http://dx.doi.org/10.15813/kmr.2017.18.3.003

빅데이터 환경 형성에 따른 데이터 감시 위협과 온라인 프라이버시 보호 활동의 관계에 대한 연구[1]

A Study of Relationship between Dataveillance and Online Privacy Protection Behavior under the Advent of Big Data Environment

박 민 정 (mjpark67@ewhain.net) 이화여자대학교 경영학과 박사과정
채 상 미 (smchai@ewha.ac.kr) 이화여자대학교 경영학과 부교수[2]

Abstract

Big Data environment is established by accumulating vast amounts of data as users continuously share and provide personal information in online environment. Accordingly, the more data is accumulated in online environment, the more data is accessible easily by third parties without users' permissions compared to the past. By utilizing strategies based on data-driven, firms recently make it possible to predict customers' preferences and consuming propensity relatively exactly. This Big Data environment, on the other hand, establishes 'Dataveillance' which means anybody can watch or control users' behaviors by using data itself which is stored online. Main objective of this study is to identify the relationship between Dataveillance and users' online privacy protection behaviors. To achieve it, we first investigate perceived online service efficiency; loss of control on privacy; offline surveillance; necessity of regulation influences on users' perceived threats which is generated by Dataveillance.

Keywords: big data, dataveillance, data surveillance, online protection behavior

1. 서론

빅데이터 시대의 등장과 IT 기술의 발전은 자동화된 방법으로 이전보다 많은 사용자의 개인정보를 쉽고 빠르게 처리할 수 있는 환경을 형성하였다(Hasan and Hyland 2001; Stelzner 2010). 이에 따라 기업은 보유한 방대한 양의 고객 데이터를 바탕으로 고객의 취향과 선호도는 물론 사용자간의 관계 정보까지 정확히 파악할 수 있게 되었다. 나아가 스마트폰에 저장된 개인의 수면시간, 건강상태, 위치정보 등의 단편적인 데이터를 조합하여 사용자에게 맞춤형 라이프 스타일을 추천해 주는 서비스의 등장은 데이터의 조합만으로도 개인의 구체적인 신상 확인(re-identification)까지가 오늘날 가능해졌음을 암시한다(Kang et al. 2011).

[1] 논문접수일: 2017년 5월 24일; 1차 수정: 2017년 7월 31일
[2] 교신저자

인텔에서 실시한 설문조사의 결과에 따르면 사용자들은 개인의 동의 없는 검색 이력, 현재 위치 등의 정보를 수집하여 보관하는 기업의 활동에 불쾌감을 느낀다고 응답하였다(Intel 2014). 응답자들은 모두 공공의 목적을 지니는 의료 연구 및 정책 개발 활동에는 개인정보를 제공할 의사가 있지만 개인식별이 불가능한 상태의 전제 조건이 형성되었을 때만 제공하겠다고 밝혔다. 이는 개인이 제공한 데이터를 바탕으로 기업이 사용자 행태 추적 및 개인식별이 가능해짐에 따라 사용자는 이에 대한 두려움을 인지하게 되었다는 것을 의미한다(Clarke 1997). 또한 사용자는 기업의 과도한 개인정보 수집 및 관리 소홀에 대한 두려움과 낯선 기업의 개인정보 보유 가능성에 대한 염려를 체감하게 되었다(Chellappa and Pavlou 2002).

국가가 수집 및 보유한 국민의 개인정보를 바탕으로 이들의 행동을 감시와 통제한다는 '빅브라더(Big Brother)' 와 개인은 항상 감시 받고 있는 듯한 착각의 두려움을 형성하는 공간의 '판옵티콘(Panopticon)' 이 오늘날 '빅데이터 감시 사회'의 형태로 재등장하였다. 이는 서버 혹은 네트워크를 통해 사람들의 실제 행동이 아닌 데이터로 추적하여 개인을 감시하거나 데이터를 활용한 정보 분석의 결과로 사용자를 통제한다는 '데이터 감시(dataveillance)'를 발생시켰다(Clarke 1988). 사용자는 개인정보를 온라인 상에 제공함에 따라 데이터 감시 사회를 형성하는 주체자인 동시에 스스로 형성한 감시 체제로 인하여 두려움과 불안함을 인지하는 피해자가 되는 모순적 역할에 오늘날 놓이게 되었다.

사용자는 데이터로 인하여 감시 및 통제 받는 듯한 느낌의 데이터 감시를 경험함에 따라 두려움과 불안함 등을 인지한다. 이에 따라 본 연구에서는 보호동기이론(PMT, Protection Motivation Theory)을 바탕으로 사용자가 온라인 환경에서 인지하는 1) 온라인 서비스의 효율성, 2) 프라이버시 통제 능력 상실, 3) 오프라인 환경에서의 감시 위협 정도, 4) 프라이버시 보호 규제의 필요성에 따른 개인의 데이터 감시 위협의 지각 정도를 우선적으로 파악하고자 한다. 이를 바탕으로 사용자가 인지하는 데이터 감시 위협의 변화가 개인의 프라이버시 보호 활동 의도에 미치는 영향을 최종적으로 밝힌다. 이를 통하여 도출된 본 연구의 결과는 향후, 기업의 정보 수집 과정에서 고객이 인지하는 데이터 감시의 두려움을 감소시킬 수 있는 방안 마련의 필요성을 제공한다. 또한 본 연구는 기존의 프라이버시 침해, 개인정보 유출 등의 제한된 정보보호 분야의 연구 범위를 확장시키며 빅데이터 환경 등장에 따라 나타난 데이터 감시라는 사회적 문제를 다룸에 따라 관련 연구 분야의 토대가 된다.

2. 문헌 연구

2.1 보호동기이론(Protection Motivation Theory)

보호동기이론(PMT, Protection Motivation Theory)은 기대가치이론(Expectancy-Value Theory)과 인지적 정보처리이론(Cognitive Processing Theory)을 기반으로 개인의 공포소구(Fear Appeal)에 따른 태도와 행동적 변화과정을 설명하는 이론으로 보건학에서 시작되었다(Ifinedo 2012). 최근에는 정보보호 분야에서도 사용자의 정보보호 행동을 설명하고자 보호동기이론을 기반으로 한 연구가 활발하게 진행되고 있다(Chai et al, 2009; Herath and Rao 2009; Vance et al 2012).

보호동기이론은 인지된 위협으로부터 개인을 보호하기 위한 동기와 잠재적으로 예상되는 부정적 결과를 회피하기 위한 행동을 비용-이익(cost-benefit) 분석을 통해 설명한다. 즉, 개인은 특정 행동을 취할 때 기대되는 이익과 동시에 예상되는 비용을 고려하여 예방

적 행동을 하게 된다(Rogers 1975). 본 연구에서는 사용자가 온라인 서비스를 이용함에 따라 획득하는 이익을 '인지된 온라인 서비스의 효율성(Perceived Online Service Efficiency)'으로 조작적 정의하여 이에 따른 개인의 데이터 감시 위협에 대한 체감 변화를 살펴본다. 또한 본 연구에서는 위협으로부터 발생하는 잠재적인 손실의 방지 및 대처 능력에 대한 개인의 확신 정도인 자기 효능감(Self-Efficacy)(Maddux and Rogers 1983)이 상실된 개인의 인지 상태로 접근하였다. 즉, 위협적인 상황에 대하여 개인이 주체적으로 대처하고 방지할 수 있는 능력에 대한 불확신 상태를 의미하는 것으로 본 연구에서는 이를 '프라이버시 통제 능력의 상실(Perceived Loss of Control on Privacy)'로 제한하였다. 또한 위협적인 사건에 의하여 개인이 평가하는 피해의 심각 정도(Ifinedo 2012)를 나타내는 인지된 심각성(Perceived Severity)은 개인의 '인지된 오프라인 감시 위협(Perceived Offline Surveillance)'으로 본 연구에서는 설정하였다. 이는 개인은 자신이 인지하는 사고, 신념 등의 심리적 요소들을 동일하게 유지하려는 상태를 추구하게 됨에 따라 개인의 심리가 일관성 있게 유지된다는 인지 일관성 이론(Theory of Cognitive Consistency)을 바탕으로 한다(Heider 1946). 즉, 개인이 오프라인 환경에서 느끼는 감시 위협에 대한 두려움 등의 감정 상태는 온라인 환경까지 유지되어 이는 인지된 온라인의 감시 위협으로 까지 이어진다.

앞선 보호동기이론의 주요 요인 이외에 본 연구에서는 개인의 '인지된 프라이버시 관련 규제의 필요성(Perceived Necessity of Regulation)'을 추가하였다. 이는 최근 개인정보 중요성의 증가에 따른 각 국의 관련 법률 등 규제가 형성된 사회적 배경을 바탕으로 한다. 따라서 사용자가 체감하는 프라이버시 관련 규제의 설치 필요성이 개인이 인지하는 온라인 환경의 감시, 통제의 위협 정도에 미치는 영향을 파악한다.

본 연구에서는 앞서 제시한 보호동기이론을 바탕으로 데이터로부터 개인이 추적, 감시 당할 가능성에 대한 두려움의 인지 정도가 사용자의 온라인 프라이버시 보호 활동 의도에 미치는 영향을 최종적으로 살펴본다.

2.2 인지된 데이터 감시 위협(Perceived Dataveillance)

Clarke(1988)에 따르면, 데이터 감시(dataveillance)는 사람들의 행동이 아닌 디지털 정보를 이용하여 지속적으로 사람들의 행동을 모니터링 및 감시하는 방법이다. 따라서 데이터 감시는 실제 감시자의 눈이나 카메라를 통한 것이 아니라 온라인 환경에 저장된 정보 즉, 데이터를 바탕으로 이루어지는 새로운 감시의 유형이다(Kang 1998). 기존의 물리적 감시(Physical surveillance)와 데이터 감시는 분명한 차이점을 갖는다. 기존의 감시는 감시 대상의 신체 및 행동의 자유에 제한하여 구속하는 반면에 데이터를 이용한 감시는 개인의 생각과 사고까지 데이터를 통하여 엿볼 수 있어 감시의 가능 범위를 넓혔다. 또한 온라인 환경에서 발생하는 데이터 감시는 실제로 감시가 발생하는지에 대하여 사용자가 정확히 확인할 수 없는 불확실성 때문에 사용자가 체감하는 데이터 감시의 두려움은 증폭되며 이러한 특징이 기존의 감시 체계와 구별된다(Clarke 1997). 즉, 개인의 행동이 누군가에 의하여 어떻게 관찰되고 감시되는지 알 수 없기 때문에 이로 인한 불안함을 사용자는 호소하게 되는 것이다. 최대선 외(2013)는 SNS 환경에 제한하여 사용자가 공개하는 개인정보는 개인의 의도와 다르게 식별될 가능성이 존재함을 지적하며, 개인정보를 공개하였을 때 이로 인하여 자신이 특정될 수 있는 가능성을 개인이 전혀 인지할 수 없는 상황도 문제임을 밝혔다.

데이터 감시와 관련된 기존 연구는 주로 국가와 국민의 관계에서 다루어졌다. Clarke(1994)는, 향후, 데이터

감시는 개인의 수준을 넘어 그룹, 지역 사회 및 커뮤니티까지 감시의 범위가 확장되어 국가가 국민을 통제할 수 있게 되며 이는 민주주의와 자유를 위협할 수 있는 존재임을 언급하였다. 또한, 데이터 감시는 형사학, 정보학에서 '데이터 감시(능력)' 으로 정의되며 프로파일링 기법과 유사한 것으로 간주하여 범죄 해결 목적의 공익 추구를 위한 측면에서 주로 연구가 이루어졌다(Ferraris et al 2013). 하지만 이와 같은 프로파일링 기법을 통하여 보호하고자 하는 공익이 오늘날 빅데이터 환경의 도입에 따라 대부분 사라지게 되었다.이는 빅데이터 환경에서의 데이터 수집과 처리 등은 모두 상업화된 데이터의 기술로 수용되기 때문에 대부분 '사업자의 사익'과 '대상자의 사익' 사이의 충돌로만 존재한다(오길영 2015). 따라서 오늘날 데이터 감시 관련 연구는 기존의 국가와 국민 차원에서 발생 가능한 개인의 존엄성 상실 및 민주주의 위협 등의 차원에서 벗어나 온라인 환경에 존재하는 방대한 양의데이터를 실제 보유하며 이를 상업화하여 적극적으로 활용하는 기업과 데이터의 주된 제공자의 고객의 측면에서 살펴볼 필요성이 있다.

빅데이터 환경의 도입은 과거와 다르게 방대한 양의 축적된 데이터와 다양한 빅데이터 분석 기법을 적용하여 기업의 경영 및 생산 환경을 변화시켰다(Hasan and Hyland 2001). 기업은 보유한 고객 데이터의 양이 증가 함에 따라 이를 효과적으로 저장 및 관리하기 위한 데이터 웨어하우스를 구축하는 동시에 신속히 데이터를 처리하기 위한 다양한 데이터 분석 기법을 적용한 빅데이터 전략을 활용한다. 이러한 빅데이터 활용 전략은 데이터 분석의 정확성 향상을 통한 기업의 매출 이익을 증가시킴에 따라 기업은 고객의 방대한 정보 즉, 빅데이터에 더욱 의존하는 형태(Data-driven)의 경영방식으로 전환되었다(Stelzner 2010). 하지만 이와 같은 데이터 중심의 기업 경영방식의 확장은 고객이 데이터 감시의 위협에서 벗어날 수 없는 구조를 형성하였다(Degli Esposti 2014). 이는 기업이 개인의 정보에 대한 자유로운 접근 및 사용자에 대한 모니터링을 가능하게 하여 고객은 늘 감시 받는 듯한 불안감을 경험하기 때문이다. 이에 따라 소비자들은 기업의 과도한 개인정보 수집과 관리에 대한 불안함 및 낯선 기업의 개인정보 보유 가능성에 대한 두려움이 증가한 반면에 이와 같은 동일한 상황을 기업은 기술 발전에 따른 진보된 경영 전략의 한 가지 유형으로 수용한다(Van Dijck 2014). 따라서 데이터를 보유한 기업과 데이터를 제공하는 소비자 사이의 데이터 감시에 대한 인식 차이가 오늘날 발생하게 되었다.

3. 가설수립 및 연구모형

3.1 인지된 온라인 서비스의 효율성(Perceived Online Service Efficiency)

사용자는 정보 공유, 전자상거래 이용, 온라인 커뮤니케이션을 통한 대인관계의 형성 및 유지 등의 목적을 바탕으로 온라인 서비스를 사용한다(Sproull 2011). 사용자의 온라인 서비스 사용 의도에는 정보 획득 등의 본래 목적을 성취함에 따라 얻는 유용성과 혜택이 존재한다(Mcquail 2000). 본래 사용 목적의 달성에 따라 높게 지각된 사용자의 온라인 서비스 품질은 사용자의 만족도를 높인다(Parasuraman 1988). Zeithaml(2000)은 온라인 서비스 품질의 측정을 위한 척도에 효율성을 포함한 총 11개 항목을 제시하며, 서비스 품질의 만족도는 사용자가 체감하는 서비스의 효율성에 따라 달라짐을 제시하였다. 즉, 온라인 서비스의 효율성을 높게 평가하는 사용자일수록 이의 만족도가 높아지며 이는 사용 지속 의도를 증가시킨다(Ko et al 2011).

온라인 서비스의 효율성을 높게 인지하는 사용자의 경우, 해당 이용 서비스를 지속적으로 사용하려는 의

도를 지님에 따라 긍정적인 측면에 주로 집중하게 되는 경향이 있다. 왜냐하면 사람들은 흔히 개인의 사고 판단을 기준으로 원하는 것만 보거나 듣고자 한다는 선택적 노출 효과(Selective Exposure)에 따라 행동하는 경향이 크기 때문이다(Frey 1986). Liu, X et al(2008)에 따르면 온라인 쇼핑 서비스의 만족도가 높은 고객의 경우, 그렇지 않은 경우에 비하여 프라이버시 염려 수준이 낮았다. 이는 사용자가 온라인 서비스를 사용함에 따라 수반되는 각종 부정적인 상황에 대하여 회피하거나 발생 가능한 위협 및 손실에 대해서는 낮게 체감하는 반면에 온라인 서비스가 제공하는 각종 혜택 및 이익 등의 긍정적 측면을 주로 인식하고자 하는 개인의 성향 때문이다. 이에 따라 온라인 서비스의 효율성을 높게 인지하는 사용자일수록 데이터로부터 추적, 통제, 감시 등의 부정적 상황에 대한 체감 수준이 낮아질 것으로 판단하여 본 연구는 다음의 가설 1을 제시한다.

H1: 사용자가 인지하는 온라인 서비스의 효율성 증가는 인지된 데이터 감시의 위협 수준에 부(-)의 영향을 미칠 것이다.

3.2 인지된 프라이버시 통제 능력 상실(Perceived Loss of Control on Privacy)

프라이버시에 대한 개인 통제 능력의 선행 연구를 살펴보면, 이는 개인과 관련된 정보의공개 혹은 유통시키는 것을 스스로 결정하거나 통제할 수 있는 권리의 소유 상태(Eberle 2001)혹은 원치 않는 이메일의 삭제 활동부터 프라이버시를 위협하는 다양한 요소들로부터 이를 보호하는 소프트웨어의 설치와 같은 적극적인 활동까지(Chen and Rea Jr. 2004)를 포함하는 넓은 범위의 의미를 갖는다. Stone et al(1990)은 프라이버시 통제 능력을 사용자가제공한 개인정보로 인하여 발생 가능한 부정적인 결과를 개인이 스스로 희석시킬 수 있는 능력의 소유 여부로 정의하였다. 또한 통제는 사회적 계약 이론(Social Contract)에 의하여절차적 정당성의 원칙을 바탕으로 움직이기 때문에 제공된 정보가 개인의 의사에 반하여 관리 및 이용되는 경우 이를 개인이 변화 및 회복시킬 수 있는 영향력을 의미한다(Gilliland 1993). 이에 따라본 연구에서는 개인의 프라이버시를 위협하는 다양한 요소 및 상황에 대하여 사용자가 능동적으로 대처할 수 없거나 개인정보의 공개 및 유통에 주체적인 권한을 행사할 수 없는 상태를 인지된 프라이버시 통제 능력의 상실로 정의하였다.

사용자의 프라이버시 통제 능력은 개인의 프라이버시 염려 수준 증감에 영향을 미친다(Culnan 1993). Malhotra et al(2004)에 따르면, 정보 프라이버시에 대한 사용자의 통제 능력 상실은 이들의 프라이버시 염려 수준을 증가시킨다. 반면에 Nowak and Phelps(1995)는 기업이 온라인 서비스 사용 고객의 데이터를 수집하는 과정에서 개인정보 활용에 대한 옵트 아웃(opt-out)의 선택권을 명시한 경우, 이들의 프라이버시 침해 우려 정도가 낮음을 제시하였다. 이는 개인정보를 제공한 기업에 대하여 사용자는 개인정보에 대한 통제 능력이 옵트 아웃의 선택권이라는 명목으로 보장되었기 때문이다. Dinev et al(2004)는 개인이 인지하는 프라이버시 통제 능력을 정보 프라이버시 염려의 선행요인으로 제시하며 통제 능력의 상실을 프라이버시의 침해 상태로 간주하였다. 또한 Milne and Rohm(2000)은 고객의 동의 없이 개인정보가수집되는 경우 이들의 프라이버시 통제 능력은 상실된 상태임을 밝혔다. 따라서 본 연구에서는 사용자가 인지하는 프라이버시에 대한 통제 능력 상실 정도의 증가는 온라인 환경에서 개인이 경험하는 감시 위협의 체감 정도를 증가시킨다는 다음의 가설 2를 제시한다.

H2: 사용자가 인지하는 온라인 프라이버시 통제 능력 상실 정도의 증가는 인지된 데이터 감시의 위협 수준에 정(+)의 영향을 미칠 것이다.

3.3 인지된 오프라인 감시 위협(Perceived Offline Surveillance)

최근 IT 기술의 발전은 사물인터넷(IoT), 인공지능(AI), 생체인식 등과 결합하여 CCTV를 비롯한 기존의 지능형 영상 감시 시스템의 감시 체계를 진화시켰다(전자신문 2017.04). 이러한 감시 체계의 발전은 범죄 및 사고 예방에 효과적인 반면에 사용자가 체감하는 감시에 대한 두려움과 불안함을 증가시켰다(Wu et al 2017). 2015년, Pew Research Center에서 시행한 설문조사의 결과에 따르면 대다수의 연령대에서 유사한 응답률을 보였지만 특히, 20대의 76%는 오늘날 개인의 행동은 CCTV로부터 자유로워질 수 없는 상황이라고 응답한 반면에 동일한 응답자의 63%는 그럼에도 불구하고 개인이 감시 받지 않는 상태에서 행동할 수 있는 권리는 중요하다고 밝혔다. 오프라인 환경에서 일반적으로 발생하는 물리적인 감시(Physical Surveillance)는 제한된 시공간을 바탕으로 CCTV와 같은 특수한 기술 장치 혹은 감시자의 눈을 통하여 직접적인 형태로 이루어진다(Clarke 2009). 앞선 설문조사의 결과에서 확인할 수 있듯이, 오늘날 CCTV를 비롯한 각종 기술의 발전은 개인이 물리적인 감시 체계에서 생활 할 수 밖에 없는 환경을 형성하였다.

앞서 서두에서 언급한 바와 같이 개인은 자신이 인지하는 심리적 요소들을 일관성 있게 유지하려는 성향을 가진다는 인지 일관성 이론(Theory of Cognitive Consistency)에 따라 본 연구에서는 사용자가 오프라인 환경에서 인지하는 감시 위협에 대한 두려움은 온라인 환경에 까지 영향을 미치게 된다고 보았다. 또한 Park et al(2016)은 온라인 커뮤니케이션의 활용은 사용자의 오프라인 관계 강도를 약화시킨다는 연구결과를 제시함에 따라, 사용자의 심리는 온라인과 오프라인의 경계 구분 없이 상호간에 영향을 주거나 확장되어 발생함을 알 수 있다. 이에 본 연구는 사용자가 오프라인 환경에서 인지하는 감시의 위협이 온라인에서의 감시 즉, 데이터를 이용하여 사용자의 동의 없는 신원 조회 혹은 감시 여부에 대한 불확실성 등이 초래하는 두려움(dataveillance)으로 까지 확장된다고 가정하여 다음의 가설 3을 제시한다.

H3: 사용자가 인지하는 오프라인 환경의 감시 정도 증가는 인지된 데이터 감시의 위협 수준에 정(+)의 영향을 미칠 것이다.

3.4 인지된 프라이버시 규제의 필요성(Perceived Necessity of Regulation)

빅데이터 시대의 등장은 온라인 환경에서 방대한 양의 데이터가 빠르게 축적됨에 따라 개인정보의 수집 및 활용이 용이해진 동시에 유출과 침해의 가능성도 함께 증가시켰다(Park et al 2017). 또한 다양한 정보통신기술의 발달은 정보의 불법적인 수집 등을 비롯한 잦은 개인정보 유출 사고를 발생시키며 이의 피해 규모도 과거에 비하여 대폭 증가시켰다(Baek et al 2014). 이러한 개인정보에 대한 최근의 사회적 변화는 사용자에게 개인정보의 중요성을 인지시키며 이를 보호하기 위한 법적 규제 마련의 필요성을 수반하였다. Litman(2000)은 개인정보보호의 불안정한 상태는 정부의 규제에 강력한 원동력이 되며 법, 정책과 같이 강제성이 수반되는 규제의 형성과 발전의 토대가 됨을 언급하였다. 이에 따라 오늘날 전세계적으로 개인정보보호와 관련된 규제는 지속적으로 제·개정의 과정을 통하여 발전하게 되었고 각 국가는 이를 바탕으로 자국내 개인정보보호 수준을 향상시키고자 한다(Zhang 2014).

국내 개인정보보호법을 비롯하여 각 국의 프라이버시 보호와 관련된 정책은 국가 혹은 기업이 수집 및 활용하는 개인정보를 보호하기 위하여 이에 대한 기술적 조치 및 개인정보 관리에 대한 책임을 제시하는 포괄적인 규정을 의미한다(Wu et al 2012). 하지만 개인정보보호를 위한 이러한 규제의 장치가 마련이 되었음에

도 불구하고 오늘날 개인정보와 관련된 유출 및 침해 사고는 꾸준히 증가하였고 이는 사용자에게 온라인 환경의 위험성과 개인정보 침해의 우려 수준을 오히려 증가시키는 계기가 되었다(윤상오 2009). 이를 종합하면 개인정보와 관련된 규제의 필요성 및 엄격함을 강하게 주장하는 사용자일수록, 온라인 환경이 내포한 위협 요소에 따른 개인정보 유출 및 침해 발생 가능성에 대한 현실 체감 정도가 높다. 따라서 본 연구는 이러한 개인정보보호 관련 법적 규제의 필요성을 강하게 인지하는 사용자일수록 온라인 환경의 불안전성에 따른 데이터 감시 위협의 체감 수준도 증가할 것이라는 다음의 가설 4를 제시한다.

H4: 사용자가 인지하는 프라이버시에 대한 법적 규제 필요성의 증가는 인지된 데이터 감시의 위협 수준에 정(+)의 영향을 미칠 것이다.

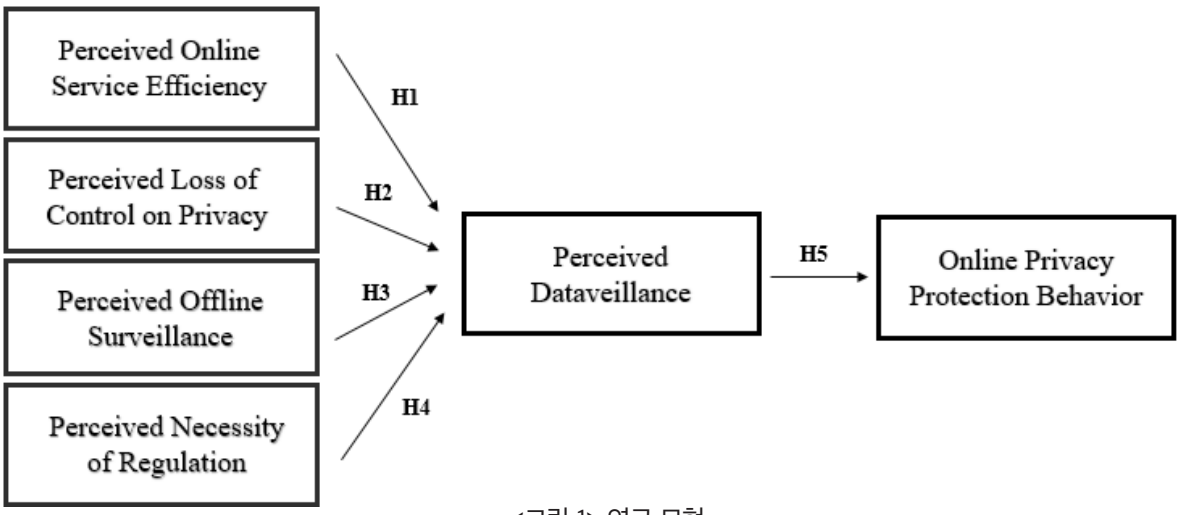
3.5 온라인 프라이버시 보호 활동(Online Privacy Protection Behavior)

Chen et al(2017)은 보호동기이론을 바탕으로 사용자의 프라이버시 보호 활동은 타인에 의하여 개인정보가 남용될 것을 염려함에 따라 발생하는 자발적인 보호 행위(Dinev and Hart 2004)와 개인정보의 유출 등에 따른 경제적 손실을 방지하기 위하여 노력이 수반되는 개인의 보호적 행동(D. Lee et al 2008)으로 분류하여 제시하였다. 사용자가 인지하는 프라이버시 염려, 개인정보 침해로 인한 금전적 손실의 두려움 등이 발생함에 따라 개인의 보호 활동 의도가 증가하며 이는 실제 개인의 정보보호 활동으로 이어지게 된다(Mohamed and Ahmad 2012). Chen et al(2017)의 연구결과에 따르면, 프라이버시 염려의 증가는 실제 프라이버시 보호 활동인 사용자의 패스워드 변경 빈도를 증가시켰다. Chai et al(2009)는 청소년을 대상으로 정보 프라이버시 중요성을 강하게 인지할수록 프라이버시 보호 활동에 적극적인 반면에 개인정보 유출, PC 내 바이러스 침투 등의 부정적인 경험은 이들의 프라이버시 보호 활동을 감소시킴을 밝혔다. 따라서 이전의 개인정보 유출 등의 사고 피해자가 향후, 다시 유사한 사건의 피해자가 될 가능성이 높음을 시사하였다. 이와 같이 사용자가 프라이버시를 보호하기 위한 구체적인 행동은 안티 바이러스 소프트웨어의 설치(D. Lee et al 2008) 및 인터넷 사용 기록을 삭제하는 쿠키 제거(Gross and Acquisti 2005) 등의 기술적 조치와 의심스러운 웹사이트의 접속을 피하거나(Youn 2009), 불명확한 발송인의 이메일을 열람하지 않는 등(Chen et al 2016)의 개인의 관리적 차원으로 구분된다.

개인정보 유출, 프라이버시 침해와 같은 온라인 환경의 다양한 위협 요인이 존재함에 따라 발생하는 개인의 불안함과 우려감은 이들의 실제 정보보호 및 예방 활동에 영향을 미친다(Buchanan, T 2007). 사용자는 불법적으로 수집되는 개인정보 탈취의 두려움에서 벗어나기 위하여 프록시 서버를 활용하여 개인의 IP 추적을 타인으로부터 방지하거나 개인의 PC에 방화벽을 설치하는 등의 다양한 정보보안 기술을 수용한다(최보미 외 2015). 따라서 본 연구는 프라이버시 염려, 개인정보 유출의 우려와 같이 온라인 환경에서 사용자가 경험하는 부정적인 상태의 데이터 감시에 따른 위협은 개인의 온라인 프라이버시 보호 활동 의도에 정(+)의 영향을 미칠 것이라는 다음의 가설 5를 제시한다.

H5: 사용자가 인지하는 데이터 감시 위협 정도의 증가는 개인의 온라인 프라이버시 보호 활동 의도에 정(+)의 영향을 미칠 것이다.

다음의 [그림 1]은 본 연구의 실증 분석 모형이다.



<그림 1> 연구 모형

4. 연구 설계

4.1 연구 데이터 수집

본 연구는 Pew Research Center에서 제공하는 데이터를 기반으로 연구를 진행하였다. Pew Research Center는 미국의 사회 전반 현황을 알아보기 위하여 설치된 대표 여론조사 전문기관이다. 해당 기관에서 프라이버시에 대한 인식을 살펴보기 위하여 2014년 1월 10일부터 27일, 약 18일간, 총 607명의 성인을 대상으로 진행된 설문조사의 응답 데이터를 본 연구에서는 활용하였다. 설문 조사 실시 결과, 해당 조사 통계 결과는 인구 통계학적 불일치를 해소하기 위해 가중치 산정이 이루어졌으며, 전체 데이터 세트에 대한 표본 오차는 ± 4.6%이다. 또한 본 연구의 분석 대상은 설문에 참여한 응답자 중, 최소한 한 개 이상의 SNS를 사용한다고 밝힌 389명의 응답자를 대상으로 진행하였으며 표본의 인구통계학적 특성은 아래의 <표 1>과 같다.

<표 1> 표본의 인구통계학적 특성

	빈도 (%)
성별	
남성	178 (45.8)
여성	211 (54.2)
연령	
18 ~ 29	89 (22.9)
30 ~ 44	119 (30.6)
45 ~ 59	113 (29.0)
60 ~	68 (17.5)
합계	389

4.2 연구변수의 측정항목

본 연구에서는 앞서 제시한 바와 같이 Pew Research Center에서 제공한 기존의 설문 문항을 활용하였으며, 선택된 문항은 실제 현상이 충분히 반영되어 변수가 이를 대표할 수 있도록 하였으며 자세한 측정항목은 다음의 <표 2>와 같다.

<표 2> 연구변수의 측정항목

측정개념	질문 및 답변 항목
인지된 데이터 감시 위협 (Perceived Dataveillance)	[질문] How concerned are you, if at all, that some of the information you share on social networking sites might be accessed by third parties, like advertisers or businesses, without your knowledge? [답변 항목] Very concerned / Somewhat concerned / Not too concerned / Not at all concerned
인지된 온라인 서비스의 효율성 (Perceived Online Service Efficiency)	[질문] I appreciate that online services are more efficient because of the increased access they have to my personal data. [답변 항목] Strongly agree / Agree / Disagree / Strongly disagree
인지된 프라이버시 통제 능력 상실 (Perceived Loss of Control on Privacy)	[질문] Consumers have lost control over how personal information is collected and used by companies. [답변 항목] Strongly agree / Agree / Disagree / Strongly disagree
인지된 오프라인 감시 위협 (Perceived Offline Surveillance)	[질문] It is hard to avoid surveillance cameras when I am out in public. [답변 항목] Strongly agree / Agree / Disagree / Strongly disagree
인지된 프라이버시 규제의 필요성 (Perceived Necessity of Regulation)	[질문] Do you think the government should do more to regulate what advertisers do with customers' personal information, or should the government not get more involved in this? [답변 항목] Should do more to regulate / Should not get more involved
온라인 프라이버시 보호 활동 (Online Privacy Protection Behavior)	[질문] Do you feel as though you already do enough to protect the privacy of your personal information online, or do you feel as though you would like to do more? [답변 항목] I already do enough / I would like to do more

5. 분석 및 결과

다음의 <표 3>은 본 연구의 목적인 사용자가 온라인 환경에서 인지하는 요인들에 따라 변화되는 인지된 데이터 감시 위협 정도를 살펴보기 앞서 실시한 기초 통계 분석 결과이다.

<표 3> 측정 변수의 기초통계량

Variables		Mean	Standard Deviation
PD	Perceived Dataveillance	1.84	0.7779
POSE	Perceived Online Service Efficiency	2.74	0.7448
PLCP	Perceived Loss of Control on Privacy	1.65	0.6622
POS	Perceived Offline Surveillance	1.84	0.7701
PNR	Perceived Necessity of Regulation	0.34	0.4750
OPPB	Online Privacy Protection Behavior	0.33	0.4705

이를 바탕으로 SPSS 통계 패키지를 이용하여 다중회귀분석을 수행하였다. 다중회귀분석을 실시하기에 앞서서 어떠한 변수가 종속변수에 얼마나 영향을 주는지 알아보고자 변수선택 방법 중 입력(Enter) 방식을 선택하였다. 이와 같은 입력 방식의 선택은 본 연구에서 제시한 4가지의 독립변수가 각각 사용자가 인지하는 데이터 감시의 위협에 미치는 정도가 확인가능하며 가장 적은 오차를 갖는 회귀모형을 선택할 수 있도록 한다. 또한 4개의 설명변수 사이에는 다중공선성이 발생하지 않도록 하여 모형의 적합성을 높이고자 다중회귀분석을 실시하였다. 이는 종속변수를 설명하는 과정에서 여러 개의 설명변수에 대한 모형설정(specification)의 정확성을 높이며, 종속변수에 대하여 누락되는 설명변수가 발생시키는 편향성 문제를 방지하게 한다. 이에 따라 본 연구는 다중회귀분석을 실시하였으며 결과는 다음의 <표 4>와 같다.

<표 4> 온라인 환경에서의 사용자 인지 요인과 데이터 감시 위협의 회귀분석 결과

가설	경로	*Unstandardized Coefficients*		*β*	*t*	*R2*	*Durbin-Watson*	결과
		b	*Std. error*					
H1	POSE→PD	-.181	.049	-.173	-3.716***	0.169	1.980	채택
H2	PLCP→PD	.320	.056	.273	5.736***			채택
H3	POS→PD	.131	.048	.129	2.730**			채택
H4	PNR→PD	.258	.076	.158	3.396**			채택
H5	PD→OPPB	.127	.030	.209	4.212***			채택

***p<.001, **p<.01

우선, 본 회귀방정식의 설명력을 의미하는 조정된 R2 값은 0.169로서 이는 해당 모형의 적합도를 약 17%로 설명 가능하다. Cohen의 기준에 따르면, 사회과학 분야에서 설문조사 방법을 활용한 연구의 경우, 결정계수가 약 13%이상이면 해당 모형의 효과를 검정하였다고 보는 것이 일반적이다(Cohen.L. 1992). 또한 도출된 회귀 모델의 Durbin-Watson 값은 1.980으로 상대적으로 자기상관에 대한 위험이 적다고 판단된다.

본 연구에서 제시한 각각의 가설 5가지는 모두 채택되었으며 이를 자세히 살펴보면 다음과 같다. 첫째, 사용자가 인지하는 온라인 서비스의 사용 효율성 증가는 데이터 감시 위협 수준을 감소시킴에 따라 가설 1은 지지되었다(β = -.181, p <0.001). 둘째, 온라인 프라이버시에 대한 개인의 통제 능력 상실 정도의 증가는 데이터 감시 위협의 인지 수준을 증가시켜 가설 2는 지지되었다(β = .320, p <0.001). 셋째, 사용자가 오프라인 환경에서 지각하는 감시 위협 정도의 증가는 온라인 환경에서의 데이터 감시의 위협 정도와 정(+)의 관계를 나타냄에 따라 가설 3도 역시 채택되었다(β = .131, p <0.01). 이는 오프라인에서 감시에 대한 두려움을 높게 지각하는 사용자일수록 온라인 환경에서의 데이터를 통한 감시에 대한 염려 정도도 높음이 검증되었다. 따라서 오프라인에서 발생한 개인의 감시 위협이 온라인까지 일관되게 유지되었다고 볼 수 있다. 넷째, 사용자가 인지하는 프라이버시 관련 규제의 필요성 증가는 데이터 감시 위협의 지각 수준을 높이며 가설 4는 지지되었다(β = .258, p <0.01). 마지막으로 사용자가 인지하는 온라인 환경에서의 감시 위협 및 두려움(dataveillance)은 개인의 온라인 프라이버시 보호 활동의 필요성을 증가시키는 요인이 됨에 따라 가설 5 역시 채택되었다(β = .127, p <0.001).

6. 시사점 및 연구의 한계

빅데이터 시대의 등장은 데이터 기반의 감시 체제인 빅데이터 감시 사회를 형성함에 따라 온라인 환경에서의 다양한 요인이 사용자가 인지하는 데이터 감시 위협에 영향을 미치고 있음을 본 연구 결과를 통하여 확인하였다. 개인이 지각하는 온라인 프라이버시 통제 능력의 상실, 오프라인 환경의 감시 위협 정도, 프라이버시 관련 규제 필요성의 수준이 증가할수록 사용자의 데이터 감시로 인한 두려움의 정도는 증가하였다. 반면에 사용자가 온라인 서비스의 효율성을 높게 평가할수록 데이터 감시의 위협 지각 정도는 감소하였다. 최종적으로 개인이 데이터를 통한 감시 위협 및 두려움을 높게 인지할수록 이들의 온라인 프라이버시 보호 활동 의도도 함께 증가하였다.

본 연구는 온라인 해킹, 프라이버시 침해 등에 따른 사용자의 염려 수준을 다룬 선행 연구와 달리 빅데이터 환경 형성에 따른 데이터 감시, 데이터 사찰의 사회적 현상에 주목하였다는 점에서 시의성을 갖는다. 특히, 본 연구 결과에 따르면 프라이버시 관련 법, 정책 등의 규제 마련의 필요성을 강하게 인지하는 사용자일수록 데이터 감시에 대한 지각 정도가 높았다. 이는 기존의 연구 대부분이 프라이버시 관련 규제 형성의 필요성(Claudio et al 2005; Schmid and Tina 2016)에 대하여 주장하는 반면에 본 연구는 개인이 체감하는 온라인 환경의 안전성이 관련 규제의 필요성 지각 정도에 따라 변화됨을 규명하였다는 점에서 의의가 있다. 해당 연구결과는 향후, 프라이버시 관련 법규의 실효성을 파악하는 연구의 토대가 된다.

현재의 사물인터넷(IoT), 인공지능(AI) 등의 기술 발전에 따라 향후 예상되는 초연결사회의 도래는 다양한 온라인 서비스와 디바이스의 사용으로 기업은 지금보다 더 많은 사용자의 개인정보를 보유하게 될 것이다. 이에 따라 사용자의 의지와 상관없이 개인정보

는 지속적으로 수집되고 이들이 체감하는 데이터 감시의 위협도 더욱 증가한다. 이에 따라 본 연구는 개인의 데이터 감시 위협 수준에 영향을 미치는 요인과의 관계를 살펴보았다는 점에서 향후 사용자가 체감하는 데이터 감시의 위협을 감소시킬 수 있는 온라인 환경 구성의 필요성 및 기업의 경영전략 마련에 필요성을 제공한다.

향후 기업은 고객의 데이터를 수집 및 관리하는 과정에서 사용자의 데이터 감시 위협을 감소시키는 방안의 제시가 필요하다. 데이터 감시의 위협이 존재하는 환경에서 기업은 개인정보 처리에 대한 정책 및 절차의 공식적인 제시는 소비자의 정보 제공 활동에 대한 불안감을 낮춘다(Ashworth and Free 2006). Hui et al(2007)에 따르면, 기업은 개인정보의 수집, 활용, 관리, 피해구제 등에 대한 전반적인 정보를 제공함으로써 사용자의 정보 프라이버시 염려를 감소시킬 수 있다. 따라서 기업은 빅데이터가 지닌 우수한 장점을 지속적으로 활용하여 이익 증대와 같은 기업의 성과를 높이기 위해서는 사용자의 입장을 고려하여 데이터를 통한 추적, 감시 등의 위협적인 상황에 대한 안전성을 제공하는 방안이 마련되어야 한다. 이러한 방안의 마련은 기업이 필요한 고객의 데이터를 전략적으로 확보할 수 있도록 도모한다. 단, 이러한 과정이 선행되지 않는다면 사용자가 인지하는 데이터 감시의 위협은 지속적으로 증가하여 개인의 온라인 활동 변화를 일으키거나 기업에 대한 고객의 불신 문제를 발생시킬 것이다. 이는 고객이 기업에게 개인정보를 제공하지 않거나 온라인 환경에서 거짓된 개인정보를 제공하는 등의 사회적 문제를 초래하며 기업의 경제적 손실 문제를 발생시킨다.

본 연구에서는 미국의 Pew Research Center에서 수집한 데이터를 기반하여 연구 모형을 설계 하였기 때문에 2차 자료 사용으로 인한 한계점을 갖는다. 응답자의 다양한 연령, 성별의 균형성을 확보하여 인구통계학적 문제는 발생하지 않았으나, 미국 국적의 SNS 사용자만을 대상으로 하여 연구 결과의 확장에 한계가 존재한다. 또한 본 연구의 주된 이론적 틀인 보호동기이론에서 차용한 지각된 심각성, 지각된 효율성과 자기 효능감 이외에 지각된 취약성과 지각된 장애의 요인을 추가 설명 변수로 고려하지 않았다는 점에서 제한점을 갖는다.

빅데이터의 등장에 따라 등장한 오늘날의 데이터 감시 사회에서 온라인 사용자는 벗어날 수 없게 되었다. 따라서 국가는 이에 대한 심각성을 깨닫고 프라이버시를 안전하게 보호할 수 있는 규제 마련 등의 적절한 사회적 차원의 방안을 강구하는 동시에 능동적인 개인의 프라이버시 보호 활동을 통해 사용자는 데이터 감시, 데이터 사찰의 문제에서 비교적 자유로워질 수 있다고 판단된다.

7. 사사

이 논문은 2016년 대한민국 교육부와 한국연구재단의 지원을 받아 수행된 연구임(NRF-2016S1A5A2A01025553).

참고문헌

[국내 문헌]

1. 오길영 2015. "빅데이터 환경에서의 정보보호 담론에 대한 비판," *헌법학연구,* 21, pp. 37-69.
2. 윤상오 2009. "전자정부 구현을 위한개인정보보호 정책에 관한 연구: 정부신뢰 구축의 관점에서," *한국지역정보화학회지*, (12:2).
3. 최대선, 김석현, 조진만, 진승헌, 조현숙 2013. "소셜 네트워크서비스 개인정보 노출 실태 분석," *정보보호학회논문지,* (23:5), pp. 977-983.
4. 최보미, 박민정, 채상미 2015. "개인정보보호 기술 수용행동에 영향을 미치는 요인에 대한 연구," *Information Systems Review,* (17:3), pp. 77-94.

[국외 문헌]

1. Ashworth, L., and Free, C. 2006. "Marketing dataveillance and digital privacy: Using theories of justice to understand consumers' online privacy concerns," *Journal of Business Ethics*, (67:2), pp. 107-123.
2. Baek, Y. M., Kim, E. M., and Bae, Y. 2014. "My privacy is okay, but theirs is endangered: Why comparative optimism matters in online privacy concerns," *Computers in Human Behavior*, 31, pp. 48-56.
3. Bettini, C., Wang, X. S., and Jajodia, S. 2005. August. "Protecting privacy against location-based personal identification," In *Workshop on Secure Data Management* (pp. 185-199). Springer Berlin Heidelberg.
4. Buchanan, T., Paine, C., Joinson, A. N., and Reips, U. D. 2007. "Development of measures of online privacy concern and protection for use on the Internet," *Journal of the American Society for Information Science and Technology*, (58:2), pp.157-165.
5. Chai, S., Bagchi-Sen, S., Morrell, C., Rao, H. R., and Upadhyaya, S. J. 2009. "Internet and online information privacy: An exploratory study of preteens and early teens," *IEEE Transactions on Professional Communication*, (52:2), pp.167-182.
6. Chellappa, R. K., and Pavlou, P. A. 2002. "Perceived information security, financial liability and consumer trust in electronic commerce transactions. *Logistics Information Management*, (15:5/6), pp.358-368.
7. Chen, H., Beaudoin, C. E., and Hong, T. 2017. "Securing Online Privacy: An Empirical Test on Internet Scam Victimization, Online Privacy Concerns, and Privacy Protection Behaviors," *Computers in Human Behavior*.
8. Chen, K., and Rea Jr, A. I. 2004. "Protecting personal information online: A survey of user privacy concerns and control techniques," *Journal of Computer Information Systems*, (44:4), pp. 85-92.
9. Clarke, R. 2009. "Privacy impact assessment: Its origins and development," *Computer law & security review*, (25:2), pp. 123-135.

10. Clarke, R. 1997. “Introduction to dataveillance and information privacy, and definitions of terms”

11. Clarke, R. 1994. “The digital persona and its application to data surveillance,” *The information society*, (10:2), pp. 77-92.

12. Clarke, R. 1993. “Profiling: A hidden challenge to the regulation of data surveillance,” *JL & Inf*. Sci., 4, 403.

13. Clarke, R. 1988. “Information technology and dataveillance,” *Communications of the ACM,* (31:5), pp. 498-512

14. Cohen, J. 1992 “Statistical power analysis”, *Current directions in psychological science,* pp.98-101

15. Degli Esposti, S. 2014. “When big data meets dataveillance: The hidden side of analytics,” *Surveillance & Society*, (12:2), 209.

16. Culnan, M.J. 1993. “How Did They Get My Name?”: An Exploratory Investigation of Consumer Attitudes toward Secondary Information Use,” *MIS Quarterly*, (17:3), pp. 341-363.

17. Dinev, T., and Hart, P. 2004. “Internet privacy concerns and their antecedents-measurement validity and a regression model,” *Behaviour & Information Technology*, (23:6), pp. 413-422.

18. Eberle, E. J. 2001. “The right to information Self-Determination,” *Utah L.* Rev., 965.

19. Ferraris, V., Bosco, F., Cafiero, G., D’Angelo, E., and Suloyeva, Y. 2013. “Defining Profiling”

20. Frey, D. 1986. “Recent research on selective exposure to information,” *Advances in experimental social psychology*, 19, pp. 41-80.

21. Gilliland, S.W. 1993. “The perceived fairness of selection systems: An Organizational Justice Perspective,” *Academy of Management Review*, (18:4), pp. 694-734.

22. Gross, R., and Acquisti, A. 2005, November. “Information revelation and privacy in online social networks,” In *Proceedings of the 2005 ACM workshop on Privacy in the electronic society* pp. 71-80.

23. Hasan, H., and Hyland, P. 2001. “Using OLAP and multidimensional data for decision making,” *IT Professional*, (3:5), pp. 44-50.

24. Heider, F. 1946. “Attitudes and cognitive organization,” *The Journal of psychology*, (21:1), pp. 107-112.

25. Herath, T., and Rao, H. R. 2009. “Protection motivation and deterrence: a framework for security policy compliance in organisations,” *European Journal of Information Systems*, (18:2), pp.106-125.

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

27. Ifinedo, P. 2012. “Understanding information

systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory," *Computers & Security*, (31:1), pp. 83-95.

28. Kang, J., Shilton, K., Estrin, D., and Burke, J. 2011. "Self-surveillance privacy," *Iowa L. Rev.*, 97, pp.809.

29. Kang, J. 1998. "Information privacy in cyberspace transactions," *Stanford Law Review*, pp. 1193-1294.

30. Ko, H. S., Kim, C. S., Jeong, M. Y., Oh, Y. J., and Lee, S. H. 2011. "The effect of social network service's quality factors on user satisfaction and the intention to continued use," *Journal of the Korean society for quality management*, (39:4), pp. 543-555.

31. Lee, D., Larose, R., and Rifon, N. 2008. "Keeping our network safe: a model of online protection behaviour. *Behaviour & Information Technology*," (27:5), pp. 445-454.

32. Leistert, O. 2012. "Resistance against cyber-surveillance within social movements and how surveillance adapts," *Surveillance & Society*, (9:4), pp. 441.

33. Litman, J. 2000. "Information privacy/ information property," *Stanford Law Review*, pp. 1283-1313.

34. Liu, X., He, M., Gao, F., and Xie, P. 2008. "An empirical study of online shopping customer satisfaction in China: a holistic perspective," *International Journal of Retail & Distribution Management*, (36:11), pp. 919-940.

35. Maddux, J. E., & Rogers, R. W. 1983. "Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change," *Journal of experimental social psychology*, (19:5), pp. 469-479.

36. Malhotra, N. K., Kim, S. S., and Agarwal, J. 2004. "Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model," *Information systems research*, (15:4), pp. 336-355.

37. McQuail, D. 2010. *McQuail's mass communication theory*. Sage publications.

38. Milne, G. R., and Rohm, A. J. 2000. "Consumer privacy and name removal across direct marketing channels: Exploring opt-in and opt-out alternatives," *Journal of Public Policy & Marketing,* (19:2), pp. 238-249.

39. Mohamed, N., and Ahmad, I. H. 2012. "Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia," *Computers in Human Behavior*, (28:6), pp. 2366-2375.

40. Morimoto, M., and Chang, S. 2006. "Consumers' attitudes toward unsolicited commercial e-mail and postal direct mail eting methods: intrusiveness, perceived loss of control, and irritation," *Journal of Interactive Advertising*, (7:1), pp. 1-11.

41. Nowak, G. J., and Phelps, J. 1995. "Direct

marketing and the use of individual-level consumer information: Determining how and when "privacy" matters," *Journal of Direct Marketing*, (9:3), pp. 46-60.

42. Park, M., Chai, S., and Lee, M. 2017. "A Study of Predicting Judgments on Causes of Online Privacy Invasions: Based on U.S Judicial Cases," Conference Proceedings, *19th Information Security and Risk Management, Singapore Jan 08-09*

43. Park, M., Choi. B., and Chai, S. 2016. "Do You Really Maintain Your Social Tie through SNS?; An Exploratory Study of Online Environment, Journal of Next Generation Information Technology," (7:1), pp. 72-82.

44. Parasuraman, A., Zeithaml, V. A., and Berry, L. L. 1988. "Servqual: A multiple-item scale for measuring consumer perc," *Journal of retailing,* (64:1), pp. 12.

45. Rogers, R. W. 1975. "A protection motivation theory of fear appeals and attitude change1," *The journal of psychology*, (91:1), pp. 93-114.

46. Schmid, G., and Gausling, T. 2016. "Data protection and the right of personality with regard to rating platforms: decisions of the German Federal Supreme Court," *Journal of Intellectual Property Law & Practice*, (11:1), pp. 46-48.

47. Sproull, L. 2011. "Prosocial behavior on the net," *Daedalus*, (140:4), pp. 140-153.

48. Stelzner, Micael A. 2010. "Social media marketing industry report: How marketers are using *social media to grow their businesses*," SocialMedia Examiner

49. Stone, E. F., and Stone, D. L. 1990. "Privacy in organizations: Theoretical issues, research *findings, and protection mechanisms," Research in* personnel and human resources management, (8:3), pp. 349-411.

50. Youn, S. 2009. "Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents," *Journal of Consumer affairs*, (43:3), pp. 389-418.

51. Van Dijck, J. 2014. "Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology," *Surveillance & Society*, (12:2), pp. 197.

52. Vance, A., Siponen, M., and Pahnila, S. 2012. "Motivating IS security compliance: insights from habit and protection motivation theory," *Information & Management*, (49:3), pp. 190-198.

53. Wu, K. W., Huang, S. Y., Yen, D. C., and Popova, I. 2012. "The effect of online privacy policy on consumer privacy concern and trust," *Computers in human behavior*, (28:3), pp.889-897.

54. Wu, Y. L., Tao, Y. H., and Chang, C. J. 2017. "A comparative review on privacy concerns and safety demands of closed-circuit television among Taiwan, Japan, and the United

Kingdom," *Journal of Information and Optimization Sciences*, (38:1), pp. 173-196.

55. Zeithaml, V. A., Parasuraman, A., and Malhotra, A. 2000. "Conceptual Framework for understanding e-service quality: Implications for future research and managerial practice"

56. Zeithaml, V. A. 2000. "Service quality, profitability, and the economic worth of customers: what we know and what we need to learn," *Journal of the academy of marketing science*, (28:1), pp. 67-85.

57. Zhang, D. Y. 2014. "Study on the Behavioral Logic of Personal Information Protection in the View of Constitution," In Advanced Materials Research, 971, pp. 1768-1771.

[URL]

1. 전자신문, [보안컬럼] "감시자에서 조력자로, CCTV의 진화," 2017.04.18, http://www.etnews.com/20170418000097

저 자 소 개

박 민 정 (mjpark67@ewhain.net)

현재 이화여자대학교 경영학과 박사과정에 재학중이며 빅데이터분석학 석사학위를 취득하였다. 주요 연구 분야는 정보보안, 개인정보보호, 빅데이터 분석이다. 그리고 최근에는 조직 구성원의 정보보안 정책 준수 활성화 방안 및 데이터 감시에 대한 연구를 활발히 진행 중이다.

채 상 미 (smchai@ewha.ac.kr)

현재 이화여자대학교 경영대학 부교수로 재직 중이다. 이화여자대학교에서 학사, 서울대학교에서 경영학 석사 학위를 취득하였으며, 미국 The State University of New York at Buffalo에서 경영학 박사학위를 취득하였다. 주요 연구 분야는 정보기술과 인간 행동에 관한 주요 이슈 IT와 조직 및 전략, 정보보안과 조직, 그리고 최근에는 빅데이터 분석 기술을 활용한 연구를 진행 중이다.