가는 현상 속에서 더욱 가시화되어 가고 있다. 이처럼 전자상거래 시장이 보다 글로벌화 되어가고 다양한 분야로 융

* 이 논문은 2016년 대한민국 교육부와 한국연구재단의 지원을 받아 수행된 연구임 (NRF-2016S1A5B5A07921030)
** 부산대학교 경영연구소 전임연구원, kimsam@pusan.ac.kr(주저자)
*** 부산대학교 경영학과 교수, jkkim1@pusan.ac.kr(공동저자)

합·확대되면서 여러 국가에서 수집된 개인정보 이용 및 보호에 관한 공통된 관심과 정책 이슈에 관한 필요성이 대두되기 시작하였다.

즉 글로벌 전자상거래 시장 활성화를 위한 국가 간 자유로운 정보 이동이 국제적인 흐름으로 자리 잡아가고 있는 상황에서 사전 동의 방식으로 인해 개인정보 제공 및 국가 간 정보 이동을 제한하고 있는 국내 정책에 대한 변화가 요구되고 있다.

이러한 관점에서 볼 때 개인정보 보호와 관련된 정책을 수립함에 있어 보다 다양한 관점이 고려될 필요가 있지만 지금까지 개인정보 보호와 관련된 정책을 수립함에 있어 중요한 프라이버시에 대한 개념은 마땅히 보호되어야할 개인의 권리라는 개념에 기반을 두어 왔다.

<표 1>과 같이 여러 연구에서 프라이버시에 대한 개념을 다양한 관점으로 정의(Pavlou, 2011; Smith et al., 2011)하고 있으며 개인정보를 여러 유형으로 분류함과 함께(한국인터넷진흥원, 2012) 개인정보의 가치를 다르게 산정할 수 있음에도(한국정보보호진흥원, 2007) 불구하고 개인정보 보호와 관련된 정책은 여러 이해관계자의 다양한 관점을 수용하지 못하고 있다. 이는 개인정보 보호에 대한 책임 분배 그리고 그에 따른 시간적·금전적 비용(감시비용, 확증비용, 잔여손실)[1] 에 대한 합리적인 분배의 불균형을 초래하게 한다.

<표 1> 프라이버시 관점의 분류

분류		정의
가치기반 (Value-based)	권리 (Right)	혼자 있을 수 있는 권리 (Westin, 1967) 혼자 있을 수 있는 개인의 일반적인 권리(Warren & Brandeis, 1890)
	상품 (Commodity)	이익과 교환할 수 있는 상품(Smith et al., 2011)
동일기반 (Cognate-based)	상태 (State)	사람에게 제한된 접근 상태 (Schoeman, 1984)
	통제 (Control)	스스로 접근을 선택적으로 통제(Altman, 1975)

김상희, 2015

예컨대 프라이버시가 침해될지도 모른다는 염려에도 불구하고 개인정보를 제공하는 인터넷 사용자의 행동적 특성과 인터넷 사용자의 개인정보를 수집·이용하는 전자상거래 업체의 개인정보 보호와 관련된 권한 위임에 대한 계약적 관계에 대한 이해(Li, 2012)가 고려되지 않은 채 프라이버시 보호에 대한 모든 책임이 전자상거래 업체에 일방적으로 전이되어 있음을 지적하고 보다 세분화되고 합리적인 비용 분배의 필요성이 요구된다.

이러한 시점에서 최근 정부는 2016년 9월 1일부터 기업 규모 및 개인정보 보유량에 따라 3가지 유형으로 분류하여 개인정보 안전조치를 수행하도록 하는 '개인정보의 안전성 확보조치 기준'을 <표 2>와 같이 시행함으로써 부분적으로 나마 정책적 변화를 꾀하고 있다(행정자치부 고시, 2016).

1) **감시비용(monitoring cost)** : 전자상거래 업체의 행위가 인터넷 사용자의 이익으로부터 이탈하는 것을 제한하기 위하여 인터넷 사용자가 부담하는 비용, **확증비용(bonding cost)** : 전자상거래 업체가 인터넷 사용자에게 해가 되는 행위를 하지 않고 있음을 확증하기 위해 전자상거래 업체가 부담하는 비용, **잔여 손실(residual cost)** : 전자상거래 업체의 의사결정과 인터넷 사용자의 입장에서 본 최적의 의사결정 사이에는 괴리가 발생하는데 이러한 괴리로 말미암아 인터넷 사용자가 감수하게 되는 부의 감소를 의미.

<표 2> 개인정보처리자 유형 및 개인정보 보유량에 따른 안전조치 기준

유형	적용 대상	비율	개정된 안전조치 주요내용
유형1 (완화)	• 보유량 1만명 미만소상공인, 단체, 개인	80%	• 내부관리계획 수립, 접근권한 관리 일부 면제 • 접근통제 기술적 조치사항 일부(고유식별정보 취약점 점검 등) 면제
유형2 (표준)	• 보유량 1만명 이상 소상공인, 단체, 개인 • 보유량 10만명 미만 대기업, 중견기업, 공공기관 • 보유량 100만명 미만의 중소기업	19.7%	• 재해·재난 대비 등 안전조치사항 면제 • 개인정보처리시스템의 접근권한 및 접근통제 강화를 위한 기술적 조치 강화
유형3 (강화)	• 보유량 10만명 이상 대기업, 중견기업, 공공기관 • 보유량 100만명 이상 중소기업, 단체	0.3%	• 내부관리계획(위기대응 절차 마련 등), 암호화키 관리 등 관리적 조치 강화 • 재해·재난 대비 안전조치 등 비상시 대책 강화

자료 : 행정자치부 보도자료

'개인정보의 안전성 확보조치 기준'은 개인정보 보유량과 상관없이 모든 기업이 획일적으로 개인정보의 안전성을 확보해야 하는 기존의 정책을 개선한 것인데 이는 개인정보 처리자가 개인정보 보호에 대한 책임이 있다는 기존의 정책적 원칙을 부분적으로 완화 및 강화한 내용이라 볼 수 있다.

개인정보 보호와 관련된 정책을 수립함에 있어 여러 이해관계자의 다양한 관점이 고려되어야할 필요성이 대두되고 있는 만큼 본 연구에서는 자신이 얻게 되는 이익과 교환하기 위해 개인정보를 제공하는 인터넷 사용자가 경제적 행동을 설명함으로써 프라이버시에 대한 개념이 권리로서의 개념과 함께 상품으로서의 개념을 내포하고 있음을 설명하고자 한다.

이를 위해 본 연구에서는 정보 프라이버시 계산 이론을 기반으로 프라이버시 침해 염려에도 불구하고 자신의 개인정보를 제공하는 인터넷 사용자의 경제적 행동을 연구모형에 반영하였고 또한 커뮤니케이션 프라이버시 관리 이론을 기반으로 인터넷 사용자의 프라이버시 침해 염려가 형성되는 과정을 연구모형에 반영하고 이를 실증분석하였다.

아울러 본 연구에서는 최근 프라이버시 연구에서 관심이 되고 있는 행동경제학 연구에서의 이중 프로세스 이론을 전체적인 연구모형 설계 과정에 반영하여 설명하고자 하였다(Goes, 2013; 김종기·김상희, 2015). 즉 이중 프로세스 이론에서 설명하고 있는 인간의 두 가지 형태의 정보처리 과정을 전체적인 연구모형 설계 과정에 반영함으로써 본 연구의 핵심요인인 프라이버시 염려가 개인정보 유출 경험 유무에 따라 다르게 나타나는지를 확인하고자 하였다.

이에 본 연구에서는 다음과 같은 연구 질문을 제시하고 이를 설명하고자 한다.

연구질문 1 : 정보 프라이버시 염려는 프라이버시를 중요하게 생각하는 프라이버시 가치성향에서 비롯한 지각된 위험과 지각된 통제 수준을 통해 생성되는가?

연구질문 2 : 개인정보 제공과 관련된 인터넷 사용자의 행동은 정보 프라이버시 염려와 상충된 지각된 이득에 의해 발생하는가?

연구질문 3 : 개인정보 유출 경험은 프라이버시

염려가 형성되는 과정에 유의한 영향을 미치는가?

Ⅱ. 이론적 배경

2.1 이중 프로세스 이론

이중 프로세스 이론(Dual-Process Theory)에서는 인간의 의사결정 절차가 두 종류의 서로 다른 생각 즉, 서로 다른 시스템을 통해 이루어진다고 설명하고 있다. 인간의 의사결정 절차가 두 종류의 시스템을 통해 이루어진다는 것은 오래 전부터 많은 연구자들에 의해 인식되어 왔지만 이중 프로세스라는 구체적인 용어와 함께 본격적으로 연구되기 시작한 것은 Wason and Evans(1975)의 연구에서 부터이다. 특히 사회적 인지 분야에서 많은 관심을 받고 있는(Dienes & Perner, 1999; Sun et al., 2005) 이중 프로세스 이론은 현재까지도 다양한 연구 분야에서 다루어지고 있다(Sloman, 1996; Barbey & Sloman, 2007; Evans, 2008; Kahneman, 2011; Stanovich et al., 2011).

인간이 의사결정을 수행하기 위해 사용하는 두 종류의 정보처리 시스템은 <표 3>과 같이 시스템1(system1)과 시스템2(system2)로 구분된다. 먼저 시스템1은 빠르고 직관적인 생각으로 크게 노력을 들이지 않아도 정보처리가 가능한 특성을 가지며 시스템2는 느리고 신중한 생각으로 분석적인 노력을 통해 정보처리가 가능한 특성을 가진다.

<표 3> 이중 프로세스 이론의 선행연구

System1	System2	Researcher
Input modules	Higher cognition	Fodor(1983, 2001)
Automatic	Controlled	Schneider & Schiffrin(1977)
Experiential	Rational	Epstein(1994, 1999)
Heuristic	Systematic	Chaiken(1980); Chen & Chaiken(1999)
Implicit/tacit	Explicit	Reber(1993); Evans & Over(1996)
Heuristic	Analytic	Evans(1989, 2006)
Associative	Rule based	Sloman(1996); Smith & DeCoster(2000)
Intuitive	Analytic	Hammond(1996)
System1 (TASS)	System2 (Analytic)	Stanovich (1999, 2004)
Holistic	Analytic	Nisbett et al.(2001)
Adaptive unconscious	Conscious	Wilson(2002)
Reflexive	Reflective	Lieberman(2003)
Stimulus-bound	Higher-order	Toates(2006)
Impulsive	Reflective	Strack & Deustch(2004)

Evan, 2008

즉 시스템1은 인간의 동물적 특성을 반영하며 인간과 동물이 보편적으로 가지고 있는 직감적이고 감정적인 특성을 말한다. 시스템2는 주류 경제학에서 설명하는 인간의 경제적인 특성을 반영하는데 교육과 진화를 통해 가지게 되는 분석적이고 통제적인 특성을 말한다.

인간은 기본적으로 자신에게 위험이 되는 상황을 회피하려는 특성을 가진다. 위험을 회피하려는 인간의 특성은 위험과 통제에 대한 직감적인 판단을 통해 태도를 형성하는데 위험에 대한 강도와 이를 통제할 수 있는지에 대한 직감적인 판단은 위험에 대한 서로 다른 태도를 가지게 한다(Kahneman, 2011). 이러한 관점을 기반으로 프라이버시 침해 위험에 대해 인간은 기본적

으로 자신의 프라이버시를 보호하려는 욕구를 가지며 자신의 개인정보를 제공하기에 앞서 전자상거래 업체에 대한 위험과 통제에 대한 직감적인 판단을 통해 해당 업체에 대한 태도를 가지게 된다. 이처럼 위험과 관련된 인간의 판단은 직감적인 특성을 가진 시스템1에 의존하게 되며 자신의 프라이버시 보호와 관련된 개인 태도 형성에 영향을 미칠 것이다.

또한 인간은 이득과 손해에 따른 계산적 판단을 통해 행동여부를 결정한다. 인간은 때때로 전자상거래 업체에 자신의 개인정보를 제공함으로써 향후 프라이버시 침해 문제가 발생할지 모른다는 염려에도 불구하고 자신의 개인정보를 제공하는 모순된 행동을 보인다(Culnan & Bies, 2003; 김상희, 2015). 이는 개인정보 제공 통해 얻게 되는 현재의 이득이 개인정보 제공으로 인해 향후 발생할 수 있는 프라이버시 침해로 인한 손해 보다 클 것이라는 계산적인 판단을 통해 결정되는 것이다. 이처럼 이득과 관련된 인간의 판단은 분석적인 특성을 가진 시스템2에 의존하게 되며 자신에게 이득이 되는 방향으로 행동을 결정하는데 영향을 미칠 것이다.

2.2 커뮤니케이션 프라이버시 관리 이론

커뮤니케이션 경계 관리(CBM, communication boundary management) 이론을 기초로 하는 커뮤니케이션 프라이버시 관리(CPM, communication privacy management) 이론은 대인관계 형성 과정에서 개인정보 공개 여부를 결정하는 것과 관련된 개인의 인지적 과정을 설명하기 위한 이론이다. Petronio(2002)에 의해 개발된 CPM 이론은 개인정보 공개 범위를 결정하기 위해 상대방에 대한 경계를 어느 범위까지 개방 또는 폐쇄해야 하는지에 대한 이분법적인 관계를 설명하고 있다.

CPM 이론과 관련하여 초기의 연구들은 의사와 환자, 부모와 자식, 상사와 부하 관계와 같은 대인관계 형성 과정에 초점을 두었지만 최근 CPM 이론에 관한 연구들은 전자상거래의 기술적 특성으로 인해 발생할 수 있는 개인정보 유출로 인한 정보 프라이버시 염려가 형성되는 과정을 설명하는데 초점을 두고 있다(Xu et al., 2011).

이는 회사 상사 및 동료에게 자신의 개인정보를 어느 정도까지 공개할지를 결정하기 위한 인지적 과정이 전자상거래 업체에게 자신의 개인정보를 얼마만큼 제공할지에 대한 인지적 과정과 유사한 절차로 이루어짐을 설명한다. 이에 Metzger(2007)은 CPM 이론에 대한 개념적 이해가 온라인상에서의 개인의 정보 프라이버시 관리에도 적용 가능하다고 설명하고 있다.

CPM 이론에는 타인에 대해 개인이 인지할 수 있는 수준의 경계 규칙이 수립되는 과정을 경계 규칙 형성, 경계 혼란, 경계 조정이라는 세 가지 핵심 요인을 통해 형성된다고 설명하고 있다. 먼저 경계 규칙 형성은 개인정보 공개 여부를 결정할 때 사용되는 기준을 개인이 어떻게 인지하고 있는지를 설명하는데 CPM 이론에서는 상황에 따라, 동기 부여 원인에 따라, 성별에 따라, 성향에 따라, 문화에 따라 개인이 인지하는 기준이 서로 다를 수 있다고 설명하고 있다. 이에 본 연구에서는 개인정보 제공을 위한 경계 규칙이 프라이버시와 관련된 개인 성향에 따른 전자상거래 업체에 대한 위험과 통제 판단으로 형성된다고 설명한다.

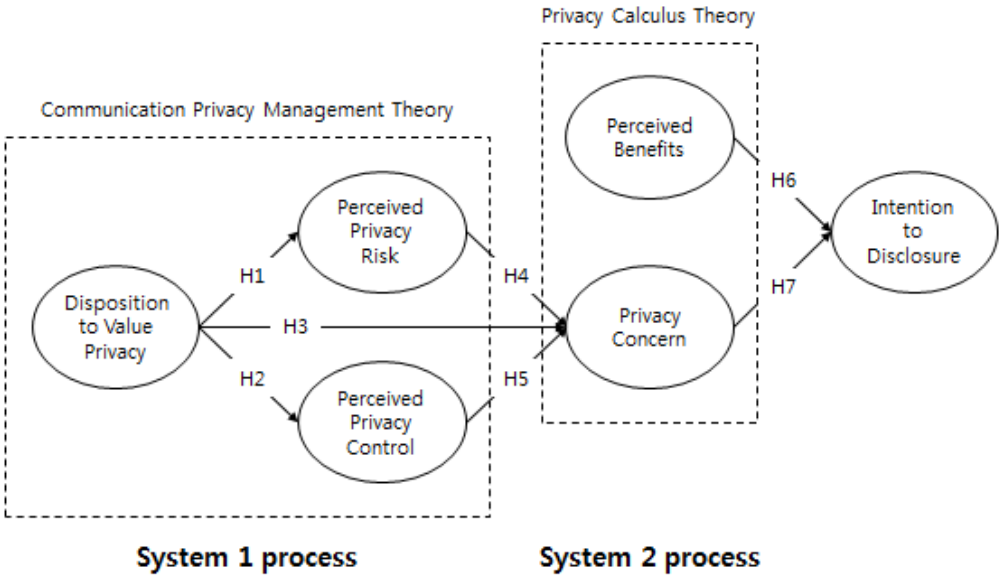
경계 혼란은 자신의 개인정보를 공동으로 가짐으로써 함께 책임지게 될 공동 소유자에 대한 개인정보 공개 범위 변화에 대한 혼란을 말한다. 즉 인터넷 사용자의 개인정보 제공으로 개인정보의 공동 소유자 및 책임자가 되는 전자상거래 업체에 대한 프라이버시 위험 평가는 전자상거래 업체에 대한 개인정보 제공 범위를 변화시키는 주요 동기가 될 것이다.

경계 조정은 자신의 개인정보를 함께 책임지는 공동 소유자에 대한 통제 수준으로 결정되는 범위 조정을 말한다. 즉 자신의 개인정보를 제공과 함께 개인정보의 공동 소유자인 전자상거래 업체에 대한 통제 수준으로 자신의 개인정보를 제공할 수 있는 전자상거래 업체를 결정하고 자신의 개인정보 제공 범위를 최종적으로 조정하는 과정을 말한다.

2.3 프라이버시 계산 이론

오랫동안 사회과학 연구 분야에서는 개인의 행동을 이해하고 이를 예측하기 위한 다양한 방법들이 제시되어 왔다. 특히 합리적인 행동 이론(TRA)과 계획된 행동 이론(TPB)은 정보 기술과 관련된 개인의 행동을 이해하고 예측하기 위한 이론으로 널리 사용되어 왔으며(Ajzen, 1991) 이를 기반으로 많은 MIS 연구자들은 개인의 행동을 이해하고 예측하기 위한 보다 진보된 이론적 근거를 제시하고자 노력해 왔다(Davis et al., 1989, Venkatesh & Bala, 2008). 하지만 사회과학 분야에서 설명하고 있는 인간은 합리적인 방향으로 행동을 결정한다는 주장은 프라이버시 침해 위험에도 불구하고 자신의 개인정보를 제공하는 인터넷 사용자들의 모순된 행동을 설명하기에는 이론적 근거로써 부족한 부분이 있다.

이에 프라이버시 계산 이론은 이러한 인간의 모순된 행동을 이해하는데 도움을 주고 있는데 인터넷 사용자들이 프라이버시 침해 염려에도



<그림 1> 연구모형

불구하고 자신의 개인정보를 제공하는 것은 개인정보 제공으로 얻게 되는 이득이 향후 발생 가능한 손해 보다 클 것이라는 이분법적 계산에 기반 한 행동으로 이해할 수 있다(Dinev & Hart, 2006; Li et al., 2010; 이동주 등, 2010; 민진영・김범수, 2013).

즉 인터넷 사용자들은 자신에게 돌아올 부정적인 결과를 최소화하는 범위 내에서 개인에게 돌아올 긍정적인 결과를 최대화하는 방법으로 행동을 하게 되며 개인정보 제공과 관련된 손해와 이득에 관한 이분법적인 판단에서 비롯한 상대적 강도에 따라 개인정보 제공 여부를 결정하는 것이다. 이에 Culnan and Bies(2003)는 인터넷 사용자들은 전자상거래를 통해 얻게 되는 긍정적인 결과가 평소 자신이 인지하고 있는 위험의 허용 수준을 넘어설 경우 개인정보의 제공과 함께 프라이버시 침해로 인한 손실을 받아들일 수 있다고 설명하고 있다.

이는 프라이버시가 마땅히 보호되어야 할 절대적인 개념이라는 관점에서 벗어나 손해와 이득에 따라 거래될 수 있는 상품으로써의 경제적 개념이 포함될 필요가 있음을 보여준다(김종기・김상희, 2012). 즉 프라이버시 계산 이론은 손해와 이득 간의 서로 상충된 개념을 통해 개인정보 제공 여부를 결정하기 위한 복잡한 의사결정 과정을 이해하는데 도움을 준다.

Ⅲ. 연구모형 및 연구가설

3.1 연구모형

본 연구에서는 전자상거래 업체에 자신의 개인정보를 얼마만큼 제공해야 하는지에 대한 공개 범위 조정을 커뮤니케이션 프라이버시 관리(CPM) 이론을 통해 설명하고자 한다. 사람들은 자신의 프라이버시가 침해되는 것에 대한 염려를 줄이기 위한 차원에서 전자상거래 업체에 대한 위험 분석과 이를 얼마만큼 통제할 수 있는지에 대한 평가로 개인정보 공개 범위를 조정한다. 즉 개인정보 제공으로 인해 발생할지 모를 프라이버시 침해에 대한 염려는 전자상거래 업체에 대한 위험과 통제 수준에 대한 인식으로 형성된다는 것이다.

이와 함께 본 연구에서는 자신의 프라이버시가 침해될지도 모른다는 염려에도 불구하고 자신의 개인정보를 제공하는 인터넷 사용자들의 행동을 설명하고자 한다. 사람들은 프라이버시 염려를 최소화하는 범위 내에서 개인정보 제공으로 얻게 되는 이득을 위해 개인정보를 제공한다. 즉 정보 제공에 대한 인터넷 사용자의 긍정적인 태도는 프라이버시 계산 이론을 기반으로 프라이버시 염려와 개인정보 제공으로 얻게 되는 이득을 계산함으로써 형성된다는 것이다. 이처럼 인터넷 사용자의 정보 제공 의도를 분석하기 위해 커뮤니케이션 프라이버시 관리 이론과 프라이버시 계산 이론에서 도출한 구성개념들로 <그림 2>와 같이 연구모형을 설계하고 연구가설을 도출하였다.

3.2 연구가설

3.2.1 프라이버시 가치성향과 지각된 프라이버시 위험, 통제와의 관계

커뮤니케이션 프라이버시 관리 이론은 대인관계에서 자신에 대한 정보를 공개할지 혹은 보

류할지 여부를 결정하는 것과 정보 경계에 대한 공개 및 폐쇄 범위를 관리하는데 있어 개인의 특성이 중요한 역할을 한다고 설명하고 있다 (Petronio, 2002).

타인에게 자신을 표현하거나 혹은 감추기 위한 사적 정보공간에 대한 경계 관리 규칙에 관한 개인의 성향은 자신의 과거 경험, 인구 통계학적 특성, 개인의 성격에 의해 영향을 받는다. 이는 타인과의 관계 형성 과정에서 신뢰자의 특성(Mayer et al. 1995) 및 신뢰에 대한 성향 (McKnight et al., 1998)이 타인에 대한 개인의 신뢰 형성에 중요한 역할을 하는 것과 맥락을 같이 한다.

이러한 맥락에서 프라이버시를 중요하게 인식하는 성향은 외부의 간섭이나 침해로부터 자유롭고자 개인의 사적 정보공간에 대한 경계를 유지하는데 필요한 개인의 특성을 반영하는 성격적인 속성이다. 본 연구에서는 프라이버시를 중요하게 인식하는 성향을 자신의 사적 정보공간을 확보하기 위해 또는 다양한 상황에서 공개될 수밖에 없는 개인정보를 제한하기 위한 개인의 성격적 특성으로 정의한다.

커뮤니케이션 프라이버시 관리 이론을 기반으로 한 본 연구에서는 프라이버시를 중요하게 인식하는 개인의 성향을 사적 정보공간에 대한 경계 개방 및 폐쇄 여부를 결정하는데 중요한 요인으로 보고 프라이버시를 중요하게 인식하는 개인의 성향이 프라이버시에 대한 위험과 통제에 관한 평가에 있어 중요한 영향을 미칠 것으로 정의하고 있다.

개인의 사적 정보공간에 대한 경계가 개인의 성향과 더불어 정보 교환을 요구하는 외부 개체와의 주어진 관계 상황, 즉 위험-통제에 대한 인식에 의해서 변화 혹은 유지된다는 설명(Xu et al., 2011)을 바탕으로 프라이버시에 대한 중요성을 높게 인식하는 사람은 자신이 규정한 사적 정보공간에 대한 경계를 확고히 하거나 전자상거래 업체가 자신의 개인정보를 이용하는 것과 관련하여 통제의 필요성을 더욱 높게 인지하게 될 것이다.

아울러 전자상거래 업체로 하여금 동일한 형태의 정보 공개 요구가 있다고 하더라도 프라이버시의 중요성을 높게 인식하는 사람은 전자상거래 업체에 자신의 개인정보를 공개하는 것과 관련하여 손실 발생 가능성에 대해서도 높게 인식하게 될 것이며 제3자가 자신의 개인정보를 이용할 수 있도록 기회를 제공하는 것 또한 프라이버시에 대한 손실로 여길 것이다.

따라서 이러한 특성을 가진 사람은 정보 공개와 관련된 프라이버시 위험을 높게 인식하게 될 것이며 이에 대한 통제의 필요성을 강하게 인지하게 될 것이다. 이에 본 연구에서는 프라이버시에 대한 중요성을 높게 인식하는 인터넷 사용자는 프라이버시 위험을 높게 인식할 것이며 아울러 프라이버시 통제에 대해서는 낮게 인식하게 될 것이라는 가설을 설정하였다.

[H1] 프라이버시 가치성향은 지각된 프라이버시 위험에 긍정적인 영향을 미칠 것이다.

[H2] 프라이버시 가치성향은 지각된 프라이버시 통제에 부정적인 영향을 미칠 것이다.

3.2.2 프라이버시 가치성향과 프라이버시 염려와의 관계

정보 프라이버시 염려를 중심으로 선행요인과 결과요인의 관계를 설정하고 통합모델을 제

시한 Smith et al.(2011)은 정보 프라이버시 염려에 대한 선행요인으로 프라이버시 경험, 개인적 차이, 프라이버시 인식, 인구통계학적 차이, 문화와 같이 다섯 가지 요인들을 제시하고 있다.

프라이버시 경험은 개인정보 유출로 인해 프라이버시 침해 경험이 있는 개인이 정보 프라이버시에 관한 심각한 염려를 갖게 된다는 것이다(Smith et al., 1996).

프라이버시 인식은 개인이 전자상거래 업체의 프라이버시 규정에 대해 알고 있는 정도를 나타내는데 개인정보 삭제 절차에 대해서 알지 못하는 인터넷 사용자는 삭제 절차를 알고 있는 인터넷 사용자 보다 프라이버시 염려를 적게 하는 경향이 있다고 설명하고 있다(Culnan, 1995; Nowak & Phelps, 1995).

또한 내향적, 외향적, 자기 독립적, 상호 의존적, 순응적, 정서 불안적, 성실성, 지성과 같은 개인의 성격은 개인의 프라이버시 염려에 영향을 미친다고 설명하고 있다. 즉 프라이버시 염려는 프라이버시 보호 절차에 대한 개인의 인식 수준과 함께 직·간접적인 프라이버시 침해 경험 그리고 개인의 성격에 따라서 다르게 나타날 수 있다는 것이다(Xu el al., 2010; Smith et al., 2011).

이에 본 연구에서는 프라이버시 경험, 프라이버시 인식, 개인 성격을 종합하여 프라이버시를 중요하게 인식하는 성향일수록 프라이버시 침해에 대한 염려가 클 것으로 보고 프라이버시에 대한 중요성을 높게 인식하는 인터넷 사용자는 정보 프라이버시 염려를 높게 인식하게 될 것이라는 가설을 설정하였다.

[H3] 프라이버시 가치성향은 프라이버시 염려에 긍정적인 영향을 미칠 것이다.

3.2.3 지각된 프라이버시 위험과 프라이버시 염려

지각된 위험은 Bauer(1960)의 연구에서 처음 소개된 개념으로 어떤 행위를 할 때 예측할 수 없는 결과가 나타날 가능성에 대한 주관적인 지각으로 설명한다(Javenpaa et al., 2000).

지각된 위험에 관한 초기 연구에서는 지각된 위험을 손실의 관점으로 보고 어떤 행동이 바람직하지 못한 결과를 가져왔을 때 그 대가로 지불하게 될 손실의 양과 잘못된 결과가 발생할 가능성에 대한 주관적 느낌으로 정의하고(Cunningham, 1967) 이를 재무 위험, 성과 위험, 사회적 위험, 시간 위험, 전반적 위험, 프라이버시 위험의 여섯 가지로 분류하여 설명하고 있다(Cox, 1967)

프라이버시 관점에서의 지각된 위험은 부정적 결과가 발생할 가능성에 대한 개인의 평가뿐만 아니라 부정적 결과가 발생할 가능성에 대한 인식도 포함한다. 인터넷 사용자의 개인정보를 수집·이용하는 전자상거래 업체의 기회주의적 행동에는 인터넷 사용자의 프라이버시 침해 가능성을 내포하고 있으며 이러한 위험과 관련된 인터넷 사용자의 부정적인 인식은 물질적, 정신적으로 개인에게 영향을 미칠 것이다(Moon, 2000).

전자상거래에 관한 여러 실증 연구에서는 일반적으로 위험 인식과 프라이버시 염려 간의 유의한 관계가 있는 것으로 설명하고 있다(Pavlou & Gefen, 2004). 회원가입 절차와 같이 자신의 개인정보를 전자상거래 업체에 제공할 때 인터

넷 사용자는 개인정보에 대한 접근 및 이용 절차에 포함된 불확실성 수준에 대해서 평가하게 된다. 불확실성 수준을 높게 평가한 인터넷 사용자는 자신의 개인정보가 위험에 노출되어 있음을 인식하게 되며 향후 자신의 프라이버시가 침해될지 모른다는 염려를 갖게 된다.

개인정보 제공에 대한 높은 위험 인식은 자신의 프라이버시가 침해될지도 모른다는 염려를 높여 자신의 개인정보를 제공해야 하는지에 대한 의문을 갖게 될 것이다. 이에 본 연구에서는 전자상거래 업체에 대한 프라이버시 위험을 높게 인식할수록 인터넷 사용자의 정보 프라이버시 염려는 높아질 것이라는 가설을 설정하였다.

[H4] 지각된 프라이버시 위험은 프라이버시 염려에 긍정적인 영향을 미칠 것이다.

3.2.4 지각된 프라이버시 통제와 프라이버시 염려

프라이버시 통제는 프라이버시에 대한 개념적 정의를 설명하기 위해 많은 연구에서 사용되고 있다. 일반적으로 정보 프라이버시는 자신에 대한 정보가 타인에게 전달되고 이용되는 일련의 절차를 정보주체로서 자율적으로 통제할 수 있는 권리로 설명할 수 있는데 이는 개인정보통제권이라는 용어와 함께 사용되고 있다. Culnan(2000)은 개인정보통제권에 대해서 자신의 개인정보가 수집・이용되는 상황을 개인이 통제할 수 있는 능력으로 설명하고 있다.

통제가 정보 프라이버시에 대한 개념적 정의에서 중요하게 다루어지고 있는 이유는 인터넷 사용자들이 자신의 개인정보를 제공하는 상황에서 위험을 매우 높게 인식하고 있기 때문이다. Malhotra et al.(2004)은 정보 프라이버시 염려를 인터넷 사용자의 정보 프라이버시 염려(IUIPC, internet user's information privacy concerns)라는 다차원적 구성개념으로 설명하고 있으며 인터넷 사용자의 정보 프라이버시 염려가 온라인 기업에 대한 개인정보의 수집(collection), 통제(control), 인지(awareness)수준으로 형성된다고 설명하고 있다.

이러한 관점에서 통제는 통제의 대상이 되는 개인정보를 강조하는 인지적 구조로 이해되며 프라이버시 염려와는 구별된 변수로 개념화되고 있다(Xu & Teo, 2004). 따라서 지각된 프라이버시 통제는 개인정보 수집・이용과 관련된 전자상거래 업체의 행위를 제한할 수 있는 개인의 능력에 대한 신념으로 정의할 수 있다.

전자상거래와 관련된 여러 실증 연구에서 개인정보 오・남용과 관련된 인터넷 사용자의 통제 수준이 프라이버시 염려와 부(-)의 관계를 형성하고 있음을 설명하고 있으며 자신의 개인정보가 유출되거나 오・남용되는 것을 통제할 수 있다는 인식을 가질 때 사람들은 자신의 프라이버시가 침해될지도 모른다는 염려를 적게 하는 것으로 나타났다.

이에 본 연구에서는 개인정보에 대한 인터넷 사용자의 지각된 통제가 프라이버시 염려와 상반된 구성개념으로 보고 전자상거래 업체에 대한 프라이버시 통제를 낮게 인식할수록 인터넷 사용자의 정보 프라이버시 염려는 높아질 것이라는 가설을 설정하였다.

[H5] 지각된 프라이버시 통제는 프라이버시 염려에 부정적인 영향을 미칠 것이다.

3.2.5 지각된 이득과 정보 제공 의도

개인정보를 경제적 이득의 대가로 교환될 수 있는 상품의 개념으로 볼 수 있다는 설명(Smith, 2011)과 함께 마케팅 분야에서의 Culnan and Bies(2003)는 높은 수준의 서비스 및 가격 할인을 제공 받는 대가로 자신의 개인정보를 공개하는 비 금전적인 교환을 2차적 교환(second exchange)이라는 개념으로 설명하고 있다. 이와 같은 맥락으로 정보시스템 연구 분야에서 설명하고 있는 프라이버시 계산(privacy calculus) 이론에서는 개인의 행동 결과로 향후 발생 가능한 비용과 이득에 대한 비교·판단으로 자신의 개인정보를 제공할지 여부를 결정하는 개인의 행동을 설명하고 있다.

이는 자신의 프라이버시가 침해될지도 모른다는 염려에도 불구하고 자발적으로 자신의 개인정보를 제공하는 인터넷 사용자들의 모순된 행동을 설명할 수 있다(Garfinkel, 2000; Campbell & Carlson, 2002). 예컨대, 포인트 점수 누적을 위해 백화점이나 마트 등에서 보너스 카드를 사용하여 자신의 구매 정보를 제공(Acquisti & Grossklags, 2005)하는 사람들의 행동, 개인화 서비스를 받기 위해 SNS나 스마트폰에서 자신의 위치정보 제공(Acquisti & Gross, 2006)을 허용하는 사람들의 행동을 보면 개인정보는 경제적 이득 및 생활의 편리를 위해 상품처럼 거래될 수 있음을 보여준다.

이에 Kobsa and Teltzrow(2005)는 웹사이트를 통해 인터넷 사용자가 얻는 이득이 자신이 제공한 개인정보와 밀접한 관련이 있는 경우 자신에 대한 더 많은 정보를 공개한다고 설명하고 있다. 이처럼 개인정보 제공으로 프라이버시가 침해될지도 모른다는 염려에도 불구하고 자신이 얻을 수 있는 이득을 위해 자발적으로 개인정보를 제공하는 인터넷 사용자의 행동 사이에는 프라이버시 역설(privacy paradox)이라는 모순된 행동이 존재한다(Awad & Krishnan, 2006; Norberg et al., 2007). 이처럼 개인정보 제공을 통해 얻게 되는 경제적, 사회적 이득은 인터넷 사용자로 하여금 개인정보 제공의 강한 동기가 될 것이다. 이에 본 연구에서는 전자상거래 업체에 대한 지각된 이득이 높을수록 정보 제공 의도는 높아질 것이라는 가설을 설정하였다.

[H6] 지각된 이득은 정보 제공 의도에 긍정적인 영향을 미칠 것이다.

3.2.6 프라이버시 염려와 정보 제공 의도

정보 프라이버시 염려는 정보 프라이버시에 대한 개인의 걱정을 측정하기 위한 구성개념으로 외부의 위험으로 인해 자신의 개인정보가 무단으로 수집되는 것, 안전하게 보호되지 않는 것, 본인의 동의 없이 2차적으로 사용되는 것, 제3자에게 판매되는 것과 관련하여(Smith et al., 1996; Malhotra et al., 2004) 이를 자신이 통제하기 어렵다는 인식에서 발생한다.

정보 프라이버시 염려가 개인정보 제공에 부정적인 영향을 미친다는 설명과 함께 정보시스템 연구 분야에서는 개인의 정보 프라이버시 염려를 측정하기 위한 다양한 방법이 제시(Stewart & Segars, 2002; Malhotra et al., 2004)되고 있는 가운데 Smith et al.(1996)은 정보 프라이버시에 대한 염려(CFIP, concern for information privacy)를 네 가지 구성개념으로 모델화 하고 있다.

먼저 수집(collection)은 개인에 대한 많은 양

<표 4> 구성개념에 대한 조작적 정의 및 측정항목

구성개념	조작적 정의	관련 연구자
프라이버시 가치성향	타인에 비해 정보 프라이버시 유지를 중요하게 생각하는 정도	Xu et al., 2011
지각된 프라이버시 위험	인터넷 사용자가 제공한 개인정보 이용에 관한 온라인 기업의 기회주의적인 행동에 대해서 지각하는 위험 정도	Javenpaa et al, 2000, Pavlou & Gefen, 2004
지각된 프라이버시 통제	온라인 기업에 의해 수집된 개인정보에 접근할 수 있는지를 통제할 수 있는 정도	Culnan, 2000
프라이버시 염려	인터넷 사용자가 제공한 개인정보에 관한 온라인 기업의 기회적인 행동에 대해서 염려하는 정도	Smith et al., 2011
지각된 이득	인터넷 사용자가 온라인 기업에 개인정보를 제공함으로써 얻을 수 있는 이득 정도	Acquisty & Gross, 2006; Culnan & Bies, 2003
정보 제공 의도	앞으로 온라인 기업에 개인정보를 제공하려는 정도	Kobsa & Teltzrow, 2005

의 데이터가 온라인 기업에 의해 수집 및 저장되고 있다는 것에 대한 염려로 설명하고 있으며, 에러(error)는 고의적이거나 우발적인 오류로 인해 개인정보 보호가 적절하게 관리되고 있지 않다는 것에 대한 염려로 설명하고 있으며, 비인가된 2차사용(unauthorized secondary use)은 개인의 허가 없이 본래의 개인정보 수집 목적이 아닌 다른 목적으로 조직 내부 또는 외부에서 사용되는 것에 대한 염려로 설명하고 있으며, 부적절한 접근(improper access)은 개인정보에 대한 이용 권한이 없는 사람이 자신의 정보를 쉽게 이용할 수 있는 것에 대한 염려로 설명하고 있다.

Smith et al.(1996)의 정보 프라이버시 염려(CFIP) 모델은 정보시스템 연구 분야에서 정보 프라이버시 염려를 측정하기 위한 방법으로 많은 연구자들에 의해 사용되고 있으며 단일 차원 개념(Bellman et al., 2004; Buchanan et al., 2007; Xu et al., 2011)뿐만 아니라 다차원적 개념(Malhotra et al., 2004; Slyke et al., 2006)으로도 사용되고 있다. 또한 Malhotra et al.(2004)은 인터넷 사용자의 정보 프라이버시 염려(IUIPC, internet user's information privacy concerns)를 온라인 기업에 대한 개인정보의 수집(collection), 통제(control), 인지(awareness) 수준으로 형성된 다차원적 개념으로 설명하고 있다.

이처럼 정보 프라이버시 염려에 대한 개념적 정의와 함께 전자상거래와 관련된 여러 연구 분야에서 정보 프라이버시 염려와 인터넷 사용자의 개인정보 제공 행동 간에 밀접한 관계를 가지고 있는 것으로 설명하고 있으며(Dinev et al., 2008; 유일 등, 2008) 자신의 프라이버시가 침해될지도 모른다는 인터넷 사용자의 염려가 전자상거래 업체에 자신의 개인정보를 제공할지 여부를 결정하는 중요한 요인임을 설명하고 있다. 이에 본 연구에서는 전자상거래 업체에 대한 정보 프라이버시 염려가 높을수록 정보 제공 의도는 낮아질 것이라는 가설을 설정하였다.

[H7] 프라이버시 염려는 정보 제공 의도에 부정적인 영향을 미칠 것이다.

Ⅳ. 연구방법

4.1 자료의 특성 및 분석 방법

4.1.1 자료 수집과 표본 특성 분석

본 연구에서는 먼저 커뮤니케이션 프라이버시 관리 이론을 통해 인터넷 사용자의 정보 프라이버시 염려가 형성되는 과정을 설명하고 아울러 자신의 프라이버시가 침해될지 모른다는 염려에도 불구하고 자신의 개인정보를 제공하는 인터넷 사용자의 모순된 행동을 프라이버시 계산 이론을 통해 설명하고자 한다.

즉 인터넷 사용자는 개인의 프라이버시 가치 성향에 따라 전자상거래 업체에 대한 프라이버시 위험과 프라이버시 통제를 다르게 인식하게 되며 이를 통해 정보 프라이버시 염려가 형성된다. 그리고 이는 전자상거래 업체를 통해 얻게 되는 이득에 대한 이분법적인 판단을 통해 자신의 개인정보를 제공할 것인지 여부를 결정하게 되는데 이러한 일련의 과정에 대해서 본 연구에서는 연구모형으로 설계하고 이를 실증분석하고자 한다.

본 연구에서는 설계된 연구모형이 연구의 구성개념들을 잘 반영하고 있는지 확인하기 위해 우선적으로 사전조사(pre-test)를 실시하였으며 이를 기반으로 본 조사에서는 사전조사에서 문제점이 발견되지 않은 18개의 설문문항을 그대로 사용하였다.

본 조사는 전자상거래를 활발하게 이용하고 있는 부산지역에 거주하는 소득이 있는 대학원생을 대상으로 하였으며 총 배포한 235부의 설문지 중 불성실하게 응답하였거나 결측치가 존재하는 16부의 설문지를 제외한 219부의 설문지를 최종적으로 선택하여 실증분석에 사용하였다.

본 연구에서는 구조방정식 모형을 통해 연구모형과 연구가설을 검증하였으며 탐색적 요인분석을 위해 SPSS 23.0과 구조방정식 모형 분석을 위해 SmartPLS 2.0을 사용하였다. 표본에 대한 인구 통계학적 특성은 <표 5>에서 요약한 것과 같으며 응답자 대부분이 직・간접적으로 개인정보 유출 경험이 있는 것에 반해 개인정보 처리방침을 자세히 읽지 않는 것으로 나타났다.

<표 5> 표본의 특성

구분		명	%
성별	남성	145	66.2
	여성	74	33.8
	계	219	100.0
나이	20~25세	181	82.7
	26~30세	36	16.4
	31~35세	2	0.9
	계	219	100.0
인터넷 이용시간 (하루)	1시간 미만	50	22.8
	1~3시간 미만	132	60.3
	3~5시간 미만	23	10.5
	5~7시간 미만	12	5.5
	7시간 이상	2	0.9
	계	219	100.0
전자상거래 이용횟수 (한달)	1~2번	138	63.0
	3~4번	56	25.6
	5~6번	16	7.3
	7~8번	3	1.4
	9번 이상	6	2.7
	계	219	100.0
개인정보 유출 경험	경험 없음	40	18.3
	소극적인 경험(스팸 메일 등)	117	53.4
	적극적인 경험 (아이디 도용 등)	62	28.3
	계	219	100.0
개인정보 이용에 대한 통지 받은 경험	경험 없다.	73	33.3
	경험 있다.	146	66.7
	계	219	100.0
개인정보 처리방침 (약관) 읽는 정도	읽지 않는다.	120	54.8
	대충 읽는다.	84	38.4
	자세히 읽는다.	15	6.8
	계	219	100.0

<표 6> 동일방법편의 검증

요인	초기고유값			추출제곱합적재량		
	전체	%분산	%누적	전체	%분산	%누적
1	6.969	27.878	27.878	6.969	27.878	27.878
2	4.566	18.263	46.141	4.566	18.263	46.141
3	2.900	11.601	57.742	2.900	11.601	57.742
4	2.147	8.587	66.329	2.147	8.587	66.329
5	1.718	6.873	73.202	1.718	6.873	73.202
6	1.064	4.257	77.459	1.064	4.257	77.459
7	0.814	3.255	80.714			

<표 7> 측정모형에 대한 집중타당성 분석

구성개념	설문문항	요인 적재량	t-값
프라이버시 가치성향 (Dis)	다른 사람들에 비해, 나는 나의 정보 프라이버시가 위협 받는 것에 대해서 더 많이 걱정하는 편이다.	0.882	65.229***
	다른 사람들에 비해, 나는 나의 정보 프라이버시가 지켜지는 것에 대해서 더욱 관심을 가지고 있는 편이다.	0.882	62.871***
	나의 정보 프라이버시가 지키지는 것은 나에게 있어서 가장 중요한 일이라고 생각한다.	0.859	68.079***
지각된 프라이버시 위험 (Ris)	웹사이트에 개인정보를 제공하는 것은 프라이버시가 위험 받게 될 가능성이 있다고 생각한다.	0.883	77.350***
	나의 개인정보는 웹사이트에 의해 부당하게 사용될 수 있다고 생각한다.	0.907	85.630***
	개인정보를 웹사이트에 제공하는 것은 여러 예기치 않은 문제를 포함한다고 생각한다.	0.917	129.938***
지각된 프라이버시 통제 (Cont)	나는 웹사이트가 수집한 나의 개인정보에 누가 접근할 수 있는지 통제할 수 있다고 생각한다.	0.921	75.271***
	나는 웹사이트가 어떤 개인정보를 공개할지 통제할 수 있다고 생각한다.	0.957	174.795***
	나는 웹사이트가 개인정보를 어떻게 사용할지 통제할 수 있다고 생각한다.	0.921	71.983***
프라이버시 염려 (Conc)	나는 웹사이트에 제공한 개인정보가 오·남용될 수 있다는 것에 대해 염려가 된다.	0.920	117.211***
	나는 개인정보가 다른 의도로 사용될 수 있기 때문에 웹사이트에 개인정보를 제공하는 것에 대해 염려가 된다.	0.944	191.787***
	나는 개인정보가 예기치 않은 방식으로 사용될 수 있기 때문에 웹사이트에 개인정보를 제공하는 것에 대해 염려가 된다.	0.940	124.111***
지각된 이득 (Ben)	웹사이트에 개인정보를 제공함으로써 쇼핑 물품에 대한 결제를 기다리지 않고 쉽게 할 수 있다.	0.788	22.804***
	나는 웹사이트에 개인정보를 제공함으로써 생일쿠폰과 같은 다양한 서비스를 받을 수 있다.	0.853	30.904***
	나는 웹사이트에 개인정보를 제공함으로써 관심 있는 물품에 관한 정보를 받아 볼 수 있다.	0.858	31.743***
정보 제공 의도 (Int)	나는 앞으로 웹사이트를 이용하기 위해 개인정보를 제공할 것이다.	0.941	119.099***
	나는 앞으로 웹사이트를 이용하기 위해 개인정보를 제공할 의향을 가지고 있다.	0.950	132.471***
	나는 앞으로 웹사이트를 이용하기 위해 개인정보를 제공할 의도를 가지고 있다.	0.885	36.835***

***$p<0.01$

4.1.2 분석 방법

실증분석을 위한 설계된 측정문항들은 선행연구를 통해 검증된 문항들로 구성하였으며 7점 리커트(Likert) 척도를 사용하여 구성하였다. 본 연구에서는 이를 재검증하고자 우선적으로 각 요인들 간의 상호독립성 평가를 위해 SPSS 23.0을 사용하여 탐색적 요인분석을 실시하였으며 다음으로 측정모형에 대한 신뢰성과 타당성 평가를 위해 연구모형의 적합도와 요인들 간의 경로분석을 위해 SmartPLS 2.0을 사용하여 연구모형 분석을 실시하였다.

4.1.3 동일방법편의 검토

개별 응답자를 대상으로 설문하는 자기보고법(self-reporting) 형태의 데이터 수집은 동일방법편의(common method bias) 문제가 존재할 수 있다(Podsakoff et al., 2003). 동일방법편의는 독립변수와 종속변수를 동일한 응답자와 방법으로 측정할 경우 발생할 수 있는 왜곡된 연구결과로 Harmen의 단일 요인 검정(harman's single factor test)을 통해 확인할 수 있다. Harmen의 단일 요인 검정은 SPSS를 이용한 탐색적 요인분석(exploratory factor analysis)에서 고유치(eigen value)가 1 이상인 요인이 한 개만 도출될 경우 또는 여러 개의 요인이 도출된다 하더라도 분산 설명력이 한 요인에만 절대적으로 나타나면 동일방법편의가 존재한다고 설명할 수 있다(백상용, 2012).

동일방법편의 검증을 위한 <표 6>의 분석결과를 보면 연구모형에 포함된 모든 요인들에 대한 분석 결과 고유치가 1 이상인 요인이 6개가 추출되었으며 첫 번째 요인에 대한 전체 분산이 27.878%만을 설명하고 있기 때문에 동일방법편의로 인한 문제가 없는 것으로 설명할 수 있다.

Ⅴ. 연구결과

5.1 측정모형에 대한 신뢰성 분석

본 연구에서는 먼저 측정모형을 분석하기 위한 신뢰도(reliability) 평가와 타당성(validity) 평가를 실시하였으며 다음으로 연구모형의 적합도와 구성개념들 간의 경로 분석을 위한 연구모형 분석을 실시하였다. 측정모형에 대한 신뢰성 분석은 설문문항들이 적절한지를 알아보기

<표 8> 측정모형에 대한 신뢰성과 판별 타당성 분석

구성개념	AVE	C.R.	α	Ben	Conc	Cont	Dis	Int	Ris
Ben	0.695	0.872	0.780	**0.834**					
Conc	0.874	0.954	0.928	0.035	**0.935**				
Cont	0.871	0.953	0.926	0.230	-0.166	**0.933**			
Dis	0.764	0.907	0.846	0.109	0.592	0.024	**0.874**		
Int	0.857	0.947	0.917	0.270	-0.159	0.116	-0.100	**0.926**	
Ris	0.814	0.929	0.886	0.053	0.667	-0.139	0.390	-0.129	**0.902**

대각선상의 수치는 AVE의 제곱근을 의미함

위한 절차로 연구모형에 포함된 구성개념들을 반복적으로 측정하더라도 측정값이 모두 동일한 결과로 나타나야 한다. 측정모형에 대한 신뢰성 평가 결과 <표 8>에서처럼 크론바흐 알파(cronbach's α)값과 합성 신뢰도(composite reliability)값이 0.7 이상으로 나타났고 평균분산추출(average variance extracted)값이 0.5 이상으로 나타나 신뢰성을 확보한 것으로 판단할 수 있다.

5.2 측정모형에 대한 타당성 분석

타당성 분석은 조사자가 측정하고자 하는 구성개념이 얼마나 정확히 측정되었는지를 알아보기 위한 절차로 집중 타당성과 판별 타당성으로 구분하여 측정한다. 집중 타당성은 측정변수들의 요인 적재값(factor loading)이 0.5 이상이면 집중 타당성이 있는 것으로 평가할 수 있으며 판별 타당성은 평균분산추출값의 제곱근값이 구성개념들 간의 상관계수 보다 크면 판별 타당성이 있는 것으로 평가할 수 있다(Fornell &Larcker, 1981).

측정모형에 대한 집중 타당성 평가를 보면 <표 7>에서처럼 모든 구성개념들에 대한 요인 적재량이 기준값인 0.7 이상으로 나타나 집중 타당성을 확보한 것으로 판단할 수 있으며 판별 타당성 평가는 <표 8>에서처럼 평균분산추출값의 제곱근값이 각 구성개념들 간의 상관계수 보다 크게 나타나 판별 타당성을 확보한 것으로 판단할 수 있다.

5.3 연구모형에 대한 평가

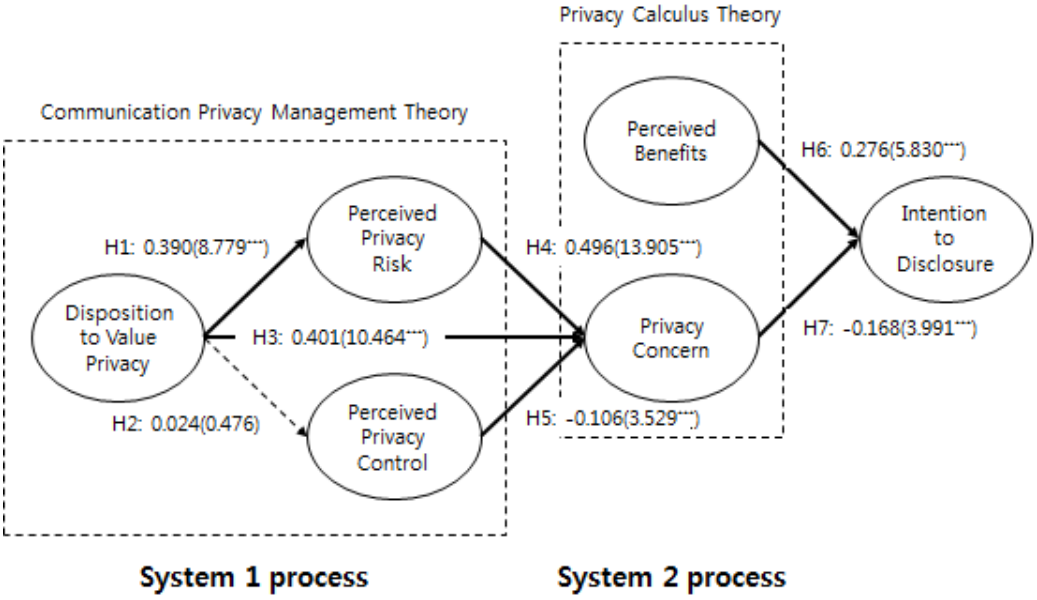
연구모형에 대한 적합도는 연구모형의 통계 추정량을 나타내는 Redundancy 값과 내생변수의 R^2 값 그리고 전체 적합도(goodness of fit)를 통해 평가할 수 있다(Tenenhaus et al., 2005). Redundancy 값이 양수이면 적합도가 있는 것으로 평가할 수 있으며(Chin, 1998) 각 구성개념들의 R^2 값이 0.26 이상이면 적합도를 '상'으로, 0.26~0.13 이상이면 적합도를 '중'으로 0.13~0.02 이상이면 적합도를 '하'로 평가할 수 있다(Cohen, 1988). <표 9>를 보면 연구모형의 적합도가 전체적으로 양호한 것으로 평가할 수 있다.

<표 9> 연구모형의 적합도 분석

구성개념	R^2	Redundancy	Communality
Dis			0.764
Ris	0.152	0.123	0.814
Cont	0.001	0.000	0.871
Conc	0.586	0.021	0.874
Ben			0.695
Int	0.101	0.063	0.857
모형 적합도	$\sqrt{0.210 \times 0.813} = 0.413$		

또한 연구모형의 전체적인 적합도(goodness of fit)을 평가하기 위해서는 R^2의 평균값과 공통성(communality)의 평균값을 곱한 값의 제곱근 값으로 평가할 수 있는데 0.36 이상이면 적합도를 '상'으로, 0.36~0.25 이상이면 적합도를 '중'으로, 0.25~0.1 이상이면 적합도를 '하'로 평가할 수 있다(Tenenhaus et al., 2005). <표 9>를 보면 연구모형의 적합도가 전체적으로 양호한 것으로 평가할 수 있다.

연구모형의 경로 간 유의성 검정은 반복적으로 표본을 추출하여 t-값을 제시하는 부트스트랩핑(bootstrapping) 방식을 이용하여 1,000회



***p<0.01

<그림 2> 연구 결과

의 반복샘플(resamples) 추출을 통해 실시하였다(Chin, 1998). <그림 2>를 보면 연구모형의 각 경로 간 경로 계수값과 t-값을 제시하여 연구모형의 경로 간 유의성 검정을 평가하였다.

5.4 연구가설 검정

본 연구에서 제시된 가설에 대한 검정 결과는 <그림 2>와 같다. 먼저 프라이버시를 중요하게 인식하는 프라이버시 가치성향은 지각된 프라이버시 위험에 유의한 영향을 미치는 것으로 나타나(t-값=8.779, p<0.01) 가설 H1은 채택되었다. 이는 프라이버시 가치성향이 프라이버시 위험에 유의한 영향 미친다는 Xu et al.(2011)의 연구를 뒷받침해 주는 결과이다.

프라이버시 가치성향은 지각된 프라이버시 통제에 유의한 영향을 미치지 않는 것으로 나타나(t-값=0.476, p<0.01) 가설 H2는 채택되지 않았다. 이는 전자상거래 이용자를 대상으로 프라이버시 가치성향이 프라이버시 통제에 유의한 결과로 나타나지 않은 Xu et al.(2011)의 연구와 유사한 결과이다.

프라이버시 가치성향은 정보 프라이버시 염려에 유의한 영향을 미치는 것으로 나타나(t-값=10.464, p<0.01) 가설 H3는 채택되었다. 이는 프라이버시 가치성향이 프라이버시 염려에 유의한 영향을 미친다는 Xu et al.(2011)의 연구와 동일한 결과이다.

지각된 프라이버시 위험은 정보 프라이버시 염려에 유의한 영향을 미치는 것을 나타나(t-값=13.905, p<0.01) 가설 H4는 채택되었다. 이는 프라이버시 위험이 프라이버시 염려에 유의한

영향을 미친다는 Xu et al.(2011)의 연구와 동일한 결과를 보여준다.

지각된 프라이버시 통제는 정보 프라이버시 염려에 유의한 영향을 미치는 것을 나타나(t-값 =3.529, p<0.01) 가설 H5는 채택되었다. 이는 프라이버시 통제를 할 수 없는 경우에 프라이버시 염려가 발생한다는 Zhao et al.(2012)의 연구를 뒷받침해 주는 결과이다.

지각된 이득은 개인정보 공개의도에 유의한 영향을 미치는 것을 나타나(t-값=5.830, p<0.01) 가설 H6은 채택되었다. 이는 위치기반 정보를 제공함으로써 얻게 되는 이득을 위해 자신에 대한 정보 접근을 허용한다는 Xu et al.(2010), Zhao et al.(2012)의 연구와 개념적으로 유사한 결과를 보여준다.

정보 프라이버시 염려는 개인정보 공개의도에 유의한 영향을 미치는 것을 나타나(t-값=3.991, p<0.01) 가설 H7은 채택되었다. 이는 프라이버시에 대한 염려가 높을수록 전자상거래 업체와의 거래 및 Social Networking Sites에서 자신에 대한 정보 제공을 꺼린다는 Dinev and Hart(2006)와 Krasnova et al.(2012)의 연구를 뒷받침해 주는 결과이다. 아울러 가설 H7의 결과는 프라이버시 염려에도 불구하고 사람들은 자신의 위치 기반 정보를 제공한다는 Zhao et al.(2012)의 연구를 뒷받침해 주는 결과이기도 하다.

<표 10> 연구가설 검정 결과

가설	경로			경로계수	t-값
H1	Des	→	Ris	0.390	8.779***
H2	Des	→	Cont	0.024	0.476^{ns}
H3	Des	→	Conc	0.401	10.464***
H4	Ris	→	Conc	0.496	13.905***
H5	Cont	→	Conc	-0.106	3.529***
H6	Bne	→	Int	0.276	5.830***
H7	Conc	→	Int	-0.168	3.919***

***p<0.01

본 연구는 프라이버시 염려를 중심으로 프라이버시 염려가 형성되는 과정을 설명하고 있으며 또한 프라이버시 염려에도 불구하고 전자상거래 이용을 위해 자신의 개인정보를 제공하는 인터넷 사용자의 모순된 행동을 설명하고 있다.

본 연구가 프라이버시 염려라는 핵심요인을 중심으로 선행요인과 결과요인 간의 관계를 설명하고 있는 만큼 프라이버시 염려가 형성되는 것과 관련된 인터넷 사용자의 개인정보 유출 경험은 중요한 표본적 특성을 가진다고 설명할 수 있다(김상현 · 박현선, 2013). 이에 본 연구에서는 개인정보 유출 경험이 있는 그룹과 유출 경

<표 11> 그룹 간 경로 차이에 대한 유의성 분석

가설	경로			표준오차		경로계수		β경험무-β경험유	t-값	자유도
				경험무	경험유	경험무	경험유			
H1	Des	→	Ris	0.029	0.048	0.443	0.389	0.054	0.524^{ns}	206
H2	Des	→	Cont	0.040	0.048	0.393	0.016	0.377	3.683***	159
H3	Des	→	Conc	0.029	0.045	0.318	0.424	-0.106	1.097^{ns}	200
H4	Ris	→	Conc	0.026	0.043	0.537	0.471	0.054	0.524^{ns}	206
H5	Cont	→	Conc	0.030	0.033	0.022	-0.083	0.106	1.466^{ns}	144
H6	Bne	→	Int	0.037	0.054	0.245	0.306	-0.061	0.525^{ns}	191
H7	Conc	→	Int	0.061	0.047	-0.022	-0.163	0.140	1.352^{ns}	92

***p<0.01

험이 없는 그룹을 구분하여 동일 연구모형에 대한 경로 간 유의성을 비교하는 그룹 간 경로 차이 분석을 실시하였다.

그룹 간 경로 차이를 보기 위한 다중 그룹 분석은 동일한 연구모형에 대한 그룹별 경로계수 값과 표준오차 값을 통한 t-값과 자유도로 판단할 수 있다(Chin, 2000; Keil et al., 2000, Eberl, 2010). 먼저 그룹 간 경로 차이 분석을 위한 t-값은 그룹별 분석결과에서 도출한 그룹별 경로계수 값과 표준오차 값을 수식(1)에 대입함으로써 얻을 수 있다(Chin, 2000, Sarstedt et al., 2011)

$$t = \frac{\beta_{group1} - \beta_{group2}}{\left(\sqrt{\frac{(m-1)^2}{(m+n-2)} SE^2_{group1} + \frac{(n-1)^2}{(m+n-2)} SE^2_{group2}}\right)\left(\sqrt{\frac{1}{m} + \frac{1}{n}}\right)}$$

수식(1)

단, $\beta_{group1/2} =$ 그룹별 경로계수 값

$m =$ group1의 샘플 수

$n =$ group2의 샘플 수

$SE_{group1/2} =$ 그룹별 표준오차

또한 그룹 간 경로 차이 분석을 위한 자유도는 그룹별 분석결과에서 도출한 표준오차 값을 수식(2)에 대입함으로써 얻을 수 있다.

$$df = \frac{(SE^2_{group1} + SE^2_{group2})^2}{\frac{SE^2_{group1}}{m+1} + \frac{SE^2_{group2}}{n+1}} - 2 \qquad \text{수식(2)}$$

개인정보 유출 경험이 있는 그룹과 경험이 없는 그룹을 대상으로 그룹 간 경로 차이 분석을 실시한 결과 <표 11>과 같이 H2의 경로에서 유의한 차이가 있는 것으로 나타났다. 이는 개인정보 유출 경험 유무에 따라 웹사이트에 대한 프라이버시 통제를 다르게 인식한다는 것으로 해석할 수 있다.

즉 개인정보 유출 경험이 없는 사람은 웹사이트의 개인정보 유출 건에 대해 적절한 통제 경험을 가지고 있지 않기 때문에 웹사이트에 대한 프라이버시 통제가 어렵다고 인식하는 반면 개인정보 유출 경험이 있는 사람은 웹사이트의 개인정보 유출 건에 대해 적절한 통제 경험을 가지고 있기 때문에 웹사이트에 대한 프라이버시 통제 수준을 낮게 인식하지 않는 것으로 이해할 수 있다.

Ⅵ. 연구결론

6.1 연구결론

연구질문 1 : 프라이버시 염려는 프라이버시를 중요하게 생각하는 프라이버시 가치성향에서 비롯한 지각된 위험과 지각된 통제 수준을 통해 생성되는가?

본 연구에서는 전자상거래에서 프라이버시 염려에도 불구하고 자신의 개인정보를 전자상거래 업체에 제공하는 인터넷 사용자의 모순된 행동에 대하여 실증분석을 실시하였다. 이를 위해 본 연구에서는 커뮤니케이션 프라이버시 관리 이론에서 도출한 프라이버시 가치성향에 따른 지각된 프라이버시 위험과 지각된 프라이버시 통제를 구성개념으로 설정하고 프라이버시 계산 이론을 통해 도출한 프라이버시 염려와 지각된 이득에 따른 정보 제공 의도를 구성개념으로 설정하여 연구모형을 설계하였다.

그리고 설계된 연구모형을 실증분석하기 위해 설문조사를 통해 자료를 수집하였고 최종적으로 다음과 같은 연구 결과를 도출하였다. 먼저 프라이버시를 중요하게 인식하는 프라이버시 가치성향은 지각된 프라이버시 위험과 프라이버시 염려에는 유의한 영향을 미치는 것으로 나타났지만 지각된 프라이버시 통제에는 유의한 영향을 미치는 것으로 나타나지 않았다.

프라이버시 가치성향은 개인의 특성과 성격적 속성을 개념화한 것으로 타인에 대한 개인의 신뢰 형성 과정에서 신뢰자의 특성(Mayer et al. 1995)과 신뢰에 대한 성향(McKnight, 1998)이 중요한 역할을 하는 것과 같이 프라이버시 가치성향 또한 프라이버시 염려가 형성되는 과정을 설명하는데 중요한 역할을 한다(김상희・김종기, 2017).

다시 말해 상대방의 행동에 대한 긍정적인 기대감을 바탕으로 불확실한 상황 하에서 위험을 감수하며 상대방을 믿고자하는 개인의 의지로 신뢰를 개념화 할 수 있는 것처럼(McKnight et al., 2002) 자신의 사적 정보공간에 대한 경계를 개방할지 여부를 결정짓기 위해 개인정보를 제공해야 하는 상황에서 개인정보 유출을 억제하려는 개인의 의지로 프라이버시 가치성향을 설명할 수 있다.

개인의 사적 정보공간에 대한 경계가 프라이버시에 대한 개인의 가치성향에 따른 위험과 통제에 대한 인식에 의해 조정된다는 설명(Xu et al., 2011)과 같이 프라이버시 가치성향은 자신이 규정한 사적 정보공간에 대한 경계를 변화시킴으로써 발생할 수 있는 개인정보 유출 위험을 크게 인식하게 될 것이다. 이에 프라이버시 가치성향과 지각된 프라이버시 위험 간의 관계를 설정한 가설 H1에 대한 실증분석 결과가 유의하게 나타난 것을 확인할 수 있다.

아울러 프라이버시 가치성향이 높은 사람은 자신의 개인정보가 무단으로 수집되는 것, 안전하게 보호되지 않는 것, 본인의 동의 없이 2차적으로 사용되는 것, 제3자에게 판매되는 것과 관련(Malhotra et al., 2004; Smith et al., 1996)하여 자신의 개인정보가 부적절하게 사용되는 것에 대해 프라이버시 염려를 갖게 될 것이다. 따라서 프라이버시 가치성향과 프라이버시 염려 간의 관계를 설정한 H3에 대한 실증분석 결과가 유의하게 나타난 것을 확인할 수 있다.

하지만 프라이버시 가치성향이 높은 사람이 프라이버시 위험을 높게 인식하는 만큼 프라이버시 통제 수준을 낮게 인식할 것이라는 가설 H2는 실증분석 결과 유의하게 나타나지 않았다. 이는 정부의 강력한 개인정보 보호 규제와 함께 개인정보 침해건수가 감소하고 있는 추세를 반영하고 있는 것으로 판단된다.

예컨대 정부에서는 2014년 8월에 개정·시행된 개인정보보호법에 따라 주민등록번호 사용을 제한하도록 하고 있으며 이를 반영하여 한국인터넷진흥원은 인증기관과 함께 인터넷상에서 이용되고 있는 개인의 주민등록번호/I-PIN 인증 내역을 간편하게 확인할 수 있는 서비스를 제공하고 있다. 또는 2012년 8월부터 연 1회 이상 이용자의 개인정보 이용내역(수집/이용/제공/위탁사항)을 연 1회 이상 이메일 등을 통해 통지하도록 하고 있어 인터넷 사용자들로 하여금 자신의 개인정보가 통제되고 있음을 인식시켜 주고 있다. 또한 2016년 9월부터는 광고성 전화 시 개인정보 수집 출처를 의무・고지하도록 하고 있어 인터넷 사용자들이 지각하는 통제는 더

욱 높아질 것으로 판단된다.

연구질문 2 : 개인정보 제공과 관련된 인터넷 사용자의 행동은 프라이버시 염려와 상충된 지각된 이득에 의해 발생하는가?

프라이버시 염려는 전자상거래 업체에 대한 프라이버시 위험 수준을 높게 인식하는 것에 반해 프라이버시 통제 수준을 낮게 인식함으로 인해 형성된다는 것을 가설 H4와 H5에 대한 실증분석을 통해 확인하였다.

다음으로 프라이버시 염려는 전자상거래 업체를 통해 얻게 되는 이득과 상충된다는 것을 확인하였다. 개인정보 제공으로 프라이버시 침해 가능성을 인식하고 있음에도 불구하고 자신의 개인정보를 제공하는 인터넷 사용자의 모순된 행동은 프라이버시 염려와 지각된 이득 간의 이분법적 계산에서 비롯된 행동으로 가설 H6과 H7을 통한 실증분석 결과로 확인할 수 있다. 온라인 쇼핑고객에 대한 프라이버시의 금전적 가치를 조사한 Jupiter Research(2002)의 연구에 의하면 설문 응답자의 82%가 100불을 받는 대가로 새로운 쇼핑 사이트에 자신의 개인정보를 제공할 수 있다고 응답하였으며, 응답자의 36%는 5불을 할인해 주는 대가로 자신의 인터넷 검색 습관을 추적할 수 있도록 허락한다고 응답한 것으로 나타났다(Tsai et al., 2011).

이처럼 경제적 이득은 프라이버시 염려와 상충된 관계를 가지고 있는데 Smith et al.(2011)은 개인정보 제공의 대가로 얻게 되는 이득에 대해서 금융 보상(Xu et al. 2010), 개인화(Chellappa & Sin, 2005), 사회적 조정(Lu et al. 2004)과 같은 세 가지 유형으로 구분하고 있으며 이러한 경제적, 시간적, 관계적 이득을 얻기 위해 프라이버시 침해 염려에도 불구하고 인터넷 사용자는 자신의 개인정보를 전자상거래 업체에 기꺼이 제공하는 경제적 행동을 한다는 것이다.

연구질문 3 : 개인정보 유출 경험은 프라이버시 염려가 형성되는 과정에 유의한 영향을 미치는가?

마지막으로 본 연구에서는 프라이버시 염려를 핵심요인으로 설정하고 있는 만큼 설문 응답자의 개인정보 유출 경험을 중요한 표본적 특성으로 보고 개인정보 유출 경험이 있는 그룹과 경험이 없는 그룹을 대상으로 그룹 간 경로 차이 분석을 실시하였다. 분석결과 개인정보 유출 경험 유무에 따라 웹사이트에 대한 프라이버시

<표 12> 전자상거래 규모에 따른 개인정보 침해 건수

(단위: 조원, 건수)

구분	05년	06년	07년	08년	09년	10년	11년	12년	13년	14년	15년
전자상거래 총 거래액	358	413	516	630	672	824	999	1,146	1,204	-	-
증감률	14.0%	15.4%	24.9%	22.1%	6.7%	22.6%	21.2%	14.7%	5.1%	-	-
개인정보 침해 건수	18,206	23,333	25,965	39,811	35,167	54,832	122,215	166,801	177,736	158,900	152,151
증감률	3.6%	28.2%	11.3%	53.3%	-11.7%	55.9%	122.9%	36.5%	6.6%	-10.6%	-4.2%

전자상거래 및 사이버쇼핑 동향 및 개인정보침해신고센터 접수자료

통제 수준을 다르게 인식하는 것으로 나타났다.

즉 개인정보 유출 경험이 있는 사람은 웹사이트의 개인정보 유출 건과 관련하여 자신의 개인정보를 보호하기 위한 차원에서 또는 해당 문제에 대한 적절한 보상을 요구하기 위한 차원에서 프라이버시 보호행동을 하게 된다. 이러한 과정에서 인터넷 사용자는 개인정보 유출과 관련된 프라이버시 보호행동에 대한 경험을 갖게 되고 웹사이트에 대한 프라이버시 통제가 어느 정도 가능하다는 것을 인식하게 된다.

인터넷 상에서의 프라이버시 보호 반응에 대한 Son and Kim(2008)의 연구를 보면 인터넷 사용자들은 웹사이트가 자신의 개인정보를 잘못 처리하는 것을 발견할 경우 추가적인 개인정보 제공을 거부하거나 허위정보를 제공하거나 웹사이트에 저장된 자신의 개인정보를 삭제하도록 요구하거나 웹사이트에 대해 부정적인 입소문을 내거나 개인정보보호와 관련된 정부기관에 문제 해결을 요구하는 행동을 하게 된다.

이처럼 프라이버시 통제와 관련하여 인터넷 사용자들은 개인정보 보호를 성실히 이행하지 못하는 웹사이트에 대해 사적 행동 또는 공적 행동내지 소극적 행동 또는 적극적인 행동을 통해 해당 문제가 해결되도록 프라이버시 보호행동을 취한다. 예컨대 2011년 넥슨의 1,320만명, 네이트의 3,500만명 고객정보가 유출된 사건 이후로 계속되고 있는 개인정보 유출 사건은 정보통신망법의 개정, 특정 시설에 대해 정보보호 인증 의무화, 개인정보 유출 신고기관의 확대 등 다양한 정책적 지원으로 이어져 개인정보 보호 및 통제에 관한 인터넷 사용자의 프라이버시 보호행동을 유도해 왔다.

이러한 정부의 노력은 개인정보 보호 및 통제에 관한 사회적 인식을 변화시켰고 나아가 <표 12>와 같이 개인정보 침해 건수가 가장 많았던 2011년 이후 처음으로 개인정보 침해 건수가 감소되는 결과로 이어지게 되었다. 이처럼 개인정보 침해 건수가 감소될 수 있었던 것은 정부 정책의 강화, 기업의 투자 그리고 개인정보 보호 및 통제에 대한 인터넷 사용자의 인식 변화와 적극적인 대응으로 가능할 수 있었다.

6.2 연구 시사점 및 한계점

본 연구는 정보 프라이버시 계산 이론을 기반으로 프라이버시가 침해 염려에도 불구하고 자신의 개인정보를 제공하는 개인의 모순된 행동을 설명하고 커뮤니케이션 프라이버시 관리 이론을 기반으로 프라이버시 침해 염려를 갖게 되는 과정을 실증분석하였다.

글로벌 전자상거래의 시장 규모가 팽창해 가고 있는 요즘 인터넷 사용자와 전자상거래 업체 간에 발생하는 대리인 감시비용 및 확증비용이 전자상거래 업체에 집중되어 있는 현행 정책에 대한 변화의 필요성을 제기하고 있다는 점에서 학술적, 정책적 시사점을 가진다.

전자상거래 국내를 벗어나 더욱 글로벌화 되어가고 있고 전자상거래 규모가 금융 산업과 융합하면서 꾸준하게 확장되어 있는 요즘, 개인정보는 무조건적으로 보호되어야 하며 보호에 대한 책임은 개인정보를 수집·이용하는 전자상거래 업체에게 귀속된다는 기존의 정책적 관점이 국제 기준에 맞춰 보다 유연화할 필요성이 제기된다.

즉 개인정보 보호에 대한 책임 분배와 함께 그에 따른 시간적 · 금전적 비용에 대한 분배를

개인정보 제공과 이를 이용하는 전자상거래 업체, 서비스 제공과 이를 이용하는 인터넷 사용자의 관점이 모두 반영된 시각에서 보다 세분화할 필요성이 있으며 이를 위해 우선적으로 프라이버시 염려에도 불구하고 자신의 개인정보를 제공하는 인터넷 사용자들의 행동적 특성을 이해할 필요가 있다(Pavlou, 2011).

예컨대, 채팅룸이나 SNS(소셜 네트워킹 서비스)에 글을 게시함으로 인해, 특정 포럼에 자신의 이름과 이메일 주소 등을 게시함으로 인해 자신의 개인정보가 제3자에게 수집될 경우 개인정보 보호에 대한 책임은 전자상거래 업체가 지지 않다는 것이다.

또한 기업의 구조조정, 합병 또는 매각으로 인해 고객의 개인정보가 제3자에게 이전될 경우 기업은 고객의 개인정보를 이전할 수 있다는 것이다. 이는 전자상거래 업체와 고객 간에 서비스 이용 대가로 제공된 개인정보에 대해서 공동 소유물에 대한 소유권 이전의 관점에서 해석할 수 있는 것이다.

아울러 글로벌 기업이 다수의 법인을 두고 있음으로서 여러 국가에서 수집된 고객의 개인정보가 각기 다른 국가에서 이용될 경우 수집된 개인정보는 APEC(아시아 태평양 경제 협력체)의 CBPR(국경간 개인정보 규정)과 같은 국제 프라이버시 규칙에 따라 관리되어야 하여 이를 위해 프라이버시에 대한 개념을 보다 확대, 해석할 필요가 있다는 것이다.

이에 본 연구는 글로벌 전자상거래 시장에서 경쟁력을 확보하고 새로운 성장 동력으로서의 역할을 전자상거래가 선도할 수 있다는 관점에서 보다 유연한 정책적 변화의 필요성을 제기하며 이를 위해 정보 프라이버시에 대한 인터넷 사용자의 행동적 특성을 설명하고 실증분석 결과를 제시한다.

또한 본 연구는 개인정보 유출 경험이 있는 그룹과 유출 경험이 없는 그룹을 비교함으로써 두 그룹 간에 인식 차이가 존재하는지를 확인하였다. 웹사이트에 대한 프라이버시 통제 가능성에 대한 인식은 개인정보 유출과 관련된 프라이버시 보호행동을 경험함으로써 얻게 되는데 이는 개인정보 보호와 관련된 정부의 정책적 지원이 반드시 병행되어야만 가능하다.

즉 개인정보 유출 경험이 있는 그룹과 유출 경험이 없는 그룹 간 인식 차이가 존재한다는 것은 개인정보 보호와 관련된 정부의 정책적 지원이 어느 정도 실효성을 거두고 있다는 것을 이해할 수 있으며 이를 본 연구에서는 실증분석 결과를 통해 설명하고 있다.

마지막으로 본 연구는 다음 같은 한계점을 가지고 있다. 첫째, 프라이버시에 대한 선행 연구에서는 성명, 나이, 이전 경험 등과 같은 구성개념들이 프라이버시 염려나 개인정보 제공에 관한 행동에 잠재적으로 영향을 미칠 수 있다고 설명하고 있다. 즉 설계한 연구모형을 실증분석하는 과정에서 성명, 나이, 경험 등과 같은 인구통계학적 변수들이 포함될 경우 종속변수와 독립변수 간의 순수한 영향력을 확인하기가 어렵게 되며 이러한 경우 성명, 나이, 경험 등과 같은 잡음 인자(nuisance factor)를 통제하기 위해 이를 통제 변수로 설정하고 연구모형에 포함할 필요가 있다.

이에 향후 연구에서는 연구 대상을 보다 확대하여 성명(Sheehan, 1999), 나이(Culnan, 1995), 프라이버시에 경험(Smith et al., 1996)을 통제 변수로 설정하고 종속변수인 정보 제공 의도에

유의한 영향을 미치는지를 확인할 필요가 있다. 아울러 최근 Amazon.com과 같은 해외 전자상거래를 이용하는 인터넷 사용자가 급증하는 것과 핀테크(fintech)의 확산으로 모바일 금융 거래를 이용하는 인터넷 사용자가 급증하는 것과 관련하여 향후 연구에서는 연구 대상의 범위를 보다 확장할 필요성이 있다고 판단된다.

둘째, 본 연구는 프라이버시 염려가 형성되는 과정을 설명함과 동시에 프라이버시가 염려에도 불구하고 자신의 개인정보를 제공하는 개인의 모순된 행동을 설명하고 있다. 그리고 이러한 일련의 과정을 이중 프로세스 이론을 기반으로 연구모형을 설계하고 실증분석하였다. 즉 개인정보 제공과 관련된 인터넷 사용자의 행동은 프라이버시 위험에 대한 감정적이고 직감적인 판단에 따른 프라이버시 염려와 웹사이트가 제공하는 이득에 대한 분석적이고 계산적인 판단을 통해 결정된다는 것이다.

하지만 이중 프로세스 이론을 통해 프라이버시와 관련된 인간의 행동을 설명하고 이를 모형으로 구체화하기 위해서는 우선적으로 개인정보 제공 의도와 실질적인 행동 간에 유의한 차이가 있는지를 확인할 필요가 있다. 이는 최근 프라이버시 연구 분야에서 태도와 행동 간에 일관성이 존재하는지에 대한 논의에서 비롯한 행동 경제학적 관점이 주목을 받고 있기 때문이다(김종기 · 김상희, 2015). 이에 향후 연구에서는 개인정보 제공과 관련된 인터넷 사용자의 태도와 실제 행동 간에 일관성이 존재하는지를 보기 위한 연구 설계와 이를 실증분석하기 위한 실험적 연구가 진행될 필요성이 있다고 판단된다.

참고문헌

김상현, 박현선, “프라이버시 보호인식 및 보호행동의도에 미치는 영향 요인과 프라이버시 침해경험의 조절효과에 관한 연구,” 인터넷전자상거래연구, 제13권, 제4호, 2013, pp. 79-105.

김상희, “정보제공의도와 실제 정보제공행동 간의 프라이버시 역설에 대한 연구,” 부산대학교 박사학위 논문, 2015

김상희, 김종기, “프라이버시 염려와 제도적 신뢰가 프라이버시 의사결정에 미치는 영향-전자상거래와 위치기반서비스의 비교,” 한국산업정보학회지, 제22권, 제1호, 2017, pp. 69-87.

김종기, 김상희, “스마트폰 위치기반서비스에서 정보제공의도: 프라이버시 계산 관점을 중심으로,” 정보시스템연구, 제21권, 제4호, 2012, pp. 55-79.

김종기, 김상희, “행동경제학 관점에서 프라이버시 역설에 관한 연구,” 정보화정책, Vol. 22, No. 3, 2015, pp. 16-35.

민진영, 김범수, “프라이버시 계산 모형을 적용한 SNS 지속 사용 의도에 대한 연구: 페이스북과 카카오톡 사례 중심으로,” Information Systems Review, Vol. 15, No. 1, 2013, pp. 105-122.

백상용, “한국 TAM 실증연구의 동일방법편의 분석,” 정보시스템연구, 제21권, 제1호, 2012, pp. 1-17.

유일, 신정신, 이경근, 최혁라, “프라이버시 염려 영향요인이 인터넷 사용자의 신뢰와 온라인 거래의도에 미치는 영향,” Journal

of Information Technology Applications and Management, Vol. 15, No. 4, 2008, pp. 37-59.

이동주, 방영석, 배윤수, "온라인상의 개인정보 제공에 있어서 정보 투명성의 역할 -프라이버시 계산 모형을 중심으로-," 정보화정책, 제17권, 제2호, 2010년, pp. 68-85.

통계청, 전자상거래 및 사이버쇼핑 동향, 2014.

통계청, 2016년 8월 온라인쇼핑 동향, 2016.

한국인터넷진흥원, 대국민 정보프라이버시 성향 분석을 위한 도구개발, 2009.

한국인터넷진흥원, 정보통신서비스 제공자를 위한 개인정보보호 법령 해설서, 2012.

한국정보보호진흥원, 개인정보의 경제적 가치 분석에 관한 고찰, 2007.

행정자치부고시, 개인정보의 안전성 확보조치 기준, 2016.

Acquisti, A. and Gross, R., "Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook," *PET'06 Proceeding of the 6th Intenational Conference on Privacy Enhancing Technologies*, 2006, pp. 36- 58.

Acquisti, A. and Grossklags, J., "Privacy and Rationality in Individual Decision Making," *IEEE Security and Privacy*, Vol. 3, No. 1, 2005, pp. 26-33.

Ajzen, I., "The Theory of Planned Behavior," *Organizational Behavior and Human Decision Processes*, Vol. 50, Iss. 2, 1991, pp. 179-211

Altman, I., The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding, Monterey, CA: Brooks/Cole Publishing, 1975.

Awad, N. F. and Krishnan, M. S., "The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to be Profiled Online for Personalization," *MIS Quarterly*, Vol. 30, Iss. 1, 2006, pp. 13-28.

Barbey, A. K., and Sloman, S. A., "Base-rate Respect: From Ecological Validity to Dual Processes," *Behavioral and Brain Sciences*, Vol. 30, Iss. 3, 2007, 241–297.

Bauer, R. A., "Consumer Behavior as Risk Taking," In *Dynamic Marketing for a Changing World*, Hancock, R. S. (ed.), American Marketing Association, Chicago, 1960, pp. 389-398.

Bellman, S., Johnson, E. J., Kobrin, S. J. and Lohse, G., "International Differences in Information Privacy Concerns: A Global Survey of Consumers," *Information Society*, Vol. 20, No. 5, 2004, pp. 313-324.

Buchanan, T., Paine, C., Joinson, A. N. and Reips, U., "Development of Measures of Online Privacy Concern and Protection for Use on the Internet," *Journal of the American Society for Information Science and Technology*, Vol. 58, Iss. 2, 2007, pp. 157-165.

Campbell, J. E. and Carlson, M., "Panopticon.

com: Online Surveillance and the Commodification of Privacy," *Journal of Broadcasting & Electronic Media*, Vol. 46, No. 4, 2002, pp. 586-606.

Chellappa, R. K. and Sin, R., "Personalization Versus Privacy: An Empirical Examination of the Online Consumer's Dilemma," *Information Technology and Management*, Vol. 6, Iss. 2, 2005, pp. 181-202.

Chin, W. W., "The Partial Least Squares Approach to Structural Equation Modeling," In *Modern Methods for Business Research*, Marcoulides, G. A. (ed.), 1998, pp. 295-336. New Jersey: Lawrence Erlbaum.

Chin, W. W., *Frequently Asked Questions: Partial Least Squares & PLS-Graph*, http://disc-nt.cba.uh.edu/chin/plsfaq.htm, 2000.

Cohen, J. O., *Statistical Power Analysis for the Behavioral Sciences (2nd ed.)*, Hillsdale, New Jersey: Lawrence Erlbaum Associates, 1988.

Culnan, M. J., "Consumer Awareness of Name Removal Procedures: Implication for Direct Marketing," *Journal of Interactive Marketing*, Vol. 9, Iss. 2, 1995, pp. 10-19.

Culnan, M. J., "Protecting Privacy Online: Is Self-Regulation Working?," *Journal of Public Policy & Marketing*, Vol. 19, No. 1, 2000, pp. 20–26.

Culnan, M. J. and Bies, J. R. "Consumer Privacy: Balancing Economic and Justice Considerations," *Journal of Social Issues*, Vol. 59, No. 2, 2003, pp 323-342.

Cunningham, S. M., *The Major Dimension of Perceived Risk : Risk Taking and in Formation Handling in Consumer Behavior*, Harvard University Press, Boston, 1967.

Davis, F. D., Bagozzi, R. P. and Warshaw, P. R., "User Acceptance of Computer Technology: A Comparison of Two Theoretical Models," *Management Science*, Vol. 35, No. 8, 1989, pp. 982-1003.

Dienes, Z., & Perner, J., "A Theory of Implicit and Explicit Knowledge," *Behavioral and Brain Sciences*, Vol. 22, Iss. 5, 1999, pp. 735–808.

Dinev, T. and Hart, P., "An Extended Privacy Calculus Model for E-Commerce Transactions," *Information Systems Research*, Vol. 17, No. 1, 2006, pp. 61-80.

Dinev, T., Hart, P. and Mullen, M. R., "Internet Privacy Concerns and Beliefs about Government Surveillance-An Empirical Investigation," *The Journal of Strategic Information System*, Vol. 17, Iss. 3, 2008, pp. 214-233.

Eberl, M., "An Application of PLS in Multy-Group Analysis: The Need for Differentiated Corporate Level Marketing in the Mobile Communications Industry," In *Handbook of Partial Least Squares:*

Concepts, Methods and Application, Esposito Vinzi, V., W. W., Chin, J., Henseler and H., Wang (eds.), Berlin, Springer, pp. 655-690, 2010.

Evans, J. St. B. T., "Dual-processing Accounts of Reasoning, Judgment and Social Cognition," *Annual Review of Psychology*, Vol. 59, Iss. 1, 2008, pp. 255–278.

Fornell, C. and Larcker, D. F., "Evaluating Structural Equation Models with Unobservable Variables and Measurement Error," *Journal of Marketing Research*, Vol. 18, No. 1, 1981, pp. 39-50.

Garfinkel, S., *Database Nation: The Death of Privacy in the 21st Century*, Sebastopol, CA: O'Reilly, 2000.

Goes, P. B., "Editor's Comments: Information Systems Research and Behavioral Economics," *MIS Quarterly*, Vol. 37, No. 3, 2013, pp. iii-viii.

Javenpaa, S. L., Tracinsky, M. and Vitale, M, "Consumer Trust in An Internet Store," *Information Technology and Management*, Vol. 1, Iss. 1, 2000, pp. 45-71.

Jupiter Research, *Seventy Percent of US Consumers Worry about Online Privacy, But Few Take Protective Action*, Press Release, 2002.

Kahneman, D., *Thinking, Fast and Slow*, The New York Review of Books, 2011.

Keil, M., Tan, B. C. Y., Wei, K. K., Saarinen, T., Tuunainen, V. and Wassenaar, A., "A Cross-cultural Study on Escalation of Commitment Behavior in Software Projects," *MIS Quarterly*, Vol. 24, No. 2, pp. 299-325, 2000.

Kobsa, A. and Teltzrow, M., "Contextualized Communication of Privacy Practices and Personalization Benefits: Impacts on Users' Data Sharing Behavior," In *Privacy Enhancing Technologies*, Springer Verlag, Martin, D. and Serjantov, A. (eds.) Heidelberg, Germany, 2005, pp. 329-343, DOI 10.1007/11423409_21.

Krasnova, H., Veltri, N. F. and Gunther, O., "Self-disclosure and Privacy Calculus on Social Networking Sites: The Role of Culture," *Business & Information Systems Engineering*, Vol. 4, Iss. 3, 2012, pp. 127-135.

Li, H., Sarathy, R. and Xu, H., "Understanding Situational Online Information Disclosure as a Privacy Calculus," *Journal of Computer Information Systems*, Vol. 51, Iss. 1, 2010, pp. 62

Li, Y., "Theories in Online Information Privacy Research: A Critical Review and An Integrated Framework," *Decision Support Systems*, Vol. 54, Iss. 1, 2012, pp. 471-481.

Lu, Y., Tan, B. C. Y. and Hui, K.-L., "Inducing Customers to Disclose Personal Information to Internet Businesses with Social Adjustment Benefits," In *Proceedings of 25th International*

Conference on Information Systems, Agarwal, R., Kirsch, L. J. and DeGross, J. I. (eds.), Washington, DC, 2004, pp. 272-281.

Malhotra, N. K., Kim, S. S. and Agarwal, J., "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.

Mayer, R. C., Davis, J. H., and Schoorman, F. D., "An Integrative Model of Organizational Trust," *The Academy of Management Review*, Vol. 20, No. 3, 1995, pp. 709-734.

McKnight, D. H., Cummings, L. I. and Chervany, N. I., "Initial Trust Formation in New Organisational Relationships," *Academy of Management Review*, Vol. 23 No. 3, 1998, pp. 473-90.

McKnight, D. H., Choudbury, V. and Kacmar, C., "Developing and Validating Trust Measures for Ecommerce: An Integrative Typology," *Information Systems Research*, Vol. 13 No. 3, 2002, pp. 334-61.

Metzger, M. J., "Communication Privacy Management in Electronic Commerce," *Journal of Computer-Mediated Communication*, Vol. 12, Iss. 2, 2007, pp. 335–361.

Moon, Y., "Intimate Exchanges: Using Computers to Elicit Self-Disclosure From Consumers," *Journal of Consumer Research*, Vol. 26, No. 4, 2000, pp. 323-339.

Norberg, P. A., Horne, D. R. and Horne, D. A., "The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors," *Journal of Consumer Affairs*, Vol. 41, Iss. 1, 2007, pp. 100–126.

Nowak, G. and Phelps, J., "Understanding Privacy Concerns: An Assessment of Consumer Information-Related Knowledge and Beliefs," *Journal of Direct Marketing*, Vol. 6, No. 4, 1992. pp 28-39.

Pavlou, P. A., "State of the Information Privacy Literature: Where Are We Now and Where Should We Go?," *MIS Quarterly*, Vol. 35, Iss. 4, 2011, pp. 977-988.

Pavlou, P. A. and Gefen, D. "Building Effective Online Marketplaces with Institution-based Trust," *Information Systems Research*, Vol. 15, Iss. 1, 2004, pp. 37-59.

Petronio, S. S., *Boundaries of Privacy: Dialectics of Disclosure (xix, pp. 268). Albany*, NY: State University of New York Press, 2002.

Podsakoff, P. M., MacKenzie, S. B., Lee, J. Y. and Podsakoff, N. P., "Common Method Biases in Behavioral Research: A Critical Review of the Literature and Recommended Remedies," *Journal of Applied Psychology*, Vol. 88, No. 5, 2003, pp. 879–903.

Sarstedt, M., Henseler, J. and Ringle, C. M.

"Multi-Group Analysis in Partial Least Squares (PLS) Path Modeling: Alternative Methods and Empirical Results," *Advances in International Marketing*, Vol. 22, pp. 195-218, 2011.

Schoeman, F. D., *Philosophical Dimensions of Privacy: An Anthology*, New York: Cambridge University Press, 1984.

Sheehan, K. B. "An Investigation of Gender Differences in On-line Privacy Concerns and Resultant Behaviors," *Journal of Interactive Marketing*, Vol. 13, Iss. 4, 1999, pp. 24-38.

Sloman, S. A. "The Empirical Case for Two Systems of Reasoning," *Psychological Bulletin*, Vol. 119, No. 1, 1996, pp. 3-22.

Slyke, C. V., Shim, J. T., Johnson, R. and Jiang, J. J., "Concern for Information Privacy and Online Consumer Purchasing," *Journal of the Association for Information Systems*, Vol. 7, Iss. 6, 2006, pp. 415-444.

Smith, H. J., Dinev, T. and Xu, H., "Information Privacy Research: An Interdisciplinary Review," *MIS Quarterly*, Vol. 35, Iss. 4, 2011, pp. 989-1016.

Smith, H. J., Milberg, S. J. and Burke, S. J., "Information Privacy: Measuring Individuals' Concerns about Organizational Practices," *MIS Quarterly*, Vol. 20, Iss. 2, 1996, pp. 167-196.

Stanovich, K. E., West, R. F. and Toplak, M. E., "The Complexity of Developmental Predictions from Dual Process Models," *Developmental Review*, Vol. 31, Iss. 2-3, 2011, pp. 103–108.

Stewart, K. A. and Segars, A. H., "An Empirical Examination of the Concern for Information Privacy Instrument," *Information Systems Research*, Vol. 13, No, 1, 2002, pp. 36-49.

Sun, R., Slusarz, P. and Terry, C., "The Interaction of the Explicit and the Implicit in Skill Learning: A Dual-Process Approach," *Psychological Review*, Vol. 112, No. 1, 2005, pp. 159–192.

Son, J. Y. & Kim, S. S., "Internet Users' Information Privacy-Protective Responses: A Taxonomy and a Nomological Model," *MIS Quarterly*, Vol. 32, No. 3, 2008, pp. 503-529.

Tenenhaus, M., Vinzi, V. E., Chatelin, Y. M. and Lauro, C., "PLS Path Modeling," *Computational Statistics & Data Analysis*, Vol. 48, No. 1, 2005, pp. 159-205.

Tsai, J. Y., Egelman, S., Cranor, L. and Acquisti, A., "The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study," *Information System Research*, Vol. 22, Iss. 2, 2011, pp. 254-268.

Venkatesh, V. and Bala, H., "Technology Acceptance Model 3 and a Research Agenda on Interventions," *Decision Sciences*, Vol. 39, Iss. 2, 2008, pp.

273~315.

Warren, S. D. and Brandeis, D. L., “The Right to Privacy,” *Harvard Law Review*, Vol. 4, No. 5, 1890, pp. 193-220.

Wason, P. C. and Evans, J. St. B. T., “Dual Processes in Reasoning?,” *Cognition*, Vol. 3, Iss. 2, 1975, pp. 141-154.

Xu, H., Dinev, T., Smith, H. J. and Hart, P., “Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances,” *Journal of the Association for Information Systems*, Vol. 12, Iss. 12, 2011, pp. 798-824.

Xu, H. and Teo, H. H. “Alleviating Consumer's Privacy Concern in Location-based Services: A Psychological Control Perspective,” *Proceedings of the 25th Annual International Conference on Information Systems*, Washington, D. C., United States, 2004, pp. 793-806.

Xu, H., Teo, H. H., Tan, B. C. Y. and Agarwal, R., “The Role of Push-Pull Technology in Privacy Calculus: The Case of Location-Based Services,” *Journal of Management Information Systems*, Vol. 26, Iss. 3, 2010, pp. 135-174.

Zhao, L., Lu, Y. and Gupta, S., “Disclosure Intention of Location-Related Information in Location-Based Social Network Services,” *International Journal of Electronic Commerce*, Vol. 16, No. 4, 2012, pp. 53-89.

김 진 성 (Kim, Jinsung)

부산대학교 경영학과에서 박사학위를 취득하고 현재 부산대학교 경영연구소에서 전임연구원으로 재직 중이다. 주요 관심분야는 정보보안관리, 정보시스템 감사, 개인정보보호, 전자상거래, 기술경영 등이다.

김 종 기 (Kim, Jongki)

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.

<Abstract>

A Study on the Internet User's Economic Behavior of Provision of Personal Information: Focused on the Privacy Calculus, CPM Theory

Jinsung Kim · Jongki Kim

Purpose

The purpose of this study is to deduct the factors for explaining the economic behavior of an Internet user who provides personal information notwithstanding the concern about an invasion of privacy based on the Information Privacy Calculus Theory and Communication Privacy Management Theory.

Design/methodology/approach

This study made a design of the research model by integrating the factors deducted from the computation theory of information privacy with the factors deducted from the management theory of communication privacy on the basis of the Dual-Process Theory. In addition, this study, did empirical analysis of the path difference between groups by dividing Internet users into a group having experience in personal information spill and another group having no experience.

Findings

According to the empirical analysis result, this study confirmed that the Privacy Concern about forms through the Perceived Privacy Risk derived from the Disposition to value Privacy. In addition, this study confirmed that the behavior of an Internet user involved in personal information offering occurs due to the Perceived Benefits contradicting the Privacy Concern.

Keyword: Dual-Process Theory, Communication Privacy Management Theory, Privacy Calculus Theory, Privacy Concern, Privacy Risk, Privacy Control

* 이 논문은 2017년 2월 8일 접수, 2017년 3월 14일 1차 심사, 2017년 3월 28일 게재 확정되었습니다.