



# Barun ICT

9 & 10  
September & October  
newsletter **KOR**

바른ICT연구소는 ICT 관련 사회 현상 연구 및 대안을 모색하고 바람직한 사회적 가치를 위한 정책 방향을 제시합니다.  
빠른 IT 보다는 바르고 건전한 IT 문화 구축에 기여하는 것을 목표로 세계적인 수준의 융합 ICT 연구소를 지향합니다.

## Barun ICT Upcoming Event

### Asia Privacy Bridge Forum & Barun ICT Research Conference 2017 개최



**일 시** 2017.11.08(Wed), Main conference

**문의** 02-2123-6694, conference@barunict.kr

**장 소** 연세대학교 백양누리(The Commons) 그랜드볼룸

**등록** <http://conference2017.barunict.kr>

## 2017 ISACA Korea Conference

### 바른ICT연구소, 2017 ISACA Korea Conference 공동개최



연세대학교 정보대학원, 바른ICT연구소 및 (사)한국정보시스템감사통제협회가 공동으로 주최한 ‘2017 ISACA Korea Conference’가 지난 9월 1일(금) 연세대학교 신촌캠퍼스 새천년관에서 ‘4차 산업혁명 시대의 IT Governance와 Risk Management’라는 주제로 개최되었다. 이번 컨퍼런스는 김형철 연세대학교 철학과 교수의 ‘로봇도 윤리적인가?’ 라는 주제의 기조연설을 시작으로 총 4개의 트랙(IT 거버넌스, 위험관리, 사이버보안, APB Forum&블록체인)으로 진행되었다. 약 230명이 참가한 이번 행사에서 공공기관, 기업, 학계의 주요 인사들이 참여하며 4차 산업혁명에 따른 사회적 이슈와 다양한 정책적/기술적 대응방안에 대한 지식을 공유하는 장이 마련되었다.



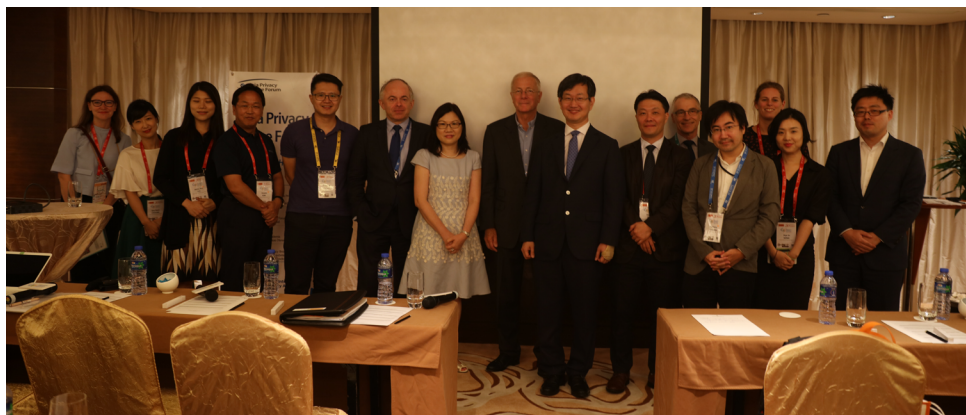
Track 4 APB Forum 세션에서는 OECD 정보보호작업반 부의장을 맡고 있는 김범수 바른ICT연구소장이 국제사회 속 개인정보보호 수준, APB의 발전방향 등에 대해 함께 토의하였다. 김범수 소장은 "빠른 ICT 기술변화 속에서 여전히 개인정보보호와 데이터 이전 관련 법이 제정되지 않은 국가들이 존재하며, 이에 대한 관심이 적은 실정이다. 법이나 제도 등의 개선 외에도 개인이 개인정보보호에 대해 쉽게 인식할 수 있는 방법은 무엇일지 고민하였고, 그 해법을 제안하는 취지에서 'Asia Privacy Bridge Forum' 행사를 개최하고 있다."라고 전했다. 연세대학교 정보대학원 그리고 바른ICT연구소는 학계, 정부, 기업 전문가들이 주로 참여하고 있으나 앞으로는 개인 및 시민단체 등과 함께 다양한 의견을 수용하며 그 범위를 더욱 넓혀 나갈 예정이다.

Track 4의 블록체인 세션에서는 이창진 한국거래소 팀장, 이종엽 한국인터넷진흥원 책임연구원, 이상기 코스콤 부서장, 그리고 박세열 IBM 실장이 블록체인 국내외 시장 동향 및 지원전략에 대해 발표하였다. 블록체인은 금융서비스 부문을 넘어 앞으로는 제조 및 유통, 공공서비스, 사회문화 부문 등 전 영역에 걸쳐 우리 생활에 파급영향을 줄 것으로 기대하며 이미 선진국에서는 대선후보 선정 온라인 투표에 활용하는 등 정부 및 민간에서 다양한 구축사례를 확대하고 있다. 활용범위를 넓히기 위해서는 기술 정교화 이외에 사회적 장치, 법과 규제 문제를 해결해야 하며, 정부와 민간이 함께 방안을 마련해 나가야 할 것이다. 🌐

정리 신아련 (연세대학교 바른ICT연구소 연구원)

## 2017 International Conference of Data Protection and Privacy Commissioners (ICDPPC)

### 바른ICT연구소, 국제개인정보보호 감독기관회의(ICDPPC) 참가



연세대학교 바른ICT연구소는 지난 9월 25일부터 29일까지 홍콩에서 개최된 제39회 국제개인정보보호 감독기관회의(ICDPPC, International Conference Data Protection and Privacy Commissioners)에 참석했다. 이번 행사 참여는 ICDPPC에서 개인정보보호 및 프라이버시 전문기관 자격으로 바른ICT를 초청하면서 이뤄지게 되었다.

바른ICT연구소는 9월 25일(월) Kowloon Shangri-La 호텔에서 열림 'Application of Privacy Bridge Project to Asia - in a Manner that Respects the Substantive and Procedural Differences among the Asian Jurisdictions' 세션에 참가하여 한국에서 Asia Privacy Bridge Forum(이하 APB Forum)을 개최하게 된 배경 및 지난 APB 포럼을 통해 축적된 정보를 공유하고, 향후 아시아 개인정보보호를 위한 발전 방향을 논의하였다.



국제개인정보보호감독기관회의(ICDPPC, International Conference Data Protection and Privacy Commissioners)는 개인정보보호 및 프라이버시를 증진하고 회원 기관 간의 대화와 협력, 정보 공유를 위한 포럼을 개최해 개인정보 보호 및 프라이버시 공동 결의와 선언을 채택하기 위해 1979년에 설립된 기관이다. 2001년부터 전 세계를 대상으로 하는 국제회의로 전환되었으며, 매년 집행위원회 회의와 정기회의를 각 1회씩 개최하여 해당 결의안의 채택 여부를 결정하는 등 국제적으로 개인정보보호 논의를 주도하는 협의체로서 중요한 역할을 하고 있다(개인정보보호 연차보고서, 2017). 

정리 손수민 (연세대학교 바른ICT연구소 연구원)

## 언론보도로 소비자 인식을 변화시킬 수 있을까?

박용완, 손수민 (연세대학교 바른ICT연구소 연구교수, 연구원)



### 무제한 요금제의 등장

과거 음성 통화 중심에서 데이터 중심의 소비패턴 변화로 인해 소비자의 데이터 사용량이 급격히 늘어났다. 이에 통신사는 소비자에게 더 나은 데이터 사용 환경을 제공하기 위해 과거와 같은 가격에 더 많은 혜택을 제공하는 '무제한 요금제' 서비스를 제공하고 있다. 과거에 받았던 혜택에 비해 요금이 저렴해졌을지라도 절대적인 가격대는 증가하였고, 결국 가계통신비에 부담을 느끼는 소비자들 및 시민단체들의 통신비 인하 요구는 정부와 이동통신 사업자들에게 하나의 커다란 사회적 압력으로 작용하였다.


올바른 정책 도입 및 실행을 위해서는 소비자들이 이동통신비에 대해 어떻게 인식하고 있는지에 대한 연구가 필요하다. 현재 이동통신비에 대한 이슈는 서비스 제공자인 통신사와 소비자 간의 견해가 서로 평행선을 달리고 있다. 이러한 간극을 줄이기 위해서는 소비자가 가지고 있는 이동통신비에 대한 인식을 이해할 필요가 있다.

### 이동통신비 언론보도 메시지에 대한 소비자의 정보처리과정

현재 이동통신비에 대한 언론보도는 크게 2가지 성향을 보이고 있다. 이동통신비가 비싸다는 논조의 언론보도와 저렴하다는 논조의 언론보도가 혼재되어 있는 양상이다. 비싸다 혹은 저렴하다는 주장의 근거는 다양하게 제시되고 있는 상황이지만, 관심의 초점은 이동통신비 인하라는 사회적 압력에 정부와 기업이 어떻게 대응하는가에 집중되어 있다.

소비자들은 자신들의 생각과 일치하는 정보는 수용하고, 불일치하는 정보는 거부하거나 예외적인 경우로 치부해버리는 경향이 있다. 또한 소비자들은 자신이 선호하는 판단 및 결론과 일치하는 정보는 그렇지 않은 정보에 비해 더 정확하고 타당하다고 판단한다. 이동통신비가 저렴하다는 언론보도는 생산자를 옹호해주는 기사이지만, 비싸다는 언론보도는 소비자들을 옹호해주는 기사로 인식할 수 있다. 결과적으로 소비자들은 이동통신비가 저렴하다는 언론보도를 접하더라도 믿지 않을 것이며, 이동통신비가 비싸다는 언론보도에는 더 많은 신뢰를 보낼 것으로 기대된다. 그리고 이동통신비가 비싸다는 자신들의 신념을 고수할 것이라 예상된다.

이를 검증하기 위한 실험을 진행하였다. 분석 결과, 이동통신비에 관한 언론보도에 대한 소비자의 신뢰성 및 중립성 평가는 각자가 가지고 있는 이동통신비에 대한 생각과의 일치 정도에 따라 결정됨을 알 수 있었다. 즉, 소비자들이 이동통신비가 저렴하다는 기사보다는 이동통신비가 비싸다는 기사를 더 신뢰하고 더 중립적으로 판단하였다. 또한, 언론보도의 내용 및 노출 여부와 관계없이 소비자들은 이동통신비가 비싸다는 인식을 강하게 유지하는 것으로 나타났다. 결국 소비자들이 가지고 있는 인식이 새로운 정보를 접하더라도 기존의 생각이 **고정관념**을 형성하여 새로운 정보를 받아들이는데 방해물로 작용하는 현상을 확인할 수 있었다.

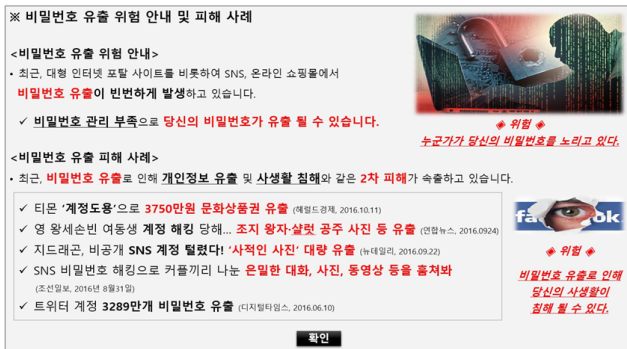
소비자들을 비롯한 시민단체들의 통신비 인하 요구는 정부 및 기업에게 해결해야 할 사회적 이슈임이 분명하며, 이동통신비와 소비자의 인식 간에는 차이가 존재하고 있다. 따라서 지속적인 연구를 통해 그 간극을 줄여나가는 노력이 필요할 것이다. 본 연구는 디지털융복합연구 9월호에 게재되었다. 

# 공포감 조성으로 비밀번호 변경을 유도한다

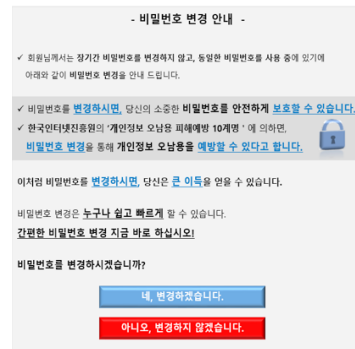
박재영 (연세대학교 정보대학원 박사과정)

최근 비밀번호가 유출되는 사고가 급증하고 있다. 2013년 야후Yahoo, 2015년 뽀뿌 사이트와 같이 해킹으로 인한 대규모 비밀번호 유출 사건이 발생했는가 하면, 개인의 비밀번호 관리 미숙으로 SNS 계정이 도용되는 사례도 속출하고 있다. 이에 기업에서는 사용자에게 비밀번호를 주기적으로 변경하라고 안내하고 있다. 하지만, 한국인터넷진흥원에서 실시한 설문에 의하면, 응답자 중 33.2%가 비밀번호를 변경하지 않는다고 하였다. 이와 같은 사실은 사용자들의 비밀번호 관리 의식이 상당히 미흡한 수준인 것을 나타낸다.

이에 본 연구에서는 비밀번호 변경행위를 증대시키기 위한 방안으로 **공포 소구**와 **메시지 프레이밍 효과**를 살펴보았다. 즉, 비밀번호 유출에 대한 메시지가 담긴 공포 소구가 개인들의 비밀번호 변경행위에 어떠한 영향을 미치는지 알아본 것이다. 이 때, 공포 소구Fear Appeal는 특정 위협의 취약성과 심각성이 담긴 메시지를 통해 수용자들이 바람직한 행동을 하게끔 유도하는 설득적 메시지를 말한다. 또한, 비밀번호 변경을 권고하는 메시지를 서로 다르게 표현할 때, 즉, 비밀번호 변경에 대한 이득을 강조할 경우와 비밀번호를 변경하지 않았을 시에 발생하는 손실에 초점을 맞출 경우에 개인들의 선택과 판단이 달라지는지 확인하였다.



[그림 1] 공포 소구 처치물



[그림 2] 메시지 프레이밍 처치물(이득)

연구결과, 공포 소구를 보여준 집단의 비밀번호 변경의도가 더 높은 것으로 나타났다. 이는 비밀번호 변경행위에 있어서 공포 소구가 효과적으로 작용했다는 것을 의미한다. 한편, 손실 프레이밍이 제시된 집단의 비밀번호 변경의도가 더 높을 것으로 가정했으나, 이에 대한 유의한 결과를 얻지 못하였다. 추가적으로 공포 소구가 제시된 집단을 대상으로 구조방정식 모델 분석을 실시한 결과, 지각된 심각성이 두려움에 영향을 주는 것으로 나타났다. 즉, 비밀번호 유출에 대한 피해를 심각하다고 느낄수록 비밀번호 유출을 두려워 한다는 것이다. 그리고 이렇게 형성된 두려움은 비밀번호 변경의도에 긍정적인 영향을 미치는 것으로 나타났다. 또한, 두려움과 변경의도 간에 메시지 프레이밍이 조절역할을 하는 것으로 나타났다. 즉, 공포 소구가 제시된 상황에서는 이득 프레이밍( $\beta: .498$ )이 손실 프레이밍( $\beta: .118$ )보다 더 효과적임을 의미하는 것이다.

본 연구결과는 기업에서 공포 소구를 적극적으로 활용해야 한다는 것을 시사한다. 현재 웹사이트에서 제공하는 ‘비밀번호 변경 안내문’을 보면, 단순히 비밀번호 보호 차원에서 비밀번호를 변경하라는 내용이 대다수를 차지하고 있다. 이런 방식은 사람들의 행동을 바꾸기가 힘들다. 따라서 기업들은 공포 소구를 바탕으로 비밀번호 변경행위를 이끌어낼 필요성이 있다.

## 클라우드 펀딩 성공 여부를 좌우하는 온라인 지인

김용석

홍공과학기술대학교 교수

클라우드 펀딩은 군중을 뜻하는 ‘클라우드crowd’와 재원 마련을 의미하는 ‘펀딩funding’이 합쳐진 단어로, 창의적인 아이디어를 가지고 있는 기업가들이 온라인을 통해서 다수의 소액투자자로부터 사업자금을 조달하는 것을 말한다.

특히 클라우드 펀딩은 소셜네트워크의 온라인 네트워크를 기반으로 이루어지는 경우가 대부분이다. 펀딩 모금자의 소셜네트워크 지인들은 다른 후원자backer들에 비해 펀딩 결정을 빨리 내리기 때문에, 지인들의 프로젝트 참여도를 높임으로써 프로젝트를 눈에 띄게 하고, 잠재적 후원자를 끌어들이며 모멘텀momentum을 일으킬 수 있다. 소셜네트워크 지인들의 펀딩 참여 여부는 프로젝트의 성패에 큰 영향을 미치고 있다.

그렇다면 소셜네트워크 지인들의 클라우드 펀딩 참여율을 높이기 위한 방법은 무엇일까? 펀딩에 참여하는 지인들의 의사결정 매커니즘은 무엇일까?


소셜네트워크의 지인이 클라우드 펀딩에 참여하게 하는 관계적 요인으로 유대 강도tie strength와 배태성embeddedness이 있다. 유대 강도란 프로젝트 개설자와 온라인 지인이 클라우드 펀딩 프로젝트 시작 전에 얼마나 교류했는가를 의미한다. 배태성이란 프로젝트 개설자와 온라인 지인 사이에 공유하고 있는 지인의 규모를 말한다.

또한 펀딩 결정에 부정적인 영향을 미치는 요인으로 프로젝트의 불확실성이 있다. 이 불확실성은 두 가지 측면에서 살펴볼 수 있는데, 첫 번째는 프로젝트 자체에 대한 불확실성이다. 프로젝트의 제품과 개설자에 대한 정보가 충분하지 않을 경우 사람들은 펀딩을 하지 않을 것이다. 또한

프로젝트의 성공여부가 불확실할 경우 펀딩을 하지 않으려 할 것이다.

온라인 네트워크를 활용하여 프로젝트의 불확실성을 줄이는 방법으로 정보전달information transfer과 상호교류에 의한 책임감obligation이 유효한 영향력을 가질 것이라 보았다.

연구 결과, 프로젝트 개설자와 후원자의 유대 강도가 높을수록, 공유하는 지인이 많을수록 펀딩 결정에 긍정적인 영향을 주는 것으로 나타났다. 하지만 두 가지 변수에는 각기 다른 매커니즘이 작용하였다. 조절변수로서 유대 강도가 클수록 제품정보의 부정적 불확실성을 완화하는 기능이, 공유하는 지인의 규모가 클수록 펀딩 성공여부의 부정적 불확실성을 완화하는 기능이 있는 것으로 나타났다.

프로젝트의 개설자와 제품에 대한 불확실성이 높을 때에는 소셜네트워크를 통해 제품에 대한 정보나 개설자에 대한 정보를 알 기회가 증가한다. 펀딩 성공 여부의 부정적 불확실성이 높을 때에는 온라인 상의 지인으로서 프로젝트 성공을 위해 도와줘야 된다는 의무감이 높게 작용한다. 이를 통해 온라인 지인 사이에서 나의 명성reputation을 높일 수 있고 향후 내가 도움이 필요로 할 때 공유하는 지인 중 누군가가 자신을 도와줄 것이라는 기대감을 갖고 펀딩 결정을 내리는 것이다. 



# 모바일 코즈마케팅, 전략도 달라져야 한다

이동원

홍콩과학기술대학교 교수

'000와 함께하는 착한 원 캠페인'  
'제품이 팔릴 때마다 원씩 적립되어 000에 후원됩니다.'

제품을 구입할 때 이러한 문구를 한번은 본적이 있을 것이다. 기업의 비즈니스 활동에 '명분Cause'을 제공하는 이러한 '코즈마케팅Cause Marketing'이 모바일로 확장되고 있다.

## 기업의 CSR활동과 코즈마케팅

기업의 사회적 책임CSR 활동과 코즈마케팅의 차이점은 사회적 책임의 경우 기업이 사회의 구성원으로서 수행하는 역할에 초점이 맞추어져 있는 반면, 코즈마케팅은 소비자를 통해 기업이 추구하는 경제적 가치와 사회가 추구하는 공익적 가치를 동시에 추구하는데 초점을 둔다. 즉 코즈마케팅은 기업의 비즈니스 활동에 정당성을 부여하여 공익적인 가치 창출 활동과 연계시키는 것이라 볼 수 있다.

## 모바일 코즈마케팅의 잠재력

최근 모바일에서의 금융거래가 증가하고 있으며, 중국의 경우 전체 e커머스에서 발생하는 금융거래 중 70%가 모바일에서 발생한다고 한다. 이전 연구에 따르면 기부활동은 소비채널을 공유하는 경우가 많다. 즉 모바일에서의 금융거래가 증가함에 따라 기부 채널로서도 잠재력을 갖게 된 것이다. 모바일이라는 채널을 이용할 경우 기업은 자신의 모바일 사용자 기반user base을 활용할 수 있고, 기부단체의 경우도 기존의 모바일 기업 플랫폼을 활용하여 큰 노력 없이 모바일에서의 입지를 확보할 수 있게 될 것이다.

## 모바일 코즈마케팅 전략

코즈마케팅은 기업이 금전적인 보조를 하는 방식 monetary subsidy이 가장 효과적인 것으로 알려져 있으며 구체적으로는 매칭과 리베이트 방식으로 나뉜다. 오프라

인 기부에서는 사람들이 자신이 기부한 것에 대해 보상을 받는 리베이트 방식 보다는 자신이 기부한 금액에 기업이 일정 금액을 더해 협력하여 기부하는 방식인 매칭 방식을 더 선호하는 것으로 알려져 있다. 그렇다면 다른 사람의 시선 없이 좀더 개인적인 모바일 환경에서 사람들은 어떤 기부 방식을 더 선호할까?

모바일 잠금 화면에 광고나 뉴스를 나타나게 허용하고 이를 슬라이드로 해제할 때마다 일정 금액을 지급하는 모바일 앱 사용자들을 대상으로 하여 매칭과 리베이트 방식 중 어떤 방식을 선호하는지, 지금 당장 보상을 받는 것과 나중에 받는 것 중 어떤 것을 선호하는 지에 대한 연구를 수행하였다.

연구 결과, 모바일 기부자의 경우 매칭 방식보다는 기부 금액에 대한 일정한 보상을 받는 리베이트 방식을 선호하는 것으로 나타났다. 또한 그 보상을 나중에 받는 것보다는 지금 당장 받는 것을 선호하였다. 모바일 푸시 알림을 사용할 경우 그 효과가 매우 큰 것으로 나타났다.

따라서 기업 또는 기부단체가 코즈마케팅을 할 경우, 사용자들에게 기부 금액에 대한 일정한 보상을 즉각적으로 제공하고 푸시 알림을 적극적으로 활용하여야 많은 기부를 유도할 수 있을 것이다. 📱



정리 손수민 (연세대학교 바른ICT연구소 연구원)

## 인구통계 데이터를 활용한 PC/Mobile 플랫폼 이용행태 분석

임지선 박근용  
연세대학교 바른ICT연구소

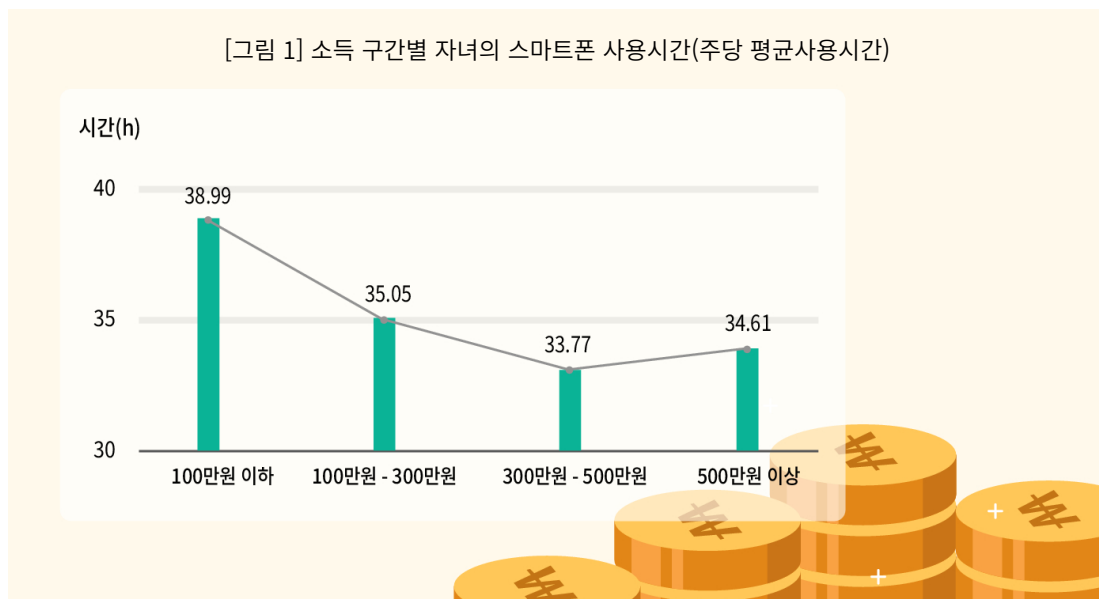
본 기획 연재에서는 연세대학교 바른ICT연구소가 외부 조사기관에 의뢰하여 2016.06.27 ~ 2016.10.02까지 총 14주간 전국의 만 7세 이상 6,090명을 대상으로 수집한 스마트폰 사용량 데이터를 자체 분석한 결과를 소개합니다.

### 고소득 가정 아이들은 스마트폰을 적게 사용할까?

- 소득 수준이 높아질수록 자녀들의 스마트폰 사용시간 감소
- 단, 고소득 가정 자녀의 스마트폰 사용시간이 가장 낮은 것은 아니야
- 맞벌이 자녀보다 외벌이 자녀의 스마트폰 사용시간이 더 길어

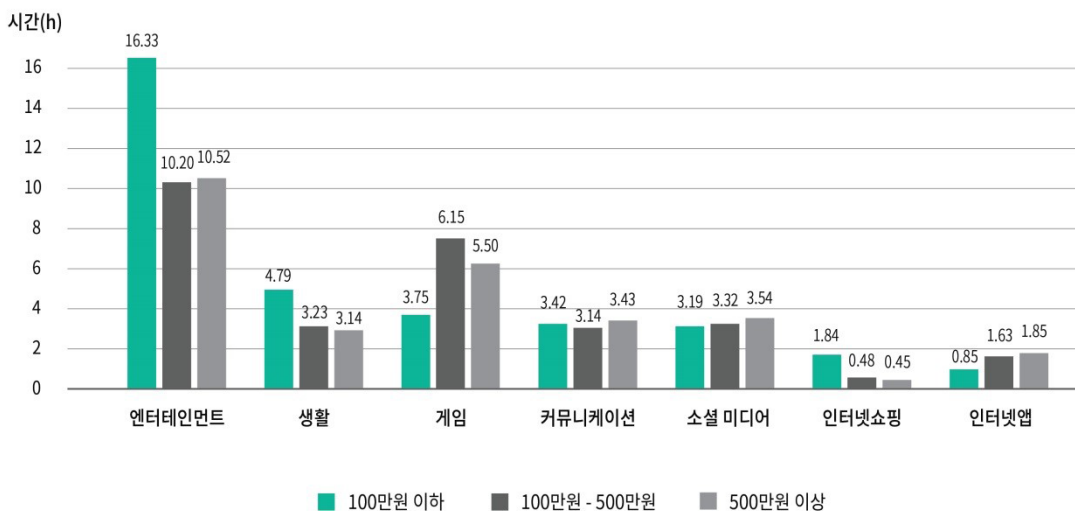
부모의 소득 및 취업여부와 아이들의 스마트폰 사용시간에는 어떤 관계가 있을까? 연세대학교 바른ICT연구소에서 2016.06.27 ~ 2016.10.02 14주 간 전국의 만 7세이상 만 18세 이하 429명 아이들을 대상으로 가계의 소득수준에 따른 스마트폰 사용량을 조사한 결과, **소득수준이 높아질수록 자녀들의 스마트폰 사용시간이 감소하는 것으로 나타났다.** 구체적으로 부모 소득수준 100만원 이하 저소득 가정 자녀의 주간 평균 스마트폰 사용시간은 38.99시간으로 가장 높게 나타났으며, 소득수준 100만원-300만원 자녀의 경우 35.05시간, 소득수준 300만원-500만원 자녀의 경우 33.77시간으로 소득수준이 높아질수록 스마트폰 사용량이 감소하는 추세가 나타났다. 그러나 소득수준 500만원 이상 고소득 가정 자녀의 스마트폰 사용량은 34.61시간으로 소득수준 300만원-500만원 자녀보다 스마트폰을 주간 평균 1.04시간 더 많이 사용하는 것으로 나타났다.

[그림 1] 소득 구간별 자녀의 스마트폰 사용시간(주당 평균사용시간)



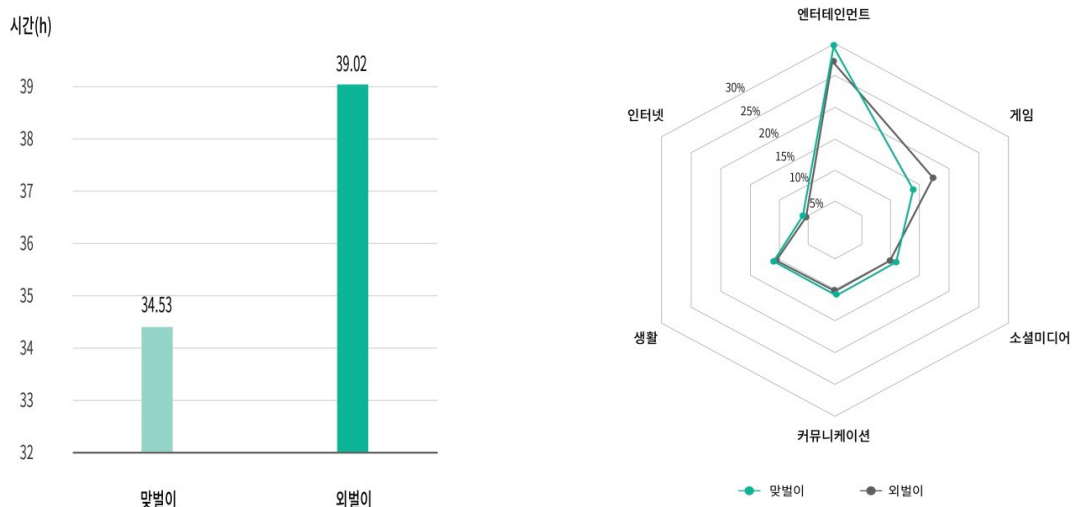


소득구간별 자녀들의 모바일 앱 카테고리별 사용시간 비중을 살펴본 결과, 소득수준과 관계없이 엔터테인먼트 앱 사용비중이 가장 높게 나타났으며, 이어 게임, 소셜 미디어 앱 사용비중이 높게 나타났다. 일반적으로 소득수준 100만원 이하를 저소득, 100만원-500만원을 중간 소득, 500만원 이상을 고소득 구간으로 구분하였을 때, **소득수준 100만원 이하 저소득층 아이들의 경우 엔터테인먼트**(저소득층: 16.6시간 > 고소득층: 10.5시간 > 중산층: 10.2시간), **생활**(저소득층: 4.8시간 > 중산층: 3.2시간 > 고소득층: 3.1시간), **인터넷 쇼핑**(저소득층: 1.8시간 > 중산층: 0.5시간 > 고소득층: 0.5시간) 앱 사용시간이 다른 소득층 아이들에 비해 상대적으로 길다. 반면, 소득수준 **100만원이상 500만원이하 중산층 아이들의 경우 게임**(중산층: 6.2시간 >고소득층: 5.5시간 > 저소득층: 3.8시간) 앱 사용시간이 다른 소득층 아이들에 비해 많았고, **소득수준 500만원이상 고소득층 아이들의 경우 소셜 미디어**(고소득층: 3.5시간 > 중산층: 3.3시간 > 저소득층: 3.2시간)**와 인터넷 앱**(고소득층: 1.9시간 > 중산층:1.6시간 > 저소득층: 0.9시간) 사용시간이 상대적으로 많게 나타났다. 즉, 소셜 미디어와 인터넷 앱의 경우 소득수준이 높아질수록 사용시간이 증가하는 것으로 나타난 반면, 생활 및 인터넷 쇼핑 관련 앱의 경우 소득수준이 높아질수록 사용시간이 감소하는 것으로 나타났다.



[그림 2] 소득구간별 모바일 앱 카테고리별 사용시간(주당 평균사용시간)

한편, 맞벌이 가정의 자녀는 외벌이 가정의 자녀보다 스마트폰을 적게 사용하는 것으로 나타났다(맞벌이 자녀: 31.9시간, 외벌이 자녀: 36.8시간). 하지만, 이와 같은 차이가 맞벌이 부부와 외벌이 부부의 소득수준을 통제한 상태에서도 유의하게 나타나, 맞벌이 부부의 자녀가 외벌이 부부의 자녀보다 스마트폰을 적게 사용하는 것이 단순히 맞벌이 부부가 외벌이 부부보다 소득수준이 높기 때문은 아닌 것으로 보인다. 다만, 맞벌이 부부의 자녀는 상대적으로 외벌이 부부의 자녀보다 게임 앱 사용비중(맞벌이: 17.1%, 외벌이: 13.7%)이 두드러지게 높게 나타났다.



[그림 3] 맞벌이/외벌이 가정의 자녀의 스마트폰 주간 평균사용시간 및 사용비중(%)

부모의 소득수준 및 취업 유무에 따른 자녀의 스마트폰 사용시간 및 사용패턴을 비교한 결과, 첫째, 부모의 소득수준이 높아질수록 자녀의 스마트폰 사용시간은 감소하는 것으로 나타났다. 하지만, 소득수준이 가장 높은 그룹 자녀의 스마트폰 사용량이 가장 적은 것은 아니었는데, 이러한 고소득 가정의 아이들은 다른 그룹의 아이들보다 소셜 미디어 및 인터넷 사용비중이 높았다. 둘째, 저소득층 아이들의 경우 스마트폰 사용시간이 상대적으로 가장 긴 것으로 나타났다. 그럼에도 불구하고 게임을 가장 많이 사용하는 그룹은 저소득층 아이들이 아니라 오히려 중산층 아이들이었다. 따라서, 게임중독 위험군은 오히려 저소득층이 아닌 중산층 아이들일 가능성이 높게 나타났다. 셋째, 맞벌이 가정의 아이들이 외벌이 가정의 아이들보다 스마트폰 사용시간이 더 높을 것이라는 예상과 달리, 실제 스마트폰 사용시간은 외벌이 가정의 아이들이 맞벌이 가정의 아이들보다 더 높게 나타났다. 다만, 맞벌이 가정의 아이들은 상대적으로 외벌이 가정의 아이들보다 게임 앱 사용비중이 높았다. 따라서 맞벌이 부부 아이들에게는 스마트폰 사용자체보다는 게임사용에 대한 주의가, 외벌이 부부 아이들에게는 게임보다는 스마트폰 사용시간에 대한 주의가 보다 강조될 필요성이 있음을 시사한다. 🎮

# Barun ICT Essay Contest

---

2017년 6월 22일 연세대학교 청솔관에서 제2회 'Barun ICT Essay Contest'가 개최되었다. 본 기획연재에서는 Best Essay로 선정된 5편의 에세이를 매달 한편씩 소개한다. 에세이는 영문으로 쓰여진 원문을 수록하였다.

## #2. Fundamental Right Persists in Cyber World

**Written By** Hyungyung Park

(English Language and Literature & Chemistry, Yonsei University)

As far as I can remember, I always knew that people's privacy is something to be respected. Privacy is a concept that I've recognized without a doubt. However, if I were asked to define the word, I would find myself speechless. It wasn't only myself that struggled with the definite meaning of the word. Throughout Modern history, there have been numerous attempts to define privacy in both philosophical and substantial context, albeit without definite success. In his paper, Michael Friedewald suggests **seven types of privacy** that includes practical sense of privacy fairly well, which are Privacy '*of the person, of behavior and action, of communication, of data and image, of location and space and of association.*' (Friedewald)

With the advance of internet technology and media, present-day privacy cannot be discussed outside of internet world. At first glance, of Friedewald's seven types of privacy, it seems as if the privacy of data and image and privacy of communication are the ones that are at risk the most. However, with progress of both the technology and the integration of technology into people's everyday life, it is all the seven types that are threatened to be violated. In these circumstances, it would do well to remind ourselves that privacy is something we rightfully deserve. Cambridge dictionary defines the word '*intrinsic*' as 'being an extremely important and basic characteristic of a person or thing.' By this definition, if something critically belongs with a person's basic properties, and therefore does not change by external circumstances, it could be said that it is intrinsic. Also, one of the main principal of laws, be it international laws or from a specific country, is to defend intrinsic human right. Therefore, laws protecting a virtue can be an evidence that it is a basic right. **Privacy is an intrinsic right because it belongs to each individual, because it is granted the protection of law and because it should not change by circumstances.**

Privacy is an intrinsic right, because personal data primarily belongs to the individual, and what belongs to the person by definition is intrinsic. A large share of what consists privacy, especially online, is creation of someone. Pictures of beautiful scenery and of artworks on Instagram, cheerful friends gathering pictures with comments uploaded on Facebook, varying topics of articles on internet blogs and news sites, writings ranging from a few lines of personal rants on twitter to novels of thousands of words, they're all each a work of someone. They created it, so it's theirs by virtue. If it's theirs, it's an intrinsic right.

For the other part, the rest of personal data existing online that is not made by someone is critically linked to the identity of the owner. A person's name, age, address, face, lists of friends- these set of facts distinguish their identity all together. The data is intrinsically reserved because it's unique to individual. For instance, while it is the owner's prerogative to allow viewing of the data for other people or companies, it is impossible for them to hand over the right itself. On Facebook, people who come across one's page can see one's name, picture, birthday, birthplace, even the name of their significant other or alma mater, depending on what the owner of the page chooses to display. Still, no one other than the owner themselves can incorporate the data into their identity. If someone takes a name, profile picture or artwork of someone else and post them online without acknowledgement, it's considered either fraud or copyright infringement. This is because the information is inherent in the owner's proprietary.

---

The fact that a person has a final say in the handling of their privacy shows the assumed concurrence that privacy belongs to an individual. Ultimately, it is the individual that decide when, how, and to whom the privacy is shared. The occasions where our online privacy is compromised most outright would be when agreeing to terms and policies on websites. In these events, privacy is not a shared property that the company and the individual make negotiation on, one with a midpoint both party have to concede even if unsatisfied. The choice simply not to click the 'agree' button is always there for the person whom the information belongs to. The company might try and write down clauses in a way beneficial to them, but at the end it is solely the individual's decision that closes the matter, and that is because it is in their possession. This clearly shows that privacy is an intrinsic right that belongs to each individual.

In addition to ownership, what law protects is what people deserve without having to earn, which includes privacy. There are more than a few provisions of legal system established to guard people's privacy on the internet. Act on Promotion of Information and Communications Network obligates information network service providers to acquire consent from the user on the use of their personal information. The act also provides extensive form of user information protection and recognizes libel in cyberspace. Electronic Transaction Act protects the benefits of online consumers and secures the credibility of the market. For preexisting privacy laws, additions and adjustments are also made to accommodate the online aspect of their subjects. For example, copyright law now includes clauses concerning cyber right on intellectual property. These laws are the evidence showing that privacy is treated as intrinsic right, provided to every person under the protection of law.

Constitution of the Republic of Korea maintains that the purpose behind the law's existence is "[the country's] responsibility to affirm and secure individual's fundamental human rights that are inviolable." (Constitution) Were it completely left at hands of people involved, without the interrogation of law, as if it were social commodity that can be shifted in market, personal information would be exploited a lot more blatantly. People would be divested of significant freedom in privacy, in exchange of the services provided by profitable companies, and possibly the government itself in the name of national security. The presence of online privacy laws shows that government recognizes privacy as a constitutional human right to be protected.

**Moreover, privacy is universal, in that it is the same regardless of race, gender or religion, which is just like other intrinsic rights.** World-wide organizations dealing with human welfare such as WHO or International Amnesty found their base on the premise that there exists fundamental human right that transcends national borders. Constitution of WHO proclaims that health is '*one of the fundamental rights of every human being without distinction of race, religion, political belief, economic or social condition.*' asserting their cause as protecting a fundamental human right. Then, what makes something a '*fundamental rights of every human being?*' To answer the question, Amnesty International directly refers to Universal Declaration of Human Rights. The Declaration was documented by legal professionals from all around the world and proclaimed by United Nation. According to the Declaration, fundamental human right is '*right to life, liberty and security of person.*' Security of privacy, especially of behavior, action and communication, is crucial to a person's liberty and security, for if a person's thoughts and words were monitored it would be violation on their freedom of speech.



---


That one of the articles of the Declaration mentions privacy as one of universal right; “No one shall be subjected to arbitrary interference with his privacy (...) or correspondence, nor to attack upon his honor and reputation.”, reaffirms the fact that privacy is an intrinsic right. (Article 12) While the legal terms and standards on privacy in law may vary by each country or group, the fact that a person is always entitled to certain principal law does not change, and that is because even if someone’s privacy is undermined by the society they belong in, they are still “entitled to an (...) international order in which the rights and freedoms (...) can be fully realized,” (Declaration) and thus privacy is an intrinsic right.

Some may argue that privacy is inevitably a shared product of society, because once it enters the digital world it’s there for everyone to take. While it is true that private data online is currently in a vulnerable state, it does not mean that things shall stay this way. The law division is actively responding to the increasing new forms of violation of privacy online. A case in point is the Geolocation Data Protection Act. The law was enacted in response to the appearance of Location Based Services, in the form of Social Networks, smartphone map service and online games. The service integrates GPS information of the user into social media platform such as Instagram, or navigation services such as Googlemap, and has gained quick popularity over past few years. While variable and convenient, this service posed serious breach of privacy in a way unprecedented, and the Act was proposed to provide geolocation data security in online network applications. As such, constant recognition of people’s innate right to privacy is relentlessly made, even under changing environment.

Other people could also be argued that privacy is a social construct because it may be negotiated for economic well-being or national security. A famous incident few years ago, however, told us a different story. On June 2013, Edward Snowden, a former CIA agent and NSA contractor, revealed that numerous surveillance programs were employed by National Security Agency of USA. The nation-wide scandal following the revelation showed the public’s stance on their privacy. Even though it was clear that the surveillance undertook solely in the name of country’s safety, people felt deeply wronged. The public was outraged because the government violated people’s right to ‘choose’ to share information. This is a clear case of counterevidence implying the unquestioned consensus was there that each person is entitled to the ownership of their personal data, that which shall not be compromised even for the national security.

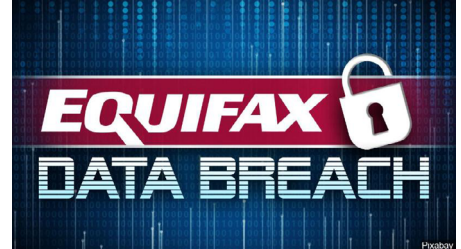
Even though there are arguments taking the perspective of privacy as social construct, I firmly believe that privacy is one of intrinsic human rights. This is because private data originally belongs to individuals, because privacy is protected by the law as the government acknowledges it as fundamental human right, and because a person’s right to privacy does not change by their affiliations such as nationality or religion.

Prior to the emergence of the wireless network, it was much easier to keep track of basic, personal details. Nowadays with fast advance of technology, the realm of internet is constantly expanding, and privacy is so conveniently invaded. People reluctantly hand over their personal data for online services that has become so quintessential of contemporary day life. As opposed to signing contract in paper or listening to terms and agreeing, clicking away “yes” to an annoying popup window is made to seem so simple and inconsequential.

Both the legal system and people’s awareness aren’t properly catching up to the velocity of technology, and this situation is shamelessly taken advantage of. The Largely argued idea of privacy as social construct is not hard to comprehend, as online-based companies are indeed treating people’s information as if it’s some negotiable goods. All the more for these circumstances, awareness should be raised. Social consensus about the importance of privacy as fundamental human right needs to be formed, and more concerned efforts should be put into protecting the vulnerable data online. 

# 에퀴팩스 개인정보 유출: 어떻게 미국인 절반의 정보가 해킹당했나?

송민선 (연세대학교 바른ICT연구소)



미국 최대 신용조사 기관인 에퀴팩스Equifax는 9월 7일 자사 고객의 개인정보가 유출되었다고 발표하였다. 해킹은 5-7월 사이에 이루어졌으며, 약 1억4,300만 명의 이름, 사회보장번호SSN, 주소 및 생년월일 등이 사이버 범죄자들에게 노출되었다. 이는 미국 인구의 44%에 해당되는 큰 규모이다. 뿐만 아니라, 이 중 20만 9,000명은 신용카드 번호까지 유출되었으며, 서비스를 이용하던 일부 캐나다와 영국 국적의 고객까지 피해를 입은 것으로 나타났다.


에퀴팩스의 데이터 유출 사건은 역대 피해 규모가 가장 큰 사건이지만, 더욱 우려스러운 점은 미국의 사이버 범죄에 대한 취약점이 드러난 사건이 이번이 처음이 아니라는 것이다. 2015년 건강보험 업체인 앤섬Anthem에서 8,000만명의 고객 건강 데이터가 해킹되는 사건이 있었고, 지난 7월에는 미 캔자스 통상부에서 500만 명의 사회보장번호가 노출되는 사건이 발생하였다. 지난 1월의 미국 리서치 기관 퓨PEW가 미국인 1,024명을 대상으로 한 조사에서, 절반 이상의 응답자들은 연방정부 및 대기업의 개인정보보호 정책을 신뢰하지 않으며, 개인정보 유출 경험이 있다고 응답하였다.

이번 데이터 유출 사건에 대해 전문가들은 기업의 보안의식과 더불어 기존의 개인 신원확인 시스템의 문제점을 지적한다. 특히 사회보장번호의 경우, 건강 및 금융기업 분야에서 정보 조회를 위한 보편적인 수단으로 사용되고 있으나, 신용카드나 온라인 상의 아이디와 달리 변경이 아주 어려우며, 다른 민감한 정보와 연결되어 있어 유출될 경우 매우 타격이 크다.

이에 대해 전자개인정보센터Electronic Privacy Information

Center의 회장 마크 로텐버그Marc Rotenberg는 의회에서 청문회를 열어 사회보장번호를 원래의 목적과 다른 용도로 수집하는 행위를 금지해야 개인정보를 효과적으로 보호할 수 있다고 주장하였다. 보안 전문가들은 기업에서 고객의 정보를 수집할 때 다양한 비밀번호나 코드를 통해 신원을 확인하는 시스템을 수립해야 한다고 권고한다. 제도적인 측면에서는 가장 민감한 정보를 보유하고 있는 금융 및 건강 산업에서 사용하는 식별자를 이분화해야 어느 한 곳에서 해킹을 당하더라도 이와 연계된 다른 정보의 유출을 막을 수 있다. 에퀴팩스 사태 이후, 미국 메디케어 Medicare 서비스에서는 베네팅 카드에서 사회보장번호를 삭제하는 방침을 검토하는 중이다.

에퀴팩스에서는 이번 유출 사태의 원인은 관련 애플리케이션의 버그로 인한 것이라고 애매하게 발표하였다. 또한 이번 사태의 신속한 원인분석 파악 실패 외에 유출 발표 전에 일부 임원들이 회사 지분을 매각했다는 정황이 드러나 기업의 윤리성에 대한 의문 또한 제기되고 있다. 해킹된 고객들에게 손해배상 청구 포기를 전제한 무료 모니터링 서비스를 제안하는 등 후속 조치보다는 기업의 이윤에 더욱 집착하는 정책을 보여서 고객의 불만이 고조되고 있다.

퓨 리서치에 따르면 미국인 64% 이상은 건강과 금융에 관한 민감한 정보가 포함된 온라인 계정을 가지고 있다. 개인정보는 더욱 디지털화 되고 사이버 보안에 대한 중요성은 더욱 커지고 있다. 기업에서는 해킹에 대한 예방을 철저히 하여야 하며, 해킹이 되었다고 하더라도 책임감을 가지고서 투명하고 신속하게 조치하고, 필요한 경우에는 정부와도 연계하여 피해를 최소화해야 한다. 

## 보안을 위해 사생활을 희생하는 것이 가치있는 것일까?



Laurel Maelynn Alley

(International Student Ambassador 1기, 연세대학교 국제학대학원)

많은 사람들이 공항 보안검색대의 긴 대기줄과 그로 인한 항공기 지연 위험, 다음 비행기를 타야 할지 모른다는 스트레스에 시달리고 있다. 하지만 만약 빠른 속도로 공항 보안 검색대를 통과하기 위해 당신의 프라이버시를 희생해야 한다면 어떨까?

현재 미국 국토안보부, 세관 및 국경 보호국의 일부는 생체인식출입구 Biometric Exit 라는 새로운 공항 보안 프로그램을 실시 중이다. 이 프로그램은 세관 비자 신청을 활용한 안면 인식 프로그램으로 앞으로 미국을 떠나는 방문객을 등록하고 국무부 여권 정보를 사용할 예정이다. 이미 여러 미국 공항에서 테스트를 시작했으며 2018년이면 모든 큰 규모의 공항에 설치될 것으로 예상된다. 항공사들에게는 고객의 공항 이용 만족도를 높이고 보안 프로세스를 가속화 할 수 있는 기회가 되겠지만 한편으로 프라이버시에 대한 우려가 뒤따르고 있다.

생체인식 출입구 프로그램은 9/11위원회에서 처음으로 국회에 위임되었지만 올해 트럼프 대통령에 의해 빠르게 추진되었다. 이 프로그램은 원래 비자 소지자의 신원을 확인하고 비자 연장 기간을 추적하기 위해 미국인 5천만 명에게만 적용될 예정이었다. 그러나 세관 및 국경 보안청은 이 프로그램이 사생활에 민감한 미국 시민을 포함한 모든 사람에게 적용될 수 있다고 말했다. 정부는 현재 미

국 시민 사진을 확인 후 폐기하고 있다고 말하면서도 향후 그러한 정보를 유지할 가능성을 배제하지 않고 있다.

존 와그너 John Wagner 세관 부국장은 지난 5월에 열린 커넥티드 ID ConnectedID 컨퍼런스에서, 시스템이 확장됨에 따라 시민권 여부와 관계없이 모든 국내 여행객에게 생체 인식 출입문 프로그램을 적용할 향후 계획에 대해 이야기 했다. 트럼프 대통령의 집행 명령이 비시민권자에 대한 사생활 보호법을 폐지하여 세관은 외국 여행자의 사진을 삭제할 법적 의무가 없다는 점에 주목해야 한다.

또한 이 프로그램은 얼굴 인식 기술에 있어 기술적 문제에 직면해 있다. 안면 인식 기술은 지문 또는 홍채 스캔과 같은 다른 생체 인식 기술보다 덜 정확하다. 국립 표준 기술 연구소는 탑승 게이트 시나리오에서 최고 알고리즘조차도 48,000명 중 4분의 1에 달하는 용의자를 인지하지 못한 것으로 나타났다. 또다른 문제점으로 MIT 미디어랩의 일부 얼굴 인식 알고리즘 테스트는 사람들의 피부색에 편향된 결과를 보였다. 미시간 주립 대학의 교수이자 안면 인식 전문가인 Anil Jain은 조명과 표정으로 인해 인식이 불가능할 수 있다는 우려를 표명했다. 그는 또한 5세 이상 차이가 나는 사진은 인식하지 못할 수 있다고 지적했다. 🤖

[Source]

- "Airport Face Scans Raise Privacy Concerns." PBS. July 15, 2017. <http://www.pbs.org/newshour/bb/airport-face-scans-raise-privacy-concerns/>.
- Brandom, Russell. "Airport Face Recognition Could Extend to US Citizens, Says Customs." The Verge. May 09, 2017. <https://www.theverge.com/2017/5/9/15591648/airport-facial-recognition-customs-tsa-biometric-exit>.

# 사이버 위험 보험의 출현



Claudine Ukubereyimfura  
(International Student Ambassador 1기, 연세대학교 언더우드국제대학)



우리는 정보와 지식이 전 세계의 조직 운영 방식을 결정하는 데 중요한 역할을 하는 시대에 살고 있다. 머지 않아 남아프리카공화국의 개인정보보호법, 유럽의 일반데이터 보호규정 General Data Protection Regulation 등이 사용자에게 더 나은 서비스를 제공하기 위해 구현될 것이다. 그에 따라 조직이 사이버 공격 위험에 대처하고 탄탄한 기업지배구조를 구축하기 위해 사이버 위험 보험의 필요성도 증대될 것이다.

4차 산업혁명의 도래와 함께 기술은 비즈니스 혁신, 사회 및 비즈니스 모델 변화에 있어 핵심적인 역할을 수행할 것이다. 따라서 향후 조직이 소유한 정보와 기술을 보호하기 위한 조치들이 필요해질 것이며 그러한 조치 중

하나가 사이버 위험 보험이 될 수 있다.

이러한 변화의 흐름을 주도하는 영국 안테미스Anthemis 그룹의 관계자에 따르면, "사이버 보험 시장은 데이터 과학 기술의 출현과 사회적시장경제Social Market Economy, SME 시장에 중점을 둔 사이버 기술 전문 기업의 출현으로 인해 빠르게 발전하고 있다."고 한다.

## 누가 사이버 위험 보험을 사용하는가?

안테미스 그룹 보고서에 따르면 사이버 위험 보험은 중소기업이 감당하기에는 지나치게 비용이 높아 가입 대상은 대부분 대기업이라고 한다. 그러나 최근 대기업과 중소기업 간의 격차를 줄이기 위해 노력하는 스타트업이 출현하기 시작했다.

## 미래 대응방안은?

사이버 공격 형태가 계속 진화함에 따라 확률론 및 적응형 AI 사이버 위험 모델에 대한 새로운 접근 방식이 필요하다. 조직이 사이버 위험에 대한 솔루션을 찾기 위해서는 우선 데이터가 일관되고 믿을 수 있는 방식으로 수집되고 제공될 필요가 있다. 🌐

[Source]

- <http://www.biztechafrika.com/article/cyber-security-insurance-missing-link-business-fin/12624/>

\* 본 연구소에서 제공되는 바른ICT뉴스레터는 국내외 우수 ICT 연구 동향 및 연구 결과를 정리하여 제공합니다.

\* 바른ICT뉴스레터를 정기적으로 받아보고 싶으신 분은 [news@barunict.kr](mailto:news@barunict.kr) 로 이메일 주시기 바랍니다.



Publisher 김범수 | Editor-in-Chief 김보라 | Editor 손수민

서울시 서대문구 연세로 50 연세대학교 302동 연세·삼성학술정보관 720호  
Phone: +82-2-2123-6694 | [www.barunict.kr](http://www.barunict.kr)

