http://dx.doi.org/10.14400/JDC.2015.13.6.1

모바일 앱 프라이버시 보호를 위한 소비자 체크리스트

이화옥*, 김린아**, 나종연***
서울대학교 소비자학과 박사과정*, 서울대학교 소비자학과 석사과정**, 서울대학교 소비자학과 교수***

Mobile App Privacy Checklist for Consumer

Hua-Yu Li*, Lin-Ah Kim, Jong-Youn Rha*****
Department of Consumer Science, Seoul National University*
Department of Consumer Science, Seoul National University**
Department of Consumer Science, Seoul National University***

요 약 최근 스마트폰이나 태블릿 PC 등 모바일 기기의 사용 확산과 함께 모바일 앱(어플리케이션)의 사용도 증가되면서 모바일 앱에서의 프라이버시 문제가 새롭게 대두되고 있다. 이에 해외 주요 기관에서는 관련 이해관계자들에게 가이드라인과 소비자 체크리스트를 발표하고 있다. 국내의 경우 가이드라인은 있으나, 소비자의 프라이버시 역량 강화를 위한 노력이 미흡하다. 이에 본 연구에서는 국내외 모바일 앱 프라이버시 관련 가이드라인을 살펴보고, 앱 사용단계별로 소비자가 경험할 수 있는 프라이버시 위험 요인을 「개인정보보호법」에 근거하여 내용을 분석하는 것을 통해 소비자의 자율적 프라이버시 보호를 위한 체크리스트를 제시하였다. 이 체크리스트는 소비자들의 프라이버시 자율관리 역량 강화에 도움이 될 것이며, 이는 모바일 생태계의 선순환 구조를 마련하는데 일조할 것이다.

주제어 : 모바일 앱, 프라이버시, 자율관리, 사용단계, 체크리스트, 융복합

Abstract In recent years, the privacy concern for mobile consumers is emerging as the use of mobile application(apps) is growing according to the rapid spread of mobile devices such as smart phones and tablet PCs. To improve privacy protections in the mobile communications and apps, overseas organizations are announcing guidelines and/or checklists for stake holders. Although personal information protection guidelines for application developers have been prepared in the country, efforts to improve consumer privacy capability is insufficient. Thus, in this paper we first scope the app privacy related guidelines in both domestic and foreign affairs, then present the risk factors of privacy invasion by the stage of mobile application use based on the 「Privacy Protection Act」, offering privacy checklists for consumers. This checklist will enhance the self-management capability of consumer privacy and create virtuous cycle in the mobile ecosystem.

Key Words : Mobile App, Privacy, Self-Management, App user stage, stage of use, Checklist, Convergence

* This article was supported by 2015 Social Science Korea(SSK).
* The first author Hua-Yu Li is supported by the governmental scholarship from the China Scholarship Council(CSC).
Received 17 March 2015, Revised 27 May 2015
Accepted 20 June 2015
Corresponding Author: Lin-Ah Kim(Seoul National University)
Email: linah1108@snu.ac.kr

ISSN: 1738-1916

1. 서론

2012년에 이미 10억 명을 돌파한 전 세계 스마트폰 이용자 수는 2014년에 이미 17억 5천만 명에 이른 것으로 전망되었으며[1], 이와 더불어 모바일 앱의 사용도 증가하고 있다. Gartner의 보고서에 따르면, 2015년에 앱 스토어에서의 연간 앱 다운로드 수가 1796억을 초과할 것이며[2], 스트라베이스의 통계자료에서는 2015년 전 세계 앱마켓 시장 규모가 전년 대비 22.7% 증가한 212억 달러에 이를 것으로 전망하였고, 이는 계속 증가되는 추세라고 밝혔다[3].

스마트폰 어플리케이션은 소비자들에게 여러 가지 다양한 서비스를 제공해 주고 있다. 소비자들은 어플리케이션을 통해 책을 읽고, 게임을 하며, 음악을 감상하고, 사진 및 비디오 등을 촬영한다. 또한 근처의 레스토랑을 찾을 수도 있으며, 물건을 구매하고, 자신의 심장박동을 모니터 할 수도 있다. 그러나 이와 같이 어플리케이션의 기능이 날로 늘어남에 따라 프라이버시에 대한 우려도 증가하고 있다. 최근 미국의 전국 조사에 따르면, 앱 이용자의 57%가 개인정보 때문에 앱을 설치하지 않았거나 앱 설치를 거절한 것으로 나타났다[4]. TRUSTe의 미국인 1천명을 대상으로 진행한 조사보고서에서는 대상자의 38%가 모바일 애플리케이션 이용 시 가장 크게 우려되는 사항으로 프라이버시를 꼽았고, 68%가 스마트폰에서의 광고가 위치 정보 등을 통해 자신들을 추적하는 것을 선호하지 않았으며, 98%가 스마트폰과 앱에 의해 수집되고 사용되는 자신의 개인 정보에 대해 더 잘 통제할 수 있기를 바라는 것으로 나타났다[5].

데스크탑 PC 등 기존의 정보통신기기와는 달리, 스마트폰은 개인화된 기기이며, 소비자가 항상 가까이에 지니고 다닌다는 점에서 기존 환경과는 비교할 수 없이 많은 정보를 수집할 수 있다. 수집된 정보는 '쉽게 결합해' 개인 식별 가능성이 높아지게 되고, 모바일 에코시스템의 복잡성으로 인해 다양한 주체들에 의해 공유 및 활용될 수 있다[6]. 또한 다양한 센서 기술의 발달로 인해 위치정보나 생체정보 등 민감도가 높은 정보도 수집, 활용될 가능성은 높아지고 있다. 반면에 스마트폰 앱을 통해 어떠한 정보가 수집, 활용되는지에 대한 소비자의 인지는 매우 낮은 수준이고, 디바이스의 소형화로 인해 스마트 폰 인터페이스를 이용해서 소비자에게 개인정보활용 관련 정보를 제공하고, 이와 관련된 소비자의 동의를 구하는 과정은 매우 제한적일 수밖에 없는 현실이다[7]. 이러한 모바일 환경의 특수성 때문에 모바일 에코시스템의 이해관계자 모두가 프라이버시에 대해 관심을 기울이는 것이 필요하다.

이에 미국, 영국, 호주, 캐나다 등 세계 주요 국가에서는 모바일에서의 프라이버시 중요성을 인식하고 이해관계자를 위한 가이드라인을 발표하였다[7,8,9,10,11]. 특히, IPC (Information and Privacy Commission)와 FTC에서는 소비자가 자율적으로 프라이버시를 관리하고, 개인정보 유출 피해를 최소화하기 위해 관련 체크리스트를 제작, 발표하였다[12,13]. 이는 서비스 이용의 주체이고, 수집되는 개인정보의 주체인 소비자 스스로가 자신의 프라이버시를 보호하고 통제할 수 있는 프라이버시 자율관리(Privacy self- management) 역량이 필요하다는 인식에서 기인한 조치라 할 수 있다. Solove(2013)는 개인정보를 정보주체가 스스로 통제할 수 있는 권한과 함께 소비자 스스로가 자신의 개인정보의 활용에 대한 의사결정을 내릴 수 있는 역량이 필요함을 강조하였고, 이러한 역량을 프라이버시 자율관리역량이라고 정의하였다[14].

국내에서도 최근 방송통신위원회와 한국인터넷진흥원에서 앱 개발자를 위한 개인정보보호안내서를 발행하였지만[15,16], 정보주체인 소비자가 자율적으로 프라이버시 보호를 할 수 있게 도와주는 조치는 미흡한 실정이다. 모바일 환경에서 사업자에게만 의존하여 프라이버시를 보호하는 것은 제한적일 수밖에 없다는 점에서, 국내에서도 소비자의 프라이버시 자율관리역량을 강화하는 방안을 모색할 필요가 있다.

이에 본 연구에서는 모바일 앱에서의 국내외 최신 프라이버시 관련 가이드라인 현황을 고찰하고, 모바일 앱 사용에 있어서 소비자가 경험하는 프라이버시 위험 요인을 도출하고, 소비자가 자율적으로 프라이버시를 관리하고 보호하는 것을 도울 수 있는 소비자의 앱 이용행태를 고려한 소비자 체크리스트를 제안하고자 한다.

2. 모바일에서의 소비자 프라이버시

2.1 모바일 앱 및 시장 현황

스마트폰은 PC와 같이 범용 운영체제를 탑재하여 다

양한 모바일 앱을 자유롭게 설치 및 실행할 수 있는 휴대폰이다[17]. 2015년 전 세계적으로 보급될 모바일기기의 수는 74억대로 세계 인구수를 추월할 것으로 전망되고 있으며 국내 또한 2014년 스마트폰 사용률이 80%에 달하였다[18].

스마트폰이 가져온 가장 큰 생활의 변화는 모바일 앱을 통한 다양한 서비스의 활용이라 할 수 있다. 모바일 앱은 스마트폰, 태블릿 PC 등 모바일 기기에서 실행되는 응용 소프트웨어(Application Software)로서 워드프로세서, 게임, 지도 등 다양한 서비스를 제공한다. 소비자들은 애플리케이션 스토어 즉 플랫폼을 방문하여 자신이 원하는 앱을 손쉽게 모바일 기기에 다운로드 받아 설치하고 삭제할 수 있다는 특징을 지닌다[19].

Gartner 보고서에 따르면 2015년에 앱 스토어에서의 연간 앱 다운로드 수가 1796억을 초과할 것이며[2], 전 세계 앱 마켓 시장 규모는 전년 대비 22.7% 증가한 212억 달러에 이를 것으로 전망하였다[3]. 한국인터넷진흥원의 조사에 의하면, 스마트폰 이용 계기는 '다양한 응용 소프트웨어(모바일 앱 등)를 이용하고 싶어서(69.1%)'인 것으로 나타나 소비자의 앱 사용이 스마트폰에서 큰 비중을 차지하는 것을 알 수 있다[19].

2.2 모바일에서의 소비자 프라이버시 중요성

국내 모바일 앱 다운로드 및 설치 이용률이 꾸준히 증가하는 가운데, 모바일 앱 상 개인정보 수집 및 활용에 따른 프라이버시 침해에 대한 관심이 대두되고 있다. 특히 PC에서와는 다른 모바일 고유의 특징 때문에 모바일 환경에서의 개인정보보호는 더욱 중요한 이슈라 할 수 있다.

첫째, 모바일은 개인적인 기기이며, 개인이 항상 휴대하는 기기이다. 따라서 PC 기반의 환경보다 훨씬 많은 양의 개인정보를 수집할 수 있고, 수집되는 정보는 더욱 사적이고 개인적인 성격을 지닌다[6,7].

둘째, 모바일 기기에 대한 정보 자체가 특정 개인을 알아 볼 수 있는 고유 식별정보가 될 수 있는 가능성도 매우 높은 것은 물론이고, 연락처, 신용카드 및 결제정보, 전화/메시지 기록, 탐색기록, 이메일, 사진 및 비디오 등 개인의 사생활에 대한 정보가 집약적으로 축적되어 있으며, GPS, 지문 탐지기 등 센서로 인한 위치정보, 생체정보 등의 민감한 정보에 대한 접근이 용이하다 [6,7,8].

셋째, PC보다 훨씬 더 작은 스크린은 사업자와 이용자 사이 커뮤니케이션에 있어서 걸림돌이 된다. PC에서도 읽지 않았던 개인정보취급방침을 모바일에서는 그보다 작은 스크린에서 봐야함에 따라 가독성이 낮으며, 접근이 용이하지도 않기 때문에 확인을 꺼리게 되는 것이다. 따라서 사업자는 개인정보보호와 관련하여 소비자와 소통할 수 있는 하나의 중요한 수단을 잃게 된다[9].

넷째, PC 기반의 온라인 서비스와는 달리 모바일 환경에서는 운영 시스템 제공자, 앱 플랫폼 제공자, 통신사업자, 단말기 제조사 등 여러 이해관계자들이 복잡한 관계를 맺고 있다. 따라서 수집되는 개인정보는 소비자가 인지하지 못하는 상황에서 더 많은 사업자에게 흘러 들어갈 가능성이 있다[7,8].

3. 모바일 프라이버시 가이드라인 현황

모바일 환경에서 앱 사용의 증가와 함께 앱 사용 시 프라이버시 이슈도 다양하게 나타나고 있다. 이에 국내외 주요 기관에서는 모바일 환경에서 소비자의 프라이버시를 보호하기 위하여 가이드라인을 제시하는 등 빠르게 대응 하고 있다.

3.1 해외 가이드라인

3.1.1 FTC

FTC는 2013년 2월, 모바일 기기에서의 프라이버시 우려를 표출하며 "Mobile Privacy Disclosures: Building Trust Trough Transparency"를 발행하였다[8]. 위원회는 사업자들의 지속적인 개인정보 수집 및 사용에 있어, 개발 단계에서부터 프라이버시가 고려되어야 하며 적절한 시간과 맥락을 고려한 선택옵션을 제공해야 함과 동시에 수집하는 정보에 대해 자세히 고지해야 하는 원칙을 제시하였다. 주로 각 이해관계자들을 대상으로 가이드라인을 제시하였는데, 개발자들에게는 플랫폼의 앱 스토어에서 개인정보보호정책을 볼 수 있도록 해야 하고 적시에 고지를 하며 긍정적 동의를 획득하여야 한다고 하였다. 또한 광고업자들과 앱에 대한 서비스를 제공하는 제3자와의 협업을 개선시켜 소비자들에게 진실 된 정보고지를 할 수 있도록 해야 함을 강조했다. 앱 시장의 문지기 역할을 하는 플랫폼은 앱 개발자들에게 영향력을

행사할 수 있기에 요구사항을 설정하거나, 이를 충족시키지 못하는 앱의 허용을 거부할 수 있는 효력을 발생시키도록 하였다. 그 중에서도 특히 소비자 이해도를 특정하기 위한 소비자조사와 효과적인 소비자 교육 캠페인을 앱 개발자들을 대표하는 거래기관 및 단체들이 학계, 프라이버시 전문가, 개발자들과 함께 협업하여 시행할 것을 강조하였다. 이는 앱 개발자를 포함한 이해관계자들이 소비자들에게 효과적으로 정보를 제공할 의무를 지니기 때문이라고 명시하였다.

3.1.2 영국 (ICO)

2013년 12월 영국의 정보위원회는 앱 개발자들을 위해 “Privacy in mobile apps”라는 가이드라인을 발표하였다[7]. 본 가이드라인은 앱에서 개인정보를 다루고 있는지를 확인하는 기준, 개인정보를 다루는 주체, 수집하는 데이터, 이용자에게 충분히 고시하고 동의를 구하는 방법, 이용자에게 피드백을 주는 방법, 수집한 데이터의 보안, 앱 테스트와 유지, 나아가 다른 중요한 합법적 고려요소들에 대해 제시하고 있다.

주요 내용을 살펴보면, 최소한의 데이터를 수집할 것, 불필요한 데이터는 삭제할 것, 디자인 단계에서 접근, 수집, 전달할 수 있는 데이터 유형을 고려하고, 이용자들에게 어떠한 영향을 주는지에 대해서 고민할 것을 제안하고 있다. 또한 어린이를 대상으로 하는 앱에서는 더욱 주의할 것을 강조한다. 만약 사용량 혹은 오류 데이터를 수집하려면 반드시 이용자에게 충분한 동의를 구하여야 하거나, 익명처리가 된 데이터를 사용하여야 한다고 제안한다. 특히 프라이버시 방침은 폭넓은 최종 이용자를 위한 쉬운 용어와 투명한 수집 목적 및 이유를 명시하여 소비자들의 이해력을 높일 수 있도록 노력해야 한다고 강조한다. 구체적인 시행방법의 예로는 이용자가 앱을 다운로드 하기 이전에 프라이버시 방침을 확인할 수 있도록 하고 이를 가능하다면 다층적(layered) 접근 방식으로 나타내며 색깔이나 아이콘 등을 사용하기를 장려하였다.

3.1.3 미국 캘리포니아 주 (CDJ)

미국은 시장의 자율규제에 입각한 소비자의 권리보호에 초점을 두고 각 주정부에서 독자적인 법률을 통해 개인정보보호에 관한 사항을 규율한다. 이에 캘리포니아 주에서는 2013년 6월에 “Privacy on the Go” 라는 보고서를 발표하였다[9].

주 내용으로는 앱 개발자들은 체크리스트를 준비하여 앱에서 수집할 수 있는 데이터가 개인 식별 정보인지를 확인하고, 개인정보는 최소한의 수집 범위로 한정해야 한다는 점을 명시하고 있다. 특히 주목할 것은 이용자가 쉽게 접근할 수 있도록 프라이버시 방침은 명확하고 정확하해야 하고, 간결하게 제시되어서 이용자들이 의미있는 선택을 할 수 있도록 장려해야 함을 강조한다. 뿐만 아니라 이용자에 대한 고려의 중요성을 강조하면서, 이용자가 앱을 다운로드하기 전에 읽을 수 있도록 플랫폼에서 용이한 접근방안을 제시하고, 운영체제와 제조사들은 글로벌 프라이버시 설정을 개발하여 이용자가 앱에서 접근할 수 있는 데이터와 디바이스 특징에 대해 통제가 가능하도록 해야 할 것을 제안하고 있다. 그 밖에 제3자는 브라우저 설정을 수정하거나 out-of-app 광고는 배제해야 하며 디바이스의 특정 식별정보는 앱 특정 식별정보 혹은 일시적인 디바이스 식별정보를 사용하는 것으로 한정시키고 있다. 모바일유통업자 또한 모바일 소비자들과의 관계를 이용하여 어린이 프라이버시 중요성을 교육해야 한다는 내용도 포함되어 있다.

3.1.4 호주 (OAIC)

호주에서도 모바일 앱 이용 증가에 다른 프라이버시 침해 우려가 고조되면서 호주 정보위원회(OAIC)에서는 모바일 앱 프라이버시 향상을 위해 앱 개발자들이 프라이버시 보호를 준수하기 위해 고려해야 할 사안들과 적용방법을 담은 ‘모바일 프라이버시 가이드라인’을 수립하였다[10]. 구체적으로는 프라이버시 정책 마련 및 공지방식, 수집할 개인정보의 종류와 활용정도 등을 제안하고 있는데, 특히 앱 개발자들이 직접 프라이버시 보호 준수 여부를 판단할 수 있도록 각각의 사안들을 체크리스트 형태로 제공하고 있다.

이용자를 위한 ‘Privacy by Design’ 원칙을 전제로 모바일 앱 프라이버시 준수를 위하여 앱 개발자들은 프라이버시 보호책임의 이행, 개방적이고 투명한 프라이버시 보호 방안의 운영, 개인정보 처리 방침의 전달 방식이 스마트폰의 특성인 작은 화면을 고려하여 적용되어야 할 것이며, 개인정보 수집에 대한 공지 및 동의 요청 시점을 적절하게 설정하고, 개인정보 수집 범위는 최소화로 한정하며, 그리고 수집한 개인정보의 보안 대책을 설정해

야 함을 강조하였다.

3.1.5 캐나다

캐나다는 모바일 환경에서 앱 경제 활성화에 반해 우려되는 소비자 개인정보 침해문제를 해결하기 위하여 Privacy Commissioner of Canada, Alberta and British Columbia에서 2012년 4월, 앱 개발자들을 위한 프라이버시 가이드라인을 제시하였다[11].

가이드라인에는 이용자들이 앱을 다운로드 하기 이전에 수집하는 개인정보에 대해 명확한 내용으로 고지해야 하며 수집 목적과 정보가 어디에 저장되는지, 누구와 공유되는지, 보유기간은 어떠한지에 대한 내용이 포함되어야 한다고 제안한다. 특히 이용자 측면을 배려하여 이용자들이 앱을 사용할 시에는 모니터링 프로그램을 가지고 제시하고 있는 개인정보취급방침에 따라 모니터링 프로그램을 구축해야 하며, 구체적이고 맞춤화된 고지를 한 후 동의획득이 필요하다는 내용과 함께 앱의 기능을 수행하기 위한 최소한의 수집과 보안상 취약하지 않도록 시스템 및 코딩을 암호화 처리하는 것 또한 필요하다고 명시하였다. 이에 더불어 모바일의 작은 화면을 고려한 layered된 방식으로 정보를 제공하고, 프라이버시 대시보드(게시판)을 제공하여 소비자들이 프라이버시 설정을 바꿀 수 있도록 허용해야 하고, 개인정보취급방침의 내용은 그래픽, 컬러, 소리 등을 이용하여 이용자에게 효과적으로 전달이 되도록 해야 함을 강조하고 있어 프라이버시에 보호를 위해 소비자가 쉽게 이해하고 접근할 수 있도록 노력하고 있는 것을 알 수 있다.

3.2 국내 가이드라인

3.2.1 방송통신위원회, 한국인터넷진흥원

방송통신위원회와 한국인터넷진흥원에서는 2012년 “앱 개발자를 위한 개인정보보호 안내서”를 발행하였다[15]. 주 내용으로는 앱 개발자가 앱 개발 준비 시, 개인정보 수집 최소화하고 신뢰할 수 있는 개발 툴을 이용하며, 소스코드상의 취약점 최소화하기 위해 보안코딩을 적용하고 앱 개발자와 서비스 제공자는 서비스 전반에 대한 보안대책을 마련해야 하고 개인정보보호 관련 법률을 검토하여 반영해야 한다고 언급하였다. 또한 이용자가 알아야 할 개인정보보호에 관한 사항을 ‘개인정보취급방침’으로 정하여 공개해야 하고, 이용자에게 개인정보 수집 및 이용(수집하는 개인정보의 항목, 개인정보의 수집 및 이용목적, 개인정보 보유 및 이용기간)에 대한 동의 획득해야 하고, 민감한 개인정보는 수집하지 않으며 제3자에게 개인정보 제공시 이용자에게 알리고 동의획득, 미성년자 개인정보 수집 시 법정대리인 동의 획득이 필요함을 제안한다. 더불어 주민등록번호의 사용 제한, 수집목적에 한해서만 이용하며, 불법적 접근 및 안전한 저장·전송을 위하여 암호화 기술 및 접근통제 설비 등을 운영해야 하고. 개인정보의 수집 목적 달성 및 이용기간의 종료하는 경우 즉시 폐기해야 한다고 명시되어 있다.

3.2.2 행정안전부

행정안전부는 뉴미디어 서비스이용·제공시 개인정보 침해사고 예방을 위해 준수해야 할 사항에 대한 가이드라인 제시를 목적으로 보고서를 발행하였다[16]. 뉴미디어 서비스 제공자 대상 가이드라인의 내용으로는 서비스 이용자가 쉽게 확인할 수 있도록 개인정보취급방침을 수립해야 하고, 개인정보 보호 관리 책임자 지정, 최소한의 정보수집원칙, 이용자로부터 동의 받은 범위 및 목적 내 이용·제공, 사전에 개인정보 위탁 목적, 범위, 대상 등에 반드시 고지, 개인정보 공개범위를 서비스 이용을 위해 필요한 최소한의 정보 제외하고 공개안함으로 하고, 개인정보 처리목적 달성 후 파기, 보호조치, 개인정보 국외 이전하는 경우 국내의 관련 법 의무사항 준수, 양도 시 고지의무, 그리고 유출사고 발생 시 이용자에게 고지하고 피해를 최소화하기 위해 노력해야 하는 내용을 포함한다.

뉴미디어 서비스 이용자의 10개 가이드라인 내용으로는 정보제공 최소화, 보호조치 확인, 공개범위 최소화, 정기적 업데이트, 중요정보의 안전한 관리, 기능 비활성화, 신중한 정보공유, 아동의 개인정보보호 인식제고, 권리보장, 그리고 침해신고에 대한 내용을 제시하고 있다.

3.3 소결

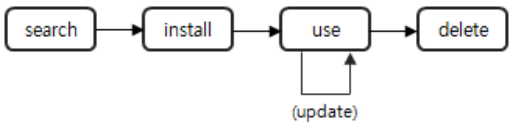
해외 및 국내 기관에서 제공하고 있는 모바일 프라이버시와 관련된 가이드라인을 살펴본 결과, 해외의 경우 전반적으로 소비자가 쉽게 접근하고, 프라이버시 보호를 위해 효과적으로 활용할 수 방법에 대한 고민을 많이 하고 있었다. 또한 세계 각국의 기관에서는 공통으로 모바일 프라이버시의 쟁점이 소비자의 인식과 이해의 부족이

가장 큰 원인이라고 지적하였다.

반면, 국내의 경우 딱딱한 법적 용어로 작성되어 있고, 포괄적인 내용이라 소비자들이 이해하고 활용하기에 어려움이 존재하는 것을 알 수 있었다.

4. 앱 사용단계별 소비자 프라이버시 침해요인

소비자는 최종적으로 앱을 사용하기까지 여러 단계를 거치게 된다. 앱 추천 시스템의 소비자중심 평가 틀을 개발한 Bohmer 외(2013)의 연구에서는 플랫폼에서 앱의 추천이 이루어진 후, 소비자가 앱을 오랜 시간동안 사용하기까지 탐색하는 단계, 설치하는 단계, 직접 사용하는 단계, 장기간 사용하는 단계 등 네 가지 단계를 거친다고 하였다[20]. 이를 기초로 본 연구에서는 앱 사용 단계에 앱 업데이트 단계를 추가하여 소비자의 전반적인 앱 사용단계를 [Fig. 1]에서와 같이 정의하였다. 구체적으로 플랫폼을 방문하여 관련 앱을 검색하는 단계, 앱 설치 단계, 앱 사용 및 사용 중 업데이트 단계, 그리고 최종적으로 앱을 삭제하는 단계로 구분하였다. 그리고 각 단계별로 국내 「개인정보보호법」에 근거를 두고 있지만[21], 온전히 보장되고 있지 않는 몇 가지 정보주체 권리에 대한 이슈에 대해 살펴보았다.

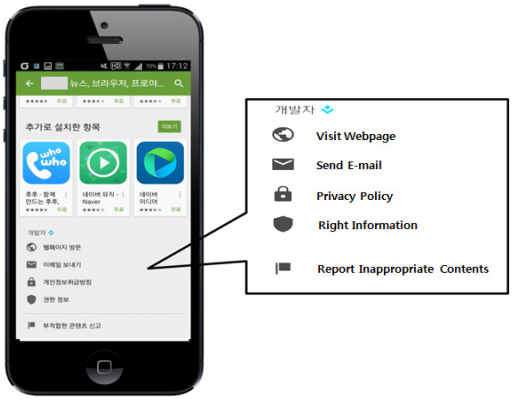


[Fig. 1] Consumer App Usage Stage

4.1 앱 검색 단계

앱을 사용하기 위해서 소비자들은 앱에 대한 정보를 획득하기 위해 앱 마켓 즉 플랫폼에서 관련 앱을 검색한다. 이 때 프라이버시와 관련해서 다음과 같은 문제점이 존재한다.

첫째, [Fig. 2][1]에서 살펴볼 수 있듯이 플랫폼 상에서는 앱의 일부 콘텐츠, 소비자의 사용 리뷰, 유사한 앱의 추천 정보 등이 제시되고 있다. 그러나 앱을 설치하기 전에 소비자가 확인해야 할 개인정보취급방침은 누락되어 있거나 페이지의 맨 밑단에서 확인을 해야 하기 때문에 스크롤을 내려야 하는 불편함이 존재한다. 이는 「개인정보보호법」 제4조에서 제시한 정보주체의 권리 중 개인정보의 처리에 관한 정보를 제공받을 권리가 잘 보장되고 있지 않음을 보여준다.



[Fig. 2] Example of App Search Stage

둘째, 플랫폼에서 앱의 개인정보취급방침을 클릭하면 웹페이지에서 제공하고 있는 개인정보취급방침의 새로운 페이지로 이동하게 된다. 즉 작은 스크린의 특성을 고려하지 않고, PC상에서 제공되고 있는 형식 그대로 제시하고 있는 경우가 많다. 따라서 가독성이 현저히 떨어진다. 또한 검색 단계에서 표준화된 양식으로 개인정보취급방침에 관한 정보를 제공받고 있지 못하기에 플랫폼 상에서 비슷한 앱들의 프라이버시 정책을 직접 비교하는 것이 불가능하다. 즉 소비자가 어떠한 앱이 프라이버시를 잘 보호하는지에 대해 확인할 수 있는 방법이 불투명하다.

4.2 앱 설치 단계

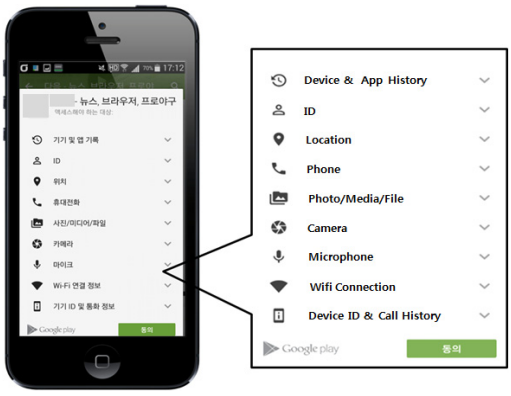
앱 검색이 이루어 진 이후 해당 앱을 사용하기 전에 설치단계로 이동하게 된다. 이 단계에서 발생하는 문제점은 다음과 같다.

첫째, 앱을 사용하기 위해 제공되어야 할 소비자의 개인정보가 최소한으로 수집되고 있는지에 대해 의문을 던

1) [Fig.2]부터 [Fig.5]까지는 2015년 3월 D사의 앱이 스마트폰에서 앱 마켓을 통해 탐색, 다운로드, 설치, 사용 및 삭제에 이르기까지의 화면을 캡처한 것이다.

질 필요가 있다. [Fig. 3]에서와 같이 '설치' 버튼을 클릭한 후 제시되는 '엑세스해야 하는 대상'에는 기기 및 앱 기록, 휴대전화, 사진·미디어·파일, 통화 정보 등이 포함되고 있다. 그러나 '사진/미디어/파일' 등과 같은 정보는 소비자에게 민감한 정보가 될 수 있음에도 불구하고 수집하고 있는 것을 확인할 수 있다. 한때 웹사이트에 회원가입을 하거나 매장에서 맴버십 카드를 만들 때 주민등록번호를 요구하는 것이 보편적이었다. 2013년 국회입법조사처의 자료에 의하면 32만여 개에 이르는 우리나라 웹사이트 중 92.5%가 주민번호를 불필요하게 수집하고 있었다[22]. 그러나 관련 문제가 제기되면서 정부에서는 개정된 「개인정보보호법」에 근거하여 2014년 8월 7일부터 주민등록번호의 수집을 원칙적으로 금지하고 있다. 현재 앱에서도 같은 문제점이 존재하고, 소비자들은 어떠한 정보가 최소한의 정보인지를 확인할 방법이 없다.

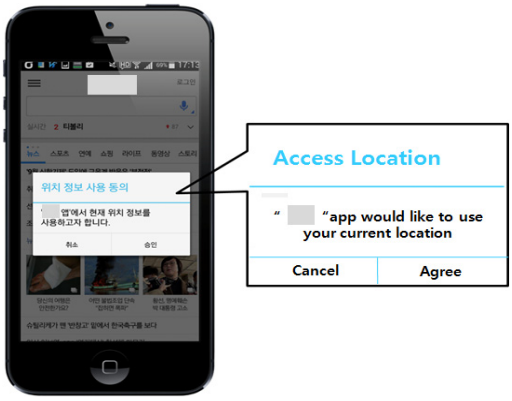
둘째, [Fig. 3]에서와 같이, 동의 획득 단계에서 수집하는 정보에 대해 포괄적 동의가 이루어지고 있다. 즉, 소비자들은 제공하고 싶지 않은 정보가 있더라도 포괄적 동의로 인해 앱을 사용하기 위해서는 다른 선택의 여지가 없이 동의버튼을 눌러야 할 수 밖에 없는 상황에 놓인다. 이는 엄격히 말하면 「개인정보보호법」 제4조 제2항에서 제시하는 '개인정보의 처리에 관한 동의 여부, 동의 범위 등을 선택하고 결정할 권리'를 보장하고 있지 않는 것에 해당된다.



[Fig. 3] Example of App Installment Stage

4.3 앱 사용 단계

앱 설치 이후, 소비자는 앱 서비스를 사용하는 단계에 들어서게 되는데, 사용 과정에서 뿐만 아니라 업데이트 할 때 또한 프라이버시 문제를 경험하게 된다.



[Fig. 4] Example of App Use Stage

첫째, 위치정보 등 수시로 수집될 수 있는 정보는 소비자가 수집을 동의한 시점과 실제 수집되는 시점이 다를 수 있다. [Fig. 4]에서와 같이 현재 위치정보의 수집에 동의를 구하고 있지만, 앱이 종료된 후에도 지속적으로 정보를 수집하는 경우가 종종 발생하고 있다. 소비자는 언제 어디서 어떤 정보가 수집되고 있는 지를 정확히 인지하지 못하고 있고, 이러한 문제에 대해 인식도 부족하다. 뿐만 아니라 앱 업데이트 시 기존에 설정한 개인정보제공수준이 소비자의 부주의거나 제대로 인지하지 못한 상황에서 변경될 가능성도 존재한다. 이는 모두 「개인정보보호법」 제4조 제1항의 개인정보의 처리에 관한 정보를 제공받을 권리를 온전히 보장하지 않은 것에 해당되는 것이다.

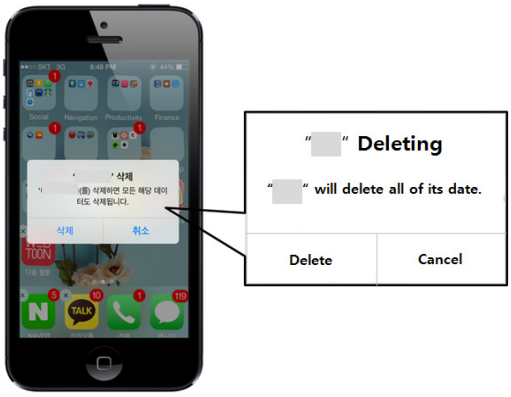
따라서 앱 사용과정에서 소비자가 스스로 개인정보 제공여부와 제공수준을 설정할 수 있고, 수시로 확인 가능한 대시보드를 마련하여 「개인정보보호법」 제4조 제1항과 제3항의 개인정보 열람권을 보장하는 것이 필요하다. 그러나 이러한 대시보드를 제공하고 있는 앱은 드문 실정이다.

둘째, 앱 업데이트 시, 개인정보의 수집 방침이 변경되었을 경우 「개인정보보호법」 제4조에서 제시한 정보주체의 개인정보 처리에 관한 정보를 제공받을 권리에 의하여 사업자는 소비자에게 이를 고지할 의무가 있다. 그러나 소비자에게 명확히 고지하지 않고 재동의절차가 생략되고 있는 문제가 보편적으로 존재한다. 즉 개인정보 수집목적 혹은 처리 자가 변경되는 경우, 소비자에게 변

경된 수집목적을 고지하여야 하고, 기존의 동의를 철회할 수 있는 옵션을 제공하여 다시 동의를 받아야 하지만 이러한 절차를 따르고 있는 앱을 찾아보기 힘들다.

4.4 앱 삭제 단계

소비자들은 더 이상 앱 서비스를 이용하고 싶지 않게 되면 앱을 삭제하게 되는데 이때 모바일 화면상에서 해당 앱이 사라지기 때문에 소비자들은 웹사이트에서 회원탈퇴를 했을 때와 같은 맥락 내에서 생각하기가 쉽다.



[Fig. 5] Example of App Delete Stage

그러나 회원탈퇴를 하지 않고 앱을 삭제한 경우에는, 한번 등록되어 있는 소비자들의 개인정보는 남아있는 경우가 많다. 축적된 정보가 추후에 다른 정보와 결합하여 파생적인 정보를 생산할 수 있다는 점에서 소비자 프라이버시에 큰 영향을 줄 수 있다. [Fig. 5]와 같이 앱을 삭제하는 버튼을 누르면 '앱을 삭제하면, 모든 해당 데이터도 삭제 합니다'라는 알림문구가 나타나지만, 해당 데이터에 개인정보에 관련한 내용도 삭제되는지의 여부는 알 수 없다. 소비자들은 「개인정보보호법」 제4조 제4항에서 보장하고 있는 개인정보의 처리 정지, 정정·삭제 및 파기를 요구할 권리를 가지고 있기 때문에 이 부분을 명확하게 고지할 필요가 있다.

5. 모바일 앱 프라이버시 체크리스트 제안

모바일 환경에서 소비자의 프라이버시를 보호하기 위해서는 시스템 개발 및 관리 차원에서 기술적인 개선도 필요하지만 소비자가 자율적으로 자신의 프라이버시를 보호하고 관리할 수 있는 역량도 필요하다. 소비자는 프라이버시를 사업자에 의해 보호되어야 한다는 입장 보다는 스스로 지켜야 한다는 주체적인 입장에서 바라보아야 한다. 특히 사용하고 있는 앱의 개인정보취급방침과 해당 앱에서의 자신의 프라이버시 설정권한을 정기적으로 확인할 필요가 있지만, 현재 확인이 필요한 항목에 대해 명확한 기준이 없는 실정이고, 소비자들이 자율적으로 프라이버시를 보호하고자 하여도 올바른 대체방법에 대한 정보가 부족하다. 따라서 소비자들의 자율적인 프라이버시 보호를 위해 반드시 확인해야 할 항목들을 체크리스트 방식으로 제시하여 소비자들이 체계적으로 프라이버시를 관리할 수 있도록 인도하는 것이 필요하다.

5.1 프라이버시 자율관리

현재 프라이버시 보호를 위한 노력은 주로 기술적 환경을 개선시키기 위해 사업자 중심에 초점이 맞춰져 있다. 그러나 언제, 어디서나 접근 가능한 모바일 특성상 기술로 통제할 수 있는 부분은 제한적이다. 이에 소비자에게도 자율적으로 프라이버시를 보호하고 통제할 수 있는 역량을 요구한다. Solove(2013)는 이 역량을 프라이버시 자율관리라고 정의하고 있다[20]. 즉 법적으로 개인정보를 스스로 통제할 수 있는 권한이 보장된 것을 통해 소비자가 자신의 정보가 수집, 사용 또는 노출되는 것에 대하여 효용과 비용을 저울질 할 수 있는 것을 의미한다.

특히 일상에서 만나는 사람에게 항상 같은 정보를 제공하지 않듯이 소비자들 또한 모바일 앱을 사용할 때, 언제나 동일한 수준의 정보를 제공해야 할 이유가 없다. 즉, 맥락과 상황에 따라 자신의 프라이버시 보호수준을 다르게 설정할 수 있어야 한다[23].

그러나 앱 사용의 주체이고, 앱에서 수집하고 있는 개인정보의 주체인 소비자는 사실상 자신이 개인정보 제공수준을 맥락에 따라 설정할 수 있다는 것조차 인지하지 못하고 있다. 소비자는 프라이버시가 보호되는 것이 아니라 능동적으로 보호해야 된다는 것을 인지하고 프라이버시 자율관리를 위해 노력해야 한다. 이를 위해 소비자는 맥락 내에서 자신의 개인정보 제공수준을 결정할 수 있어야 하며, 수집된 개인정보가 어떻게 어디에서 활용이 되는지 등에 대해 알 필요가 있다. 따라서 모바일 앱 프라이버시를 보호하기 위해 필수적으로 확인해 할 체크

리스트가 필요하다.

5.2 프라이버시 관련 소비자 체크리스트 사례

FTC의 보고서(2013)에 의하면 미국에서 다른 사람의 개인정보를 도용하여 제품이나 서비스를 구매하는 명의 도용 범죄로 인한 피해가 매우 심각한 수준이라고 한다. 이에 2013년 5월 미국 SEC(Securities and Exchange Commission)는 CFTC(Commodity Futures Trading Commission)와 FTC의 협력으로 신원 도용을 예방·탐지·대응할 수 있도록 "Regulation S-ID: Identity Theft Red Flags"를 수립하고 SEC와 CFTC에 등록된 모든 기관에 이를 준수할 것을 요구하였다[24]. 같은 해 9월 FTC는 "Guide for Assisting Identity Theft Victims"를 발표하였고, 부록에 신원도용을 당한 피해자들의 손실을 최소화하기 위해 각 기관에서 이용할 수 있는 체크리스트를 첨부하였다[13].

이와 유사하게 미국의 정부기관과 단체들에서는 소비자들이 스스로를 보호하고, 피해를 최소화하기 위해 사용할 수 있는 체크리스트를 개발, 제공하고 있다. 일례로 미국 법무부는 "Identity Theft Checklist"는 도용당할 수 있는 정보, 신원이 도용당함을 알아차릴 수 있는 방법, 신원을 도용당한 후의 세 단계 대응절차에 관련한 내용을 포함하는 체크리스트를 개발, 배포하고 있다. 또한 FTC에서 신원도용 피해자를 위해 운영되고 있는 사이트(IdentityTheft.gov)에도 소비자를 위한 체크리스트가 일목요연하게 제시되어 있으며, Teachers Credit Union에서도 피해자들을 위한 "Identity Theft Victim Checklist"를 제공하고 있다.

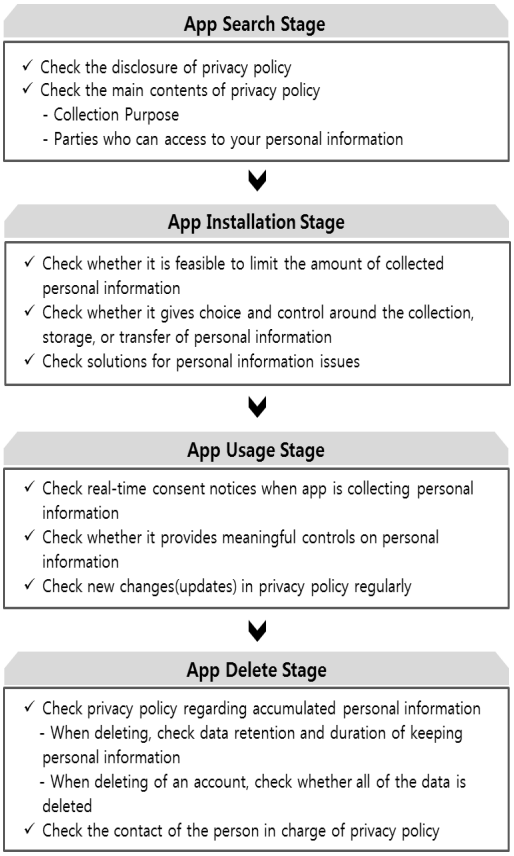
모바일 프라이버시와 관련한 체크리스트의 사례로는 IPC (Information and Privacy Commission)에서 2014년 5월에 발표한 "Mobile apps: know the risks" 있다[12]. 이 보고서에서는 모바일 앱을 사용하는 소비자들이 자율적으로 모바일 프라이버시를 관리할 수 있도록 여섯 가지 항목으로 구성된 체크리스트를 제시하고 있다.

국내의 경우 모바일 앱 프라이버시 보호를 위한 소비자 체크리스트는 아직 제안된 바 없지만, 유사한 맥락에서 개인정보유출 사태를 대응하기 위해 금융위원회에서 개발, 발표한 2014년 4월 "개인정보 유출 관련 필수체크사항 10가지"와 같이 소비자가 스스로의 개인정보보호를 위해 알아야 하는 내용을 정리, 공유하고자 하는 노력이 이루어지고 있음을 알 수 있다.

한국인터넷진흥원(2013)에서도 최근 신원정보를 도용하여 범죄에 사용하는 사례가 증가함에 따라 도용이 의심되거나 피해가 발생할 경우, 소비자가 대응할 수 있는 절차를 체크리스트 형식으로 개발하여 기관 및 소비자에게 제공할 필요가 있다고 주장한 바 있다[25].

5.3 모바일 앱 프라이버시 체크리스트 내용

모바일 환경에서 소비자 프라이버시 침해요인과 「개인정보보호법」에서 보장하고 있는 정보주체의 권리에 근거하여 앱 사용 단계별로 프라이버시 보호를 위한 체크리스트를 구성하면 [Fig. 6]과 같다.



[Fig. 6] Mobile App Privacy Checklist for Consumer

첫째, 앱을 검색하는 단계에서 소비자는 먼저 플랫폼에서 해당 앱의 개인정보취급방침을 확인하고 주요내용

을 파악할 필요가 있다. 이를 통해 자신의 개인정보를 무엇 때문에 수집하고, 누구에 의해 처리되고, 누구랑 공유하는지를 확인할 수 있으며, 이는 앱의 사용여부를 결정하는 데에 도움이 될 것이다.

둘째, 앱을 설치하는 단계에서는 최소한의 정보를 제공하여 서비스를 이용할 수 있는지를 확인하여야 한다. 서비스 이용을 위해 수집하는 정보들이 많다고 생각되면 해당 정보를 수집하는 이유와 목적을 확인할 필요가 있다. 또한 원치 않는 개인정보의 수집을 요구하는 경우, 소비자가 자신이 제공하는 개인정보들에 대해 선택을 할 수 있도록 소비자의 자기결정권을 보장하고 있는지도 확인하여야 한다. 앱을 처음 설치 할 경우, 개인정보처리 책임자의 연락 가능 방안과 그 해결방안에 대해 알아두는 것이 향후 개인정보 관련 문제가 발생했을 때 도움이 될 것이다.

셋째, 앱을 사용하는 단계에서 소비자는 수집되는 개인정보가 적절한 시점에서 고지되고 있는지를 확인하여야 한다. 또한 앱을 사용하지 않음에도 불구하고 개인정보가 수집되고 있는데 이를 인지하지 못하는 경우와 업데이트 시 설정수준이 변경되는 경우를 대비하여 프라이버시 설정기능을 숙지하는 것이 필요하고 정기적으로 설정수준을 체크하여 관리하는 것이 프라이버시 보호에 도움이 된다. 또한 개인정보취급방침이 변경될 경우 고지여부를 확인하고, 고지하지 않는 경우 정기적으로 변경된 내용이 없는지를 확인하는 것이 필요하다.

최종적으로 앱 서비스를 삭제하는 단계에서 소비자는 삭제 버튼으로 서비스 이용을 종료하였지만, 서비스 이용 시 제공한 개인정보는 결코 즉시 삭제되지 않는다는 사실을 인지해야 한다. 따라서 앱의 개인정보취급방침을 확인하여 앱을 삭제하거나 회원탈퇴를 할 경우 앱을 사용하면서 누적된 개인정보에 대한 처리 방침을 알아보는 것이 중요하다. 처리 방침에 의의가 있거나 불만족스러울 경우, 관련 내용을 처리하는 개인정보 책임자에게 연락할 수 있는 방안을 확인하여 해결할 수 있다.

6. 결론

최근 스마트폰 사용의 증가와 함께 모바일 환경에서의 개인정보 활용이 많아지면서 모바일 앱에서의 프라이버시 문제가 대두되고 잇다. 이에 해외 주요 나라들에서는 안전한 모바일 앱 생태계 조성을 위해 모바일 프라이버시 관련 이해관계자들을 대상으로 가이드라인을 마련하고 있다. 특히 프라이버시 보호를 앱 개발 단계에서부터 고려하도록 앱 개발자들에게 요구하고 있는 등 기술적인 측면에서부터 프라이버시 보호를 위해 적극적인 노력을 하고 있다. 그러나 변화하는 기술 환경에서 소비자의 프라이버시 보호를 위해서는 시스템 개발 및 관리 차원에서의 기술적인 개선도 필요하지만 소비자가 자율적으로 자신의 프라이버시를 관리하고 보호할 수 있는 프라이버시 자율관리 역량도 필요하다.

따라서 본 연구에서는 소비자가 자율적으로 프라이버시를 관리 및 보호할 수 있도록 앱 사용단계별로 프라이버시 체크리스트를 제시하였다. 첫째 검색 단계에서는 개인정보취급방침의 제공여부를 확인하고 개인정보취급방침의 주요내용을 파악하여야 한다. 둘째, 설치 단계에서는 최소한의 정보를 제공할 수 있는지, 수집되는 개인정보의 선택적 동의가 가능한지, 개인정보 관련 문제 발생 시 해결 방안을 확인 할 필요가 있다. 셋째, 앱 사용단계에서는 초기설정 외 개인정보 수집 시 실시간 고지를 하는지, 개인정보제공 수준이 변경 가능한지, 개인정보취급방침 변경 시 고지를 하고 있는지를 확인하여야 한다. 넷째, 앱 삭제 단계에서는 지금까지 누적된 개인정보의 처리방침과 개인정보 책임자의 연락 방식을 확인하는 것이 필요하다.

본 논문에서 살펴본 유사 사례의 경우 정부가 주도해서 이와 같은 체크리스트를 작성하고, 다양한 기관과 협력하여 배포하는 것이 가장 보편적이었다.

본 연구에서 제시한 체크리스트는 소비자들로 하여금 자신의 개인정보가 어떻게 사용되고 있는지에 대한 정보를 확인하게끔 유도하고, 개인정보 제공 수준을 원하는 만큼 설정하고, 피해 발생 시 해결방안에 대한 정보도 쉽게 제공받을 수 있게 한다. 이를 통해 소비자는 프라이버시 자율관리 역량이 강화되고, 똑똑해진 소비자들로 하여 사업자들은 프라이버시를 신중히 다룰 수밖에 없는 선순환 구조가 형성될 수 있다. 이러한 환경에서는 소비자의 프라이버시 보호를 위해 적극적으로 노력하고 합법적으로 사용하는 사업자가 궁극적으로 소비자의 신뢰를 획득하여 시장에서 경쟁우위를 차지할 수 있다. 이러한 선순환은 모바일 에코시스템의 건전한 발전에 일조할 수

있을 것이라 기대한다.

기존 소비자 분야에서의 개인정보 혹은 프라이버시에 관련한 연구들은 대부분 개인정보를 활용한 기술의 수용에 관한 것이고, 정작 프라이버시와 관련한 소비자의 역량을 강화하고자 한 논문은 미비하다. 본 연구에서는 소비자의 프라이버시 자율관리 역량을 강화할 수 있는 하나의 수단으로써 체크리스트를 제시하였는데 이는 향후 연구의 기초자료로 활용될 수 있을 것이다.

본 연구에서는 「개인정보보호법」에 근거를 두고 도출한 내용을 토대로, 소비자의 앱 이용단계를 고려해서 소비자들이 쉽게 이해하고 따라갈 수 있는 자율적 프라이버시 보호를 위한 체크리스트 안을 제안했다. 이를 시작으로, 이러한 개념적 모델을 실증적으로 적용하는 등의 후속연구를 통해 소비자 프라이버시 자율관리 역량을 강화할 수 있는 효율적 방안에 대한 지속적 관심이 요구되는 바이다.

ACKNOWLEDGMENTS

This article was supported by 2015 Social Science Korea(SSK). Also the first author Hua-Yu Li is supported by the governmental scholarship from the China Scholarship Council(CSC).

REFERENCES

[1] Smartphone Users Worldwide will Total 1.75 Billion in 2014, eMarketer, http://www.emarketer.com/Article/Smartphone-Users-Worldwide-Will-Total-175-Billion-2014/1010536, January 5, 2015..

[2] J. Rivera, R. van der Meulen, Gartner Says Mobile App Stores Will See Annual Downloads Reach 102 Billion in 2013, Gartner, http://www.gartner.com/newsroom/id/2592315, September 19, 2013

[3] 2014 Market closure and 2015 market outlook series(21)-App, Market, Strabase, http://www.strabase.com/contents/view.php?num=17448&leftCate, January 08, 2015.

[4] J. L. Boyles, A. Smith, M. Madden, Privacy and Data Management on Mobile Device, Pew Internet & American Life Project, September 5, 2012.

[5] Mobile Privacy: User's Perspective, TRUSTe, 2011, https://www.truste.com/resources/harris-mobile-survey/, January 06, 2015.

[6] J. Rha, Smartphone and Consumer Privacy: leakage and investigation of personal information, Korea Future Consumer Forum, 2014.

[7] Information Commissioner's Office, Privacy in mobile apps: Guidance for app developers, December, 2013.

[8] Federal Trade Commission, Mobile Privacy Disclosures: Building trust trough transparency, February 2013.

[9] California Department of Justice, K. D. Harris, Privacy on the go: Recommendations for the mobile ecosystem, January 2013.

[10] Office of the Australian Information Commissioner, Mobile Privacy: A better practice guide for mobile app developers, September 2014.

[11] Office of the Privacy Commissioner of Canada, Seizing Opportunity: Good Privacy Practices for Developing Mobile Apps, October 2012.

[12] Information and Privacy Commission, Mobile Apps: know the risks, May 2014.

[13] Federal Trade Commission, Guide for Assisting Identity Theft Victims, September 2013.

[14] D. F. Solove, Introduction: Privacy Self-Management and the Consent Dilemma, Harvard Law Review, Vol. 126, No. 7, pp1880-1903, 2013.

[15] Korea Communication Commission, Korea Internet & Security Agency, Privacy policy guidelines for app developers, 2012.

[16] Ministry of Public Administration and Security, Privacy Policy Guideline for New Media Service, January 2012.

[17] Korea Internet & Security Agency, Publication of Result in Mobile App Privacy Trend Research, September 2013.

[18] Gallup Korea , Research in Smartphone uses in 2012-2014, August 2014.
[19] H. Jo, A study on current status of Smartphone user by age and sex, Internet & Security Focus, No. 11, 35-51, 2013.
[20] M. Bohmer, L. Ganev, A. Kruger, AppFunnel: A Framework for Usage-centric Evaluation of Recommender Systems that Suggest Mobile Applications, Proceedings of the 2013 international conference on Intelligent user interfaces, pp19-22, 2013.
[21] Ministry of Government Administration and Home Affairs, Personal Information Protection Act, November 2014.
[22] Ministry of Security and Public Administration, Guideline of Prohibition of Collecting Resident Registration Number, January 2014.
[23] U. Jendricke, M. Kreutzer, A. Zugenmaier, Mobile Identity Management, Proc. 1st Workshop Security, UBICOMP, 2002.
[24] Securities and Exchange Commission, Regulation S-ID: Identity Theft Red Flags, May 2013.
[25] Cyber Security Issue in May, pp54-55, Korea Internet & Security Agency, 2013

이 화 옥(Li, Hua Yu)

- 2011년 7월 : Dongbei University of Finance and Economics(Bachelor of Management)
- 2014년 2월 : 서울대학교 소비자학과(생활과학 석사)
- 2014년 9월 ~ 현재 : 서울대학교 소비자학과(박사 과정)
- 관심분야 : 소비자 프라이버시, 소비자 정보탐색, 소비자 가치, 소비자 기대
- E-Mail : huayulee@naver.com

김 린 아(Kim, Lin Ah)

- 2013년 2월 : 한양대학교 경영학과(경영학 학사)
- 2013년 9월 ~ 현재 : 서울대학교 소비자학과 (석사 수료)
- 관심분야 : 소비자 프라이버시, 빅데이터 분석, 온라인 소비자 행동.
- E-Mail : lina24060@gmail.com

나 종 연(Rha, Jong Youn)

- 1998년 2월 : 서울대학교 소비자학과(석사)
- 2002년 6월 : The Ohio State University, Dept. of Consumer and Textile Science(박사)
- 2002년 7월 ~ 2003년 8월 : University of Delaware, Dept. of Consumer Studies, 조교수
- 2004년 3월 ~ 현재 : 서울대학교 소비자학과 교수
- 관심분야 : ICT 환경의 변화와 소비자 후생, 소비자 프라이버시
- E-Mail : jrha@snu.ac.kr