온라인 광고산업의 발전과 프라이버시 침해*

손 상 영 (정보통신정책연구원 연구위원)
유 지 연 (정보통신정책연구원 부연구위원)

1. 서 론

온라인 광고는 일반적으로 인터넷을 통해 전달되는 광고를 지칭해왔다. 그러나 스마트폰이 보급되면서 온라인 광고의 개념은 모바일 인터넷과 모바일 앱을 통해 전달되는 모바일 광고까지 포함하게 되었다. 한국온라인광고협회에 의하면 국내 전체 광고시장에서 온라인 광고시장이 차지하는 비중은 2000년 2.3%에서 지속적으로 증가하여 2011년에는 21.2%에 도달하였으며 온라인 광고시장 규모는 1조 8천8백억 원으로 성장하였다. 또한 최근 삼성증권의 발표에 의하면 국내 모바일 광고시장은 2011년 온라인 광고시장의 3.1%에 불과하지만 향후 급속히 성장하여 2020년경에는 온라인 광고시장의 약 46%를 차지할 것으로 예측하였다.

온라인 광고기술이 발전하면서 온라인 광고는 광고효과를 제고하기 위해 기존 광고에서는 거의 불가능하였던 개인화된, 맞춤형 표적광고(personal, customized, target advertisement)를 지향하는 방향으로 발전하고 있다. 그런데 이를 위해서는 광고서비스 업체가 개인을 식별할 수 있는 정보뿐만 아니라 개인의 웹서핑에 대한 추적 정보, 소셜 네트워크에서의 활동정보 등 행태정보 그리고 현실공간에서의 위치추적 정보, 개인의 블로그나 댓글 분석 그리고 온라인 거래내역 분석 등을 통한 개인의 성향 및 선호 정보 등 소위 '빅 데이터 분석(big data analytics)'을 통해 개인정보를 수집, 활용하고 있으며 제3자에게 판매도 이루어지고 있다. 이에 따라 인터넷 이용자의 프라이버시 침해가 심화되고 있어 세계 주요국에서 프라이버시 보호 강화를 위한 정부와 의회의 움직임이 활발해지고 있다. 특히 미국의 공정경쟁 정책당국인 FTC(Federal Trade Commission)는 최근 프

* 본 원고는 2011년 정보통신정책연구원의 연구보고서 "온라인 광고시장에서 불공정행위와 대응방안"의 일부 내용을 재정리하고 보완하였음.

라이버시 보호를 위한 적극적인 활동을 하고 있다.

지금까지는 온라인 광고서비스 업자들의 개인정보 수집에 대해 프라이버시 침해의 관점에서 논의되어 왔지만 온라인 광고시장에서의 경쟁이 치열해 짐에 따라 경쟁 상대의 개인정보 수집행위의 불법성을 고발하고 경쟁당국에 제소하는 일종의 불공정경쟁 관련 사건이 발생할 가능성도 있다. 이것은 전통적인 광고시장에서는 발생할 수 없는 새로운 유형의 불공정경쟁 행위가 될 것이다. 온라인 광고서비스 사업자가 수집, 활용하는 개인정보들은 위에서 언급한 바와 같이 매우 다양하고 복잡하게 때문에 경쟁 상대의 정보수집의 불법성을 밝혀내기 위해서는 고도의 전문성이 필요하게 된다. 이에 따라 이런 업무를 전문적으로 위탁 수행할 새로운 사업체들이 등장할 수도 있다.

본고는 온라인 광고산업의 발전이 야기하는 프라이버시 침해 심화의 문제에 대한 대책을 마련하고 향후 발생 가능한 개인정보 수집과 관련된 온라인 광고서비스 업체간 갈등에 대응하기 위한 기본적인 논의와 정책 방향을 도출하는 것을 목표로 한다. 이를 위해 온라인 광고시장의 주요 플레이어인 애플과 구글의 이용자 추적사건과 이에 대한 청문회 내용을 검토하고, 미국을 비롯한 주요국들의 프라이버시 정책방향의 변화 움직임을 살펴본다. 이상의 논의를 바탕으로 프라이버시 보호관련 쟁점을 제시하고 정책방향을 도출하고자 한다.

본고는 다음과 같이 구성된다. 제2장에서는 2011년에 발생한 애플과 구글의 사용자 추적사건의 개요와 이 사건에 대한 미국 의회의 청문회 내용을 소개한다. 제3장에서는 최근 온라인 광고분야에서 광고 효과를 제고하기 위해 어떻게 빅 데이터 분석기법을 활용하고 있는지를 설명한다. 제4장에서는 미국, EU, 일본 그리고 한국의 개인정보보호 법제를 간략하게 소개하고 최근 온라인 광고업체들에 의한 프라이버시 침해 심화에 따른 정책적 대응 방향을 파악한다. 제5장에서는 프라이버시 보호와 개인정보 이용의 조화를 도모하는 법제도적 방법 이외의 대안적 정책과 전략에 대한 사례들을 소개하고 그 시사점에 대해 논의한다. 제6장에서는 '비식별개인정보' '포괄적 동의' '쿠키에 의한 정보수집' '불공정 약관' 등 최근 온라인상의 프라이버시 침해와 관련된 대표적인 쟁점들을 소개하고 이에 대한 정책적 대응방향을 논한다.

2. 애플과 구글의 사용자 추적 사건

1) 사건 개요

2011년 4월 애플은 사용자의 동의 없이 사용자의 위치를 추적하고 있었다는 이유로 고발당하였다. 애플의 iOS 기기는 한 백업 파일에 다량의 위치정보를 저장하고 있음이 드러났다. 게다가 그 파일은 암호화되어 있지 않아서 누군가 그 파일에 접근할 수 있다면 그 파일에 들어있는 정보를 이용하여 사용자를 추적할 수 있게 되며 이는 사용자의 프라이버시를 침해함을 의미한다.

애플 측에서는 그 데이터는 GPS 신호가 약한 경우 사용자 기기가 사용자의 위치를 보다 신속하게 파악하기 위해 인근 기지국이나 WiFi 접근점의 위치를 애플로부터 내려받은 것들을 저장한

것이라고 해명하였다. 그러나 애플은 데이터가 필요 이상으로 많이 저장되었음을 시인하고 iOS를 업그레이드 하면서 저장되는 데이터 양을 제한하고 암호화하며 사용자의 기기에 백업되지 않도록 하겠다고 하였다. 또한 사용자가 새 기기를 처음 설정할 때 익명의 진단정보를 애플로 전송할 것을 선택하면 애플의 iOS 기기는 주기적으로 기지국과 WiFi 위치를 수집하고 있다고 하였다. 그리고 이 데이터는 암호화되어 있고 ID를 포함하지 않기 때문에 이 데이터를 이용해서 애플이 특정 사용자를 추적하는 것은 불가능하다고 하였다.

안드로이드 기기도 애플의 iOS 기기와 유사하게 기지국과 WiFi 위치를 저장하고 있는 것으로 알려졌다. 다만 안드로이드 경우는 기지국과 WiFi 숫자를 가장 최근 위치부터 각각 50개와 200개로 제한하고 있다. 안드로이드 기기는 수초에 한 번씩 이러한 위치정보를 수집하여 한 시간에 몇 번씩 구글로 전송하며 구글은 이 데이터에 무작위의 ID를 붙여 놓아서 이 데이터가 누구에 관한 정보인지 간단하게 알아낼 수는 없으나 고도의 개인식별 기술을 적용하면 데이터의 주인을 알아낼 수 있다고 한다. 구글도 프라이버시 침해로 고발당하였다.

국내에서는 한 변호사가 애플이 아이폰을 이용하여 자신의 위치정보를 수집하여 정신적 피해를 주었다고 애플을 상대로 소송을 제기한 결과 승소하여 100만원의 위자료를 받았다. 2011년 8월 3일 방송통신위원회는 애플 코리아가 사용자의 동의가 철회된 이후에도 이를 무시하고 계속 위치정보를 스마트폰에 저장한 행위에 대해 300만 원의 과태료를 부과하였고, 애플코리아와 구글코리아가 위치정보를 암호화하지 않고 사용자 기기에 저장한 행위에 대해서는 시정명령을 내렸다. 한편 미국과 유럽 각국에서는 이 사건에 대한 법적 공방이 진행되고 있다.

2) 사건 관련 미국 의회 청문회 내용

애플과 구글의 사용자 위치정보 수집사건을 계기로 미국 의회에서는 이에 대한 청문회가 열렸다. 2011년 5월 10일 미국 상원의 '프라이버시, 기술 그리고 법'에 관한 법률 소위원회에서는 "Protecting Mobile Privacy: Your Smartphone, Tablets, Cell Phones and Your Privacy"라는 제목 하에 청문회가 열렸다. 이 청문회에는 상원의원들과 관련 정부관료 그리고 해당 업계 대표와 민간 전문가들이 참석하여 자신의 의견을 개진하였다. 그 주요 내용은 다음과 같다.

이 청문회의 의장인 상원의원 Franken은 위치기반 서비스가 제공하는 혜택과 프라이버시에 대한 국민의 권리 사이에 균형을 찾는 것이 청문회의 궁극적 목표라고 하였다.

FTC의 대표자는 모바일 기기는 항상 연결되어 있고 항상 소비자와 같이 있기 때문에 모바일 기기는 속성상 매우 개인적인 정보를 가지고 있으며 모바일 기업은 청소년을 포함한 모바일 기기 이용자를 추적할 수 있는 능력을 가지고 있다고 하였다. FTC는 모바일 기기 사용 중에는 접근하기 어려운 모바일 기업의 프라이버시 정책에 의존하지 말고 이용자가 언제 어떻게 자신의 정보가 이용되고 있는지를 알려주는 간단한 방법을 모바일 기기에 내재시키는 기술을 개발할 것을 권유하고 있다고 하였다. 또한 기업들은 자신의 제품과 서비스를 개발할 때 프라이버시를 설계원칙으

로서 실행함으로써 소비자가 자신의 정보가 어떻게 이용되고 있는지를 쉽게 이해하고 선택할 수 있도록 할 것을 권고한다고 하였다.

애플의 대표자는 애플은 사용자의 위치를 추적하지 않으며 그런 적도 없다고 주장하였다. 또한 애플의 기기들은 특정 소비자에게 고유한 정보를 애플에게 전송하지 않는다고 하였다. 애플은 소비자들이 이용할 수 있는 앱들을 계약에 의해 관리하고 있으며 만약 앱이 애플의 프라이버시 요구사항을 충족하지 않는다면 앱스토어는 그러한 앱들을 취급하지 않는다고 하였다. 또한 애플은 앱스토어가 취급하는 앱들이 애플 소비자들의 프라이버시를 적절히 보호하도록 앱들에 의해 발생하는 네트워크 트래픽을 무작위로 감시하고 조사한다고 하였다. 애플의 iOS에서 어떤 앱이 위치정보를 이용하면 스크린 우측 상단에 자주색 아이콘이 나타나서 이용자가 그 사실을 알게 함으로써 프라이버시 정책이 서비스에 내재되도록 하고 있다고 하였다. 그러나 현재의 iOS는 위치정보를 지나치게 오랫동안 저장하는 경향이 있어 조만간 이를 시정할 것이라고 설명하였다.

구글의 대표자는 구글은 소비자가 원하는 경우에 한해서 위치기반 서비스를 제공하며 소비자가 원한다는 의사표시를 하지 않는 경우에는 그의 모바일 기기는 구글에게 어떠한 위치정보도 전송하지 않는다고 주장했다. 또한 모든 제삼자 앱은 앱이 사용자의 기기에 설치되기 전에 사용자에게 앱이 사용자의 위치정보에 접근한다는 것을 고지해야 하고 이에 대해 사용자의 동의를 받아야 한다고 하였다. 구글은 사용자의 사전 동의를 받은 경우에만 위치정보를 수집하고, 일단 수집된 정보는 익명성을 보장하는 고도의 안전성 기준을 실행하는 등 사용자에게 정보 취급 관행에 관한 고도의 투명한 정보를 제공하고 있다고 하였다.

끝으로 청문회 의장인 Franken 상원의원은 현행법은 소비자에게 충분한 프라이버시를 보장하지 못하고 있으며 법제나 정부기관의 법 집행이 기술의 발전을 따라가지 못하고 있다고 하였다. 또한 그는 소비자들은 어떠한 개인정보가 수집되고 있는지, 언제 그리고 누구와 그들의 정보가 공유되고 있는지에 대해 알 기본적인 권리가 있다고 주장하였다. 그리고 이러한 권리는 모바일 기기로부터 발생하는 데이터와 같이 민감한 정보에 관해서는 특히 중요하다고 하였다.

위의 공청회에 이어서 2011년 5월 19일 미국 상원의 다른 소위원회에서 모바일 기기와 관련된 프라이버시 문제를 다루는 공청회가 열렸다. 여기서는 FTC, 애플, 페이스북 그리고 구글의 대표자들이 증인으로 채택되었다. 이 청문회는 상원의원 Rockefeller와 상원의원 Pryor가 주재하였는데 그들의 궁극적인 목적은 모바일 기기들이 대량의 개인정보를 수집하고 전송하는 이 시대에 소비자의 프라이버시를 보호하기 위한 법적 기준을 마련하는데 있어서 정부의 역할이 무엇인가를 규명하는 것이다.

상원의원 Kerry는 “프라이버시가 혁신의 적이다”라는 일부 주장에 반대한다고 하면서 소비자의 신뢰가 증가하면 소비자들은 더 많은 서비스에 가입할 것이라고 하였고, 소비자에게 어떤 정보가 수집되고 있는지, 왜 그들의 위치가 추적되고 있는지, 그 정보가 어떻게 제삼자들과 공유되는지를 고지하는 종합적인 기초 프라이버시 기준을 요구한다고 하였다.

다음은 증인들의 발언요지이다. FTC의 대표자는 지난 5월 10일 청문회에서의 FTC 대표자와 마찬가지로 프라이버시가 서비스에 포함되도록 설계할 것을 권고하였다. 페이스북의 대표자는 10년 전의 인터넷은 정적인 환경이었으나 오늘날 인터넷은 사회관계와 정보공유를 통해서 동적인 경험을 하는 환경으로 변모하고 있다고 말하면서 프라이버시 보호를 위해 사용자, 서비스 제공자, 제삼자 개발자 그리고 입법가 등 모두가 나름대로의 역할이 있음을 강조하였다.

애플의 대표자는 5월 10일 청문회에서와 마찬가지로 애플의 엄격한 프라이버시 규정을 홍보하면서 애플은 최근 자신의 온라인 광고서비스 자회사인 iAd의 정책을 개정하여 어린이를 표적으로 하는 앱 광고와 미성년자들로부터 정보를 수집하려는 의도가 있는 앱을 불허한다고 하였다.

구글의 대표자는 구글지도 사용의 40%는 모바일 기기에서 이루어진다고 하면서 소비자가 자신의 프라이버시가 보호된다고 믿지 않는다면 이러한 서비스는 지속되지 않을 것이라고 주장하였다. 상원의원 Thune이 구글은 최근 Gmail과 구글의 실패한 SNS인 Buzz 사이에 부적절한 정보교환으로 구글이 FTC의 감시 하에 있음을 지적하자 구글의 대표자는 구글은 프라이버시를 최우선으로 하는 정책을 채택해왔으며 이용자들로부터 적극적인 동의를 받아왔다고 주장하였다. 또한 구글은 향후 20년간 프라이버시 정책의 실행에 대하여 FTC의 감사를 받도록 협약을 맺었음을 언급하였다.

미디어 업계 전문가로 이 청문회에 참석한 Amy Shenkan은 어린이들의 프라이버시를 강조하면서 다음과 같이 법제화되어야 할 5개의 행동지침을 제시하였다. 첫째, 정보수집과 공유에 있어서 정보주체의 동의에 관해서는 사전동의(opt-in)가 업계표준이 되어야 한다. 둘째, 명확하고 투명한 정책이 있어야 한다. 셋째, 미성년에 대한 추적은 절대 금지되어야 한다. 넷째, 아이들과 부모를 위한 프라이버시 인식과 교육이 제고되어야 한다. 다섯째, 아이들과 부모가 온라인에서 부적절한 정보를 쉽고 안전하게 제거할 수 있는 메커니즘을 가져야 한다.

애플과 구글의 사용자 추적 사건과 이에 따른 미국 의회 청문회는 뒤에서 소개할 프라이버시 강화를 위한 입법 추진을 촉발하게 된다. 위에서 소개된 청문회에서의 논의 내용이 주는 시사점을 다음과 같이 정리된다. 첫째, 서비스가 주는 혜택과 프라이버시 침해는 trade-off 관계가 있으므로 사회후생을 극대화 할 수 있는 균형점에 대한 사회적 합의를 도출하는데 정부의 역할이 있다. 둘째, 소비자는 자신이 개인정보를 누가 어떤 목적으로 수집하고 누구와 공유하는지에 대해 알 권리가 있고 이를 통제할 권리가 있다. 셋째, 기업의 정보 수집 및 활용 과정이 투명해질수록 소비자들은 그 기업을 신뢰하게 되어 그 기업이 제공하는 서비스를 더 많이 활용하게 된다. 온라인 광고업체도 사회적 신뢰를 받게 되면 소비자는 그 업체가 제공하는 광고에 대한 거부감이 줄어들 것이다.

3. 빅 데이터 분석과 온라인 광고

페이스북, 애플 등의 기업들이 자신의 이용자들에 관한 정보, 특히 앱을 이용하면서 발생시키는 정보들을 추적하고 수집하여 효과적인 맞춤형 광고 서비스 제공에 활용하려는 의도를 보이자 미

국의 FTC는 백악관에게 인터넷 상의 사생활 보호를 위한 조치를 강화해 줄 것을 촉구한 바 있다. FTC는 웹상에서의 행적을 추적하지 못하게 하는 선택권을 인터넷 이용자에게 부여하는 'Do Not Track mechanism'을 실행할 것을 권고하였다. 미국의 사례가 시사하는 바와 같이 경쟁당국은 광고시장에서의 경쟁촉진과 함께 프라이버시의 문제를 동시에 고려해야 할 상황을 맞이하고 있다.

최근 급속히 발전하고 있는 빅 데이터 분석은 웹, 소셜 네트워크 상에서 발생하고 있는 수많은 개인의 행적들을 실시간으로 추적하고 분석하여 광고, 마케팅에 활용하고자 하므로 이에 따라 프라이버시의 문제가 더욱 심각해 질 것으로 예상된다. 사람들은 온라인에서 그리고 점점 더 모바일 기기를 통해서 행위들을 하고 있다. 그 과정에서 사람들은 자신의 디지털 표상을 남기게 되는데 그것은 자신의 관심, 욕망, 필요, 구매행위, 사회적 연결과 관계의 범위뿐만 아니라 물리적 공간과 시간으로 표현되는 현 위치의 의미까지도 표시하게 된다. 즉 우리 자신의 프로파일을 만들어 내면서 자기 자신이 인지하고 있는 것보다 더 많은 것을 드러내게 된다.

> "어디를 가든지 무엇을 하든지 이 세상 어디에서도 무엇인가가 당신을 추적하고 있다. 당신의 랩톱과 아이패드, 스마트폰 또는 블랙베리와 같은 개인기기들은 당신이 좋아하는 것, 관심사, 선호하는 항공사, 좋아하는 휴가장소, 당신의 지출규모, 정치적 관계, 친구관계, 구독하는 잡지, 운전하는 자동차의 메이커와 모델, 구입하는 식품의 종류 등등에 대한 자세한 문건을 작성하는데 역할을 하고 기여한다. ... 편리한 교통카드는 당신의 통근을 용이하게 하지만 특정일, 특정 시간에 당신이 어디에 있었는지를 정확한 그림으로 보여주는데 도움을 줄 수 있다. 이는 ATM 기계에 부착된, 가게 안에, 은행에, 주유소에, 고속도로에, 교차로에 있는 비디오 카메라들도 미찬가지다(Craig and Ludloff, 2011: 43)."

정보기술이 발전하고 그 편리성이 증가하여 더 많이 활용할수록 그에 대한 대가로 이용자는 자신의 프라이버시를 지불해야 한다. 더군다나 이용자는 자신의 프라이버시가 침해당하고 있다는 사실조차도 인지하기 어렵다. 다음 사례는 이러한 가능성을 시사하고 있다.

> "iPhone 4S가 제공하는 새로운 기능으로서 음성인식 기반 개인비서 서비스인 시리(Siri)가 있다. 시리는 애플의 서버를 이용해서 질의어를 처리하고 관련 결과를 보여주기 때문에 3G나 와이파이로 인터넷 연결이 되어 있어야 이용이 가능하다...시리는 인공지능 기능이 있어서 시간이 지나면 사용자가 선호하는 것을 인지한 다음 그에 가장 알맞게 결과를 내놓을 수 있다(주간기술동향 2011. 10.28: 42)."

시리의 이용자는 음성인식과 인공지능 덕분에 매우 편리한 검색 서비스를 받을 수 있겠지만 시리의 인공지능은 이용자의 선호를 분석하여 그 결과는 애플의 서버로 전송될 것이고 애플은 이 결과를 이 이용자를 표적으로 하는 온라인 광고를 제공하는데 활용할 수 있을 것이다.

인터넷 기업들이 이용자 개인정보를 취득하는 가장 쉬운 방법은 자신의 사이트에서 이용자들이

상호작용을 하면서 많은 정보들을 자발적으로 제공하는 것이다. 그러나 인터넷 기업들은 자신이 필요로 하는 정보를 획득하기 위해 쿠키, 스파이웨어, Packet Inspection과 같은 적극적인 디지털 추적기술을 사용한다.

많은 데이터가 수집되고 다른 데이터 세트와 연계되면 개인정보라고 여겨지는 정보들을 획득할 수 있게 되고 나아가 그 정보를 특정 개인과 결부시킬 수도 있게 된다. 다양한 경로를 통해 수집된 추적정보들로 이루어진 다수의 데이터 세트를 가지고 개인에 대한 상세한 프로파일을 만들어 갈 수도 있다.

온라인 광고시장에는 웹 이용자들의 행적을 추적하는 수백 개의 온라인 광고회사들이 생태계를 형성하고 있다. 그들은 대부분 자신의 추적 네트워크를 가지고 이용자들에 대한 데이터를 수집하여 광고주들에게 직접 판매해 왔으며 최근에는 거의 실시간으로 이용자 데이터에 대한 거래가 이루어지고 있다.

4. 주요국 프라이버시 정책 동향

1) 미국

미국에서 프라이버시의 보호와 관련하여 입법화 논의가 진행된 것은 1972년에 있었던 워터게이트 사건으로부터 시작된다. 이로 인하여 1974년에 현대적 의미로는 최초로 프라이버시에 대한 권리가 포함된 프라이버시법(Privacy Act of 1974)이 입법화되었다. 미국의 개인정보보호 법률은 공공부문과 민간부분이 분리되어 각 분야에서 필요에 의해 개인정보보호 법규를 정비하는 개별법 체계를 따르고 있으며 공공, 민간부문을 통합적으로 포괄하는 개인정보보호 법률체계가 정비되어 있지는 않는데, 프라이버시법은 미국 공공부문에 한정되어 일반법적인 역할을 담당하고 있다.

1974년의 프라이버시법은 개인정보를 처리하는 각 공공기관이 준수하여야 할 의무와 정보주체의 권리들을 상세하게 규정하고 있다. 물론 이 법은 유럽처럼 그 의무와 권리를 집행하는 독립된 감독기구를 별도로 두고 있지는 않지만, 연방 공공기관에 대해서는 '프라이버시법'에 의해 관리예산처(OMB)가, 민간분야에 대해서는 FTC가 주도적으로 개인정보보호업무를 담당하고 있다. 나아가 법원에 의한 효과적인 권리구제절차를 마련해 놓고 있다.[1)]

예컨대, 미국의 비디오프라이버시보호법(Video Privacy Protection Act)은 비디오 가게에서 고객이 빌린 특정 영화의 제목을 공개하는 것을 금지하고 있을 뿐이고, 인터넷상에서 스트리밍 비디오(streaming video)를 보는 관람행위에 대해서는 아무런 보호를 하지 않고 있다. 이러한 부분적 보호의 접근모델에 있어서 개인정보보호의 기준을 설정하는 기본원칙은 자율규제이다. 즉 개인정보보호는 의회의 법 제정에 의한 법적 권리에 의해서라기보다 주로 산업계의 자율규범 내지 실무

1) 미국의 권리구제절차 및 개인정보보호법률에 대한 상세한 소개는 김일환(1999) pp.325-400 참조.

규약이나 계약에 의해 이루어지고 있다.

특히 미국은 자유로운 정보유통(free flow of information)을 제1의 원리로 삼는 강한 언론자유의 전통을 가지고 있다. 자유로운 정보유통이 사적 활동과 자율을 촉진시키는 것이기 때문에, 그만큼 정부규제보다는 사적 계약이야말로 개인정보보호의 기본원칙이 되어야 하고, 이에 따라 개인은 자기 자신의 권리를 스스로 주장하고 요구하여야 한다는 것이다(Reidenberg, 2000: 1342).

이러한 자유주의적 전통은 미국이 개인정보보호의 기본원칙들을 집행함에 있어서 큰 의미를 가진다. 포괄적인 입법이 아닌 부문별 입법을 통한 접근방법은 민간영역에서 이루어지는 개인정보처리에 대해 정부의 개입을 최소화하고자 하는 것이다. 즉 법에서 개인정보가 어느 범위까지 보호되어야 할 것인지에 관한 실체적 내용을 규율한다기보다 시장거래과정(market process)을 규제하는 것에 초점을 맞추어져 있다.

<표 1> 미국의 개인정보보호법제 현황

보호대상	개인정보 관련 주요 법률
신용정보	공정신용평가법(Fair Credit Reporting Act, 1970)
정부보유정보	프라이버시법(Privacy Act, 1974)
정부보유정보	정보공개법(Freedom of Information Act, 1974)
교육정보	가족의교육권및프라이버시법(Family Education Rights and Privacy Act, 1974)
금융정보	금융프라이버시권법(Right to Financial Privacy Act, 1978)
출간정보	프라이버시보호법(Privacy Protection Act, 1980)
케이블통신정보	케이블통신정책법(Cable Communications Policy Act, 1984)
전자기록정보	전자통신프라이버시법(Electronic Communications Privacy Act, 1986)
컴퓨터접근정보	컴퓨터사기및남용방지법(Computer Fraud and Abuse Act, 1986)
컴퓨터보안정보	컴퓨터보안법(Computer Security Act, 1987)
비디오대여정보	비디오프라이버시보호법 (Video Privacy Protection Act, 1988)
연방수혜자정보	컴퓨터정보결합및프라이버시보호법(Computer Matching and Privacy Protection Act, 1988)
근로자정보	근로자거짓말탐지기보호법(Employee Polygraph Protection Act, 1988)
텔레마케팅거부정보	전화소비자보호법(Telephone Consumer Protection Act, 1991)
운전자 및 차량정보	운전자프라이버시보호법(Driver's Privacy Protection Act, 1994)
통신정보	법집행을위한통신지원법(Communications Assistance for Law Enforcement Act, 1994)
통화정보	전기통신법(Telecommunications Act, 1996)
의료정보	건강보험관리및책임에관한법률(Health Insurance Portability and Accountability Act, 1996)
온라인이용아동정보	아동온라인프라이버시보호법(Child Online Privacy Protection Act, 1998)
고객금융정보	금융현대화법(Gramm-Leach-Bliley Act, 1999)
테러방지용정보	대테러감시법(Patriot Act, 2001)
전자정부서비스정보	전자정부법(E-government Act, 2002)
CCTV 등	비디오감시방지법(Video Voyeurism Prevention Act of 2004)

자료: 한국전산원, 2004.

이로 인하여 민간부문에서는 각 산업분야와 관련하여 다양한 법률이 제정되어 있다. 민간부문의 대표적인 개인정보 관련 입법현황은 <표 1>과 같다.

21세기 들어 온라인 광고가 활성화되면서 이용자 행태정보 기반 온라인 광고의 프라이버시 침해에 대응한 입법 시도가 있었으나 아직 논의가 진행 중이다. 그동안의 경과와 주요 논의 내용은 다음과 같다. FTC는 행태정보 기반 온라인광고로 인한 이용자 프라이버시 침해의 방지를 위한 광고업계의 자율규제를 촉구하며 2009년 2월에 '행태정보 기반 온라인광고에 대한 자율규제 원칙(Self-regulatory Principles for Online Behavioral Advertising)'을 다음과 같이 제시하였다.

① 투명성 및 이용자 통제권(Transparency and Consumer Control)
② 이용자 정보에 대한 합리적인 보안과 정보 보유 제한(Reasonable Security and Limites Data Retention for Consumer Data)
③ 기존 프라이버시 정책에 대한 중대한 변경 시 명시적 동의 획득(Affirmative Express consent for Material Changes to Existing Privacy Promises)
④ 행태 기반 광고 목적을 위한 민감 정보 이용 시에 명시적인 동의 획득 또는 금지(Affirmative Express consent to (or Prohibition Against) Using Sensitive Data for Behavioral Advertising)

FTC는 이보다 앞서 2007년 11월에 공청회를 개최하고 행태정보 기반 온라인광고를 위한 개인정보 수집 · 처리 · 활용에 대한 가이드라인을 다음과 같이 제안하였다.[2)]

① 온라인상의 행동양태에 따른 맞춤형 광고를 위해 이용자 정보를 수집하는 모든 웹사이트는 명확하고 눈에 쉽게 띄는 통지(clear and prominent notice)를 이용자에게 주어야 하고 이용자에게는 그러한 목적을 위해서 본인의 정보가 수집되는 것을 거절할 수 있는 선택권을 부여하여야 한다.
② 온라인상의 행동양태에 따른 맞춤형 광고를 위해 사용자 정보를 수집하거나 저장하는 모든 사업자는 해당 데이터에 대한 적절한 보안(reasonable security)을 제공하여야 하며 수집된 데이터는 합법적인 사업상의 목적, 또는 법 집행을 위하여 필요한 기간 동안만 보관하여야 한다.
③ 사업자가 사용자 정보를 수집하던 당시 사용자에게 약속한 정책과 상당히 다른 방법으로 사용자 정보를 사용한다면 그러한 사용 이전에 사용자로부터 긍정적이고 명확한 동의(affirmative express consent)를 얻어야 한다.

2) http://www.ftc.gov/opa/2007/12/principles.shtm

④ 사업자는 사용자로부터 긍정적이고 명확한 동의 없이는 온라인상의 행동양태에 따른 맞춤형 광고를 위하여 민감 정보를 수집할 수 없다.

또한 FTC는 가이드라인에서 식별개인정보 뿐만 아니라 온라인 광고를 위해 수집된 특정한 이용자의 정보 또는 컴퓨터 · 장치 그리고 개인을 식별할 수 있는 장치들과 연관될 수 있는 것이라고 하면 어떤 개인정보라도 보호의 대상이 되어야 한다고 규정하였다.[3] 그리고 개인적으로 민감한 정보의 수집 및 이용 등에 의하여 제기되는 프라이버시 침해 이슈가 더욱 심각해짐에 따라 온라인 행태 광고를 제공하는 기업들은 개인정보를 수집하기 전에 이용자들로부터 명시적인 동의를 받도록 촉구하였다.

FTC의 가이드라인이 기업들에게 규제의 지침과 방향성을 제시해 주었다는 점에서는 큰 의의가 있다. FTC의 가이드라인 발표 후 많은 사업자들은 이용자가 온라인 맞춤형 광고를 거절할 수 있는 절차를 마련하였고 야후와 구글은 이용자가 사후거부(opt-out) 할 수 있는 절차를 제공하였다. 또한 마이크로소프트사는 사용자가 브라우징이나 검색 히스토리, 쿠키, 폼데이터와 비밀번호 등을 저장하지 않도록 설정할 수 있는 기능을 개발하였고, 사용자 기능을 설정하고 사용자가 로그오프하면 사용자의 브라우저 캐시가 모두 삭제되는 기능을 Internet Explorer 8에 추가하였다(양지연, 2009: 11).[4]

미국의 5대 광고단체들은[5] 2009년 7월에 온라인 광고의 집행과정(개인정보 수집 또는 활용단계)에서 수반되는 프라이버시 침해문제를 예방하고, 온라인 광고에 대한 신뢰를 향상시키기 위하여 자율 협정인 "온라인 행태광고를 위한 자율규제안"을 발표하였다. 이 자율규제안은 아래와 같은 7가지 원칙으로 구성되어 있으며, FTC의 규제원칙과 부합한다.

① 투명성의 원칙이다. 서비스제공자[6] 및 제3자는[7] 온라인 광고에 따른 정보수집 및 사용에

3) FTC에 의하면 식별개인정보(PII: Personally Identifiable Information)는 개인을 식별하거나, 개인을 접촉하거나 또는 위치를 알아낼 수 있는 정보, 그러한 정보를 이용하여 개인의 식별정보나 또는 연락정보를 추출해 낼 수 있는 정보를 의미한다. 개인식별가능한 정보에는 이름, 주소, 전화번호, 팩스번호, 이메일 주소, 재무정보, 의료기록, 사회보장번호(social security number), 그리고 신용카드정보 등이 포함된다. 또한 개인에 관한 프로파일, 특이식별정보(Unique Identifier), 생체정보, 그리고/또는 IP주소가 개인식별가능한 정보와 연관될 때에는 그러한 정보도 개인식별가능한 정보로 간주된다. 그러나 익명으로 수집된 정보(개인사용자의 신분증명정보를 사용하지 않고 수집된 정보, 또는 개인과 연결이 되지 않는 인구통계학적인 정보)는 제외된다(양지연, 2009: 8).

4) http://yhoo.client.shareholder.com/releasedetail.cfm?ReleaseID=327212
http://googleblog.blogspot.com/2008/08/new-enhancements-on-google-content.html 참조.

5) 미국광고대행사협회(AAAA: American Association of Advertising Agencies), 미국광고주협회(ANA: Association of National Advertisers), 다이렉트마케팅협회(DMA: Direct Marketing Association), 양방향광고협회(IAB: Interactive Advertising Bureau), 경영개선위원회(CBBB: Council of Better Business Bureaus)

6) 인터넷 접속 서비스, 툴바, 인터넷 브라우저, 데스크탑 응용 소프트웨어 또는 클라이언트 소프트웨어 제공자로서 그 기업의 활동 중에 온라인 행태광고를 위해 웹브라우저가 거쳐간 모든 URL로부터 나온 정보를 수집

대한 설명 내용과 프라이버시 보호정책 등을 이용자가 쉽고 명확하게 확인할 수 있도록 웹사이트를 통하여 설명하여야 하며, 이 경우 식별개인정보를 포함한 수집정보의 유형 및 용도를 명확하게 설명하여야 한다.

② 이용자 통제권의 원칙이다. 제3자는 온라인 광고를 목적으로 정보를 수집 또는 사용하는 경우 이용자에게 그 수집 및 사용에 대한 결정권이 있음을 고지하여야 한다.

③ 온라인 광고에 대한 서비스 제공자의 책임이다. 서비스 제공자는 이용자의 동의 없이 온라인 광고를 목적으로 정보를 수집하거나 사용할 수 없다. 인터넷서비스 제공자는 이용자로부터 동의를 받은 경우에도 온라인 광고를 위한 정보 수집 및 사용에 대한 동의를 철회할 수 있는 수단을 마련하여야 한다.

④ 정보보안의 원칙이다. 기업은 온라인 광고를 목적으로 수집, 사용되는 정보들을 보호하기 위하여 적절한 물리적 · 전자적 · 관리적 보호조치들을 마련하여야 하고, 정보보안표준은 연방통신위원회의 개인정보보호에 관한 내용을 준용하되 정보의 민감성을 고려하여 융통성 있게 변경할 수 있어야 한다. 이 경우 정보의 재구성 방지를 위해 식별개인정보나 독특한 식별자를 변경 · 익명화하고 무작위(randomize)하여야 한다. 온라인 광고를 위해 수집되고 이용되는 정보는 합법적인 사업을 위하여 필요한 기간 또는 관련 법률에서 요구하는 기간만큼만 보관하여야 한다. 서비스 제공자는 수집된 정보가 온라인광고를 위한 목적으로 사용되고 있음을 밝혀야 하고, 이 같은 사실은 문서화된 증서로 증명하여야 한다.

⑤ 종래의 온라인 광고 정책 및 관행 개정에 관한 원칙이다. 기업은 온라인 광고를 위한 정보 수집 정책 및 관행의 개정에 앞서 이용자에게 동의를 얻어야 하며, 주요한 내용의 개정 이전에는 기존 정책과 관행을 유지하여야 한다. 정책 및 관행의 개정 이전에 수집된 정보에 대해서도 동 정보를 이용하기 위해서는 반드시 동의가 필요하다.

⑥ 민감한 정보의 수집제한 원칙이다. 아동의 온라인 프라이버시 보호법(COPPA: Children's Online Privacy Protection Act)[8] 규정에 따르면 13세 미만의 아동에 대한 개인정보는 수집이 제한된다. 금융계좌번호, 사회보장번호, 의약품처방전, 의료기록 등에 대하여 개인의 동의 없이 수집할 수 없다.

⑦ 관리책임의 원칙이다. 광고단체들에게는 온라인 행태광고 자율규제안을 더욱 발전시켜야 할 책임이 요구된다. 온라인 행태광고 자율규제 프로그램에 따라 온라인 행태광고에 관여하는 기업이 규제되고, 기업이 자율규제를 따를 수 있도록 도움을 주는 시스템이 구축되어야 한

하고 사용하는 범위까지를 자율규제의 대상으로 본다.

7) 관계자 이외의 웹사이트(non-affiliate's Web site)에서 온라인 행태광고에 참여하는 기업을 말한다. 예를 들어 광고주가 온라인 행태광고 목적으로 정보를 수집하면 제3자가 되며, 제3자에 대한 책임이 부여된다. 이때 관계자(affiliate)라 함은 다른 기업을 통제하거나, 다른 기업에 의해서 통제 받거나 또는 다른 기업과 공동의 통제를 받고 있는 기업을 말한다.

8) COPPA는 아동들의 정보수집에 있어서 부모의 동의를 받도록 요구하고 있다.

다.

미국 하원 에너지통상위원회의 통신 · 기술 · 인터넷 소위원회에서 Rick Boucher 의원, Cliff Sterns 의원과 Bobby Rush 의원 등은 2010월 9월에 온라인광고 시장에서 프라이버시를 보호하기 위한 인터넷 프라이버시 법안(Internet Privacy Bill)을 제안한 바 있다. 동 법안은 크게 네 가지 내용을 담고 있다.

① 프라이버시 정책의 공개에 관한 내용이다. 식별개인정보를 수집하는 기업은 개인정보가 어떻게 수집 · 이용 · 공개되는지를 설명하는 이해하기 쉬운 명문의 프라이버시 정책을 고지해야 한다.
② 정보의 수집 및 이용에 관한 내용이다. 일반적으로 기업이 개인정보를 수집하는 것에 대해서 개인이 사후거부를 하지 않는다면 해당 기업은 개인정보를 수집해도 된다. 기업은 개인의료기록, 금융계좌, 사회보장번호, 성적 성향, 정치적 성향 및 정확한 지리적 위치와 관련된 정보를 포함한 개인의 민감정보를 수집하기 위해서는 해당 개인의 사전동의가 필요하다.
③ 제3자에 대한 정보의 공개에 관한 내용이다. 기업이 업무처리상의 목적 이외에 식별개인정보를 제3자와 공유하기 위해서는 개인의 동의를 얻어야 한다.
④ 이행과 집행에 관한 내용이다. FTC는 개인정보 관련 조치들을 이행하고 집행하기 위한 규칙을 채택하고 각 주는 FTC의 규칙을 주 법무장관이나 주 소비자보호원을 통하여 집행한다.

2011년 2월 상원의원 Jackie Speier는 인터넷 이용자들이 인터넷 상에서 자신의 정보를 추적하고 사용하는 것을 사전 거부할 수 있는 "Do-Not-Track Online Act of 2011"를 제안하였다. 또한 FTC로 하여금 이 법을 집행하도록 하였다. 그 후에 마이크로소프트가 먼저 자신의 차기 Internet Explorer 브라우저에 Do-Not-Track을 내재할 것이라고 발표하였고, 구글도 유사한 반응을 보였다. 그러나 이 법안은 NetChoice의 부실법안의 리스트에 들어가면서 관련 업계의 비판을 받고 있는 것으로 알려졌다.[9)]

2011년 4월에 John Kenny 의원과 John McCain 의원이 상거래 프라이버시 권리헌장 법안(Commercial Privacy Bill of Right of Act, S.799)을 상원 상무 · 과학 · 교통위원회에서 발의하였다. 동 법안은 FTC 산하에 개인정보의 포괄적인 보호를 위한 규제 프레임워크를 확립하는 것으

9) Mozilla의 Alex Fowler에 따르면 Do-Not-Track을 최초로 수용한 브라우저인 Firefox4 이용자의 1-2%만 Do-Not-Track을 작동하고 있는 것으로 알려졌다. Do-Not-Track은 웹 서핑을 하는 동안 타인이 자신을 추적하는 것을 쉽게 봉쇄할 수 있는 수단이지만, 이는 광고자가 이용자의 요청을 수용하는 경우에만 작동하며 아직 이러한 광고자는 소수이다. 또한 삭제된 쿠키를 복원할 수 있는 플래시 쿠키는 Do-Not-Track을 무용지물로 만들 수 있는 것으로 알려져 있다(pii 2011 conference).

로, 보안과 책임에 관한 권리, 통지권 및 개인의 참여권, 데이터 최소수집과 정보유통의 제한 및 데이터 무결성에 관한 권리 및 집행, 협력적 규제 세이프하버(safe harbor) 프로그램,[10] 기타 연방 법률들의 적용, 상무부에 의한 상거래 데이터 프라이버시 정책의 개발 등 전체 7장으로 구성되어 있다.

법안 적용대상은 5,000명 이상의 개인정보를 12개월 동안 연속으로 수집 · 이용 · 전송 · 보관하는 일반통신사업자 및 비영리 단체이며, 보호대상 정보는 성명, 주소, 사회보장번호, 신용카드번호, 지문과 같은 생체정보 등 식별개인정보와 쿠키에 포함된 고객번호, 이용자 ID, 프로세서 또는 장치 일련번호 등 고유식별정보로 하고 있다. 서비스 제공 또는 사기 방지를 위하여 필요한 정보만 수집 가능하며, 서비스 제공에 필요한 기간 동안만 보관이 가능하도록 한다. 개인이 통지를 받지 않았거나 사용에 동의하지 않은 경우 제3자에 의한 식별개인정보의 비인가 사용을 금지한다. 그리고 동 법안은 고의 또는 상습적으로 법을 위반하는 경우에 위반한 일수마다 일별 16,000달러를 민사벌금으로 부과하도록 규정하고 있다.[11]

미국은 (인터넷 이용자의 웹경로 정보 등) 개인정보 보호범위에 대해서, 그리고 정보주체의 동의 방식에 관해서 어느 범위까지 사전동의 방식을 적용할 것인지 등에 대해서는 아직 논쟁 중인 가운데, 이용자가 개인정보 관련 침해 이슈에 대응할 수 있도록 하기 위하여 현행 법률의 적용범위를 확대하고 처벌규정을 강화하는 방식으로 대응하고 있다.

2) EU

EU는 개인정보보호를 자연인의 기본적 권리와 자유로 인식하며 인권보호법으로 분류하고 있다. EU의 개인정보보호 감독기구인 유럽데이터보호감시국(EDPS: European Data Protection Supervisor)은 EU의 개인정보보호법의 근거로 1995년 개인정보보호지침과 2002년 정보통신분야 개인정보보지침 외에, EU설립조약(EU Treaty) 제6조, 유럽공동체조약(EC Treaty) 제286조, EU 기본권 헌장(Charter of Fundamental Rights of the EU) 제8조를 들고 있다. EU설립조약 제6조는 EU가 자유, 인권, 민주주의, 법의 지배 등의 원칙 위에 건립된 것이며, 따라서 EU는 1950년 유럽인권협약이 보장하고 있는 기본적 권리를 존중해야 한다고 규정하고 있다. 한편 유럽공동체조약 제286조과 EU 기본권 헌장 제8조는 개인정보처리에 대한 개인의 자기결정권을 선언하면서 개인정보보호와 관련하여 EU가 채택한 법률원칙들은 유럽공동체 내의 조직과 기관에게도 그대로 적용되어야 한다고 규정하고 있다.

EU가 개인정보보호정책을 인권보호 차원에서 출발하였다는 것은 매우 의미 있고 흥미로운 일

10) 미국과 EU 간에 맺은 식별개인정보(PII)의 전송에 관한 협정으로 2000년부터 시행되었다. 공정정보규정(FIP)에 근거하여 미국 상무성의 세이프하버에 등록하고 이를 준수하는 기업들은 EU에서 미국으로 전송되는 식별개인정보에 대해 적절한 보호 조치를 취한 것으로 간주된다. 협정 내용에는 고지, 선택, 접근, 제3자 전송, 보안, 데이터 무결성 및 법률 시행 등 7개의 원칙이 있다.

11) The Library of Congress(2011.4.12). "S.799-Commercial Privacy Bill of Right Act of 2011".

이다. 이것은 두 가지 의미를 내포하는 것으로 해석할 수 있다. 하나는 개인정보의 처리와 관련된 개인의 권리를 기본권(fundamental rights)으로 봄으로써 개인정보보호의 중요성을 강조하려고 한 것이다. 다른 하나는 당해 개인정보의 처리가 자연인의 기본적 권리 및 자유를 침해하거나 프라이버시를 침해할 정도로 심각한 것이 아니면 개인정보보호를 이유로 개인정보의 처리를 금지하거나 제한해서는 안 된다는 의미를 포함하고 있다. 이 두 가지 목적은 상호 모순적인 것처럼 보이나 개인정보의 보호와 이용의 조화를 의미하는 것으로서 상호 보완적으로 이해하지 않으면 안 된다. EU 개인정보보호법의 이같은 취지는 1995년 개인정보보호지침 서문에도 잘 나타나 있다.

개인정보보호지침(EU Directive on Privacy Protection, 1995/46/EC, 1995. 10. 24)은 개인정보의 처리 및 자유로운 이동에 관한 지침이다. 개인정보보호지침은 단순히 원칙을 선언하는 것에 그치지 않고 구체적으로 개인정보의 처리기준, 처리방법, 처리절차, 정보주체의 권리, 피해구제, 관리 · 감독의무, 국외 이전제한 등을 상세히 규정하고 있다. 이 지침을 통하여 회원국에게 개인의 기본 권리로서 개인정보보호 책임을 부과하고 궁극적으로 개인에게 개인정보보호 권리를 보장하고자 하는 목적으로 제정되었다.

동 지침은 EU 회원국과 업무를 하는 비회원국들에도 적용된다. 또한 이 지침은 민간부문은 물론 공공부문에도 적용된다. 즉 EU는 개인정보의 수집 · 처리와 관련하여 민간부문과 공공부문을 특별히 차별하지 않고 있다. 전체적 또는 부분적으로 자동처리수단에 의해서 처리되는 개인정보를 보호 대상으로 하지만, 수동으로 처리되는 개인정보라도 파일링 시스템의 일부를 구성하거나 구성할 의도로 수집 · 처리되는 개인정보는 보호의 대상이다. 특히 개인정보의 수집 및 보유와 관련하여 공정하고 정확하게 처리할 것, 구체적이고 합법적인 목적을 위해서만 자료를 수집하고 명시된 목적을 위해서만 사용할 것, 수집 및 처리되는 개인정보의 목적에 적절하고 연계된 사항에 대해서만 다룰 것, 데이터를 정확하게 유지하고 필요한 경우 갱신할 것, 필요한 경우 정보주체 식별이 가능한 형태로 유지할 것 등의 요구조건을 만족시켜야 한다. 동 지침은 개인정보 처리자에게 개인정보 보호를 위한 기술적 · 조직적 조치 의무를 부과하는 한편, 개인정보가 EU 수준으로 적절하게 보호되고 있지 않는 나라로의 개인정보 이전을 금지하고 있다. 이 지침은 EU 회원국은 물론 제3국의 개인정보 정책과 법제에도 큰 영향을 미치고 있다.

EU는 위치정보와 관련하여 2002년에 '전자통신부문에서 개인정보처리와 프라이버시 보호에 관한 지침(Directive 2002/58 on Privacy and Electronic Communications; 이하 "ePrivacy 지침"이라 함)'을 별도로 제정하였다. 위치정보를 공중 전자통신서비스 이용자의 단말장치의 지리적 위치를 표시하는 전자통신망 내에서 처리되는 정보로 정의하고 위치정보 이용 시에 이용자의 사전 동의, 이용자의 일시적인 수집 거부권 및 위치정보 처리사업자의 자격 등을 규정하고 있다. 이후 2009년 개정을 통하여 쿠키에 대한 규정을 신설하였다. 쿠키 정보를 수집 · 처리하는 사업자는 이용자에게 쿠키의 이용 목적을 알기 쉽게 설명하고 이용자의 사전 동의가 있어야만 쿠키 정보를 사용할 수 있으며 쿠키 등을 거부하는 기회를 이용자에게 알기 쉬운 형태로 제공하도록 규정하고

있다. 2011년 5월 재개정을 통하여 사업자는 쿠키를 저장하기 전에 이용자에게 명백한 동의가 필요함을 강조하고 관련 조치들을 강화하였다. 대부분의 EU 국가들이 명백한 동의를 어떻게 정의할 것인가에 대해 혼란해 하고 있는 가운데, 유럽연합집행기관(European Commission)은 새로운 규칙에 적용하지 못한 국가들에 대해서 법적 행동을 시작하였다.

3) 일본

일본에서는 1975년에 동경의 쿠니타찌시(國立市)가 컴퓨터 도입과 관련하여 '전자계산기조직의운영에관한 조례'를 제정한 것을 효시로 하여 지자체 조례를 중심으로 개인정보보호 체계가 구축되기 시작하였다. 국가차원에서는 OECD가 1980년에 발표한 프라이버시 보호와 국가간 개인정보의 자유로운 이동을 보장하기 위한 가이드라인(OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data)을 계기로, 1988년에 '행정기관이보유한전자계산기처리에관한개인정보의보호에관한법률'을 공포하여 공적부분에서의 개인정보보호체계를 정비하였다. 이러한 공적부분과는 달리 민간부분에 적용되는 개인정보 관련법이 없어 민간부분의 개인정보는 프라이버시 마크제도와 같은 자율규제나 정부 가이드라인 등에 의해 보호되었다.

그러나 일본에서 대내적인 정보사회의 급속한 진전과 대외적인 국제적 정보유통의 확대 및 디지털화로 인해 정보사회의 역기능, 즉 프라이버시 등 개인 권리이익의 침해 가능성과 불안감이 증대되었으며, 개인정보의 보호와 이용의 조화를 목적으로 하여 민간 및 공적부분의 개인정보보호 법제를 확립하고자 하였다. 이에 따라 '개인정보의보호에관한법률'(이하 개인정보보호법) 등 5개 개인정보보호 관련 법률이 2003년 5월 참의원 본회의에서 가결되고 2005년 4월 전면적으로 시행되었다.

개인정보보호법은 개인정보의 적정한 취급과 관련한 사항을 규정하여 개인정보의 유용성을 배려하면서도 개인의 권리이익을 보호하는 것을 목적으로 명시하고 있다. 개인정보를 생존하는 개인에 대한 정보로서 당해 정보에 포함되어 있는 성명, 생년월일, 그 밖의 기술 등에 의하여 특정 개인을 식별할 수 있는 것(다른 정보와 용이하게 대조할 수 있고, 그로써 특정 개인을 식별할 수 있도록 되어 있는 것을 포함)으로 정의하고 있다. 그리고 개인정보 데이터베이스 등을 구성하는 개인정보를 개인데이터라고 별도로 정의하고 있다. 개인정보 데이터베이스 등은 개인정보를 포함한 정보의 집합물로서 특정 개인정보를 전자계산기를 이용하여 검색할 수 있도록 체계적으로 구성한 것과 그 외에 특정 개인정보를 용이하게 검색할 수 있도록 체계적으로 구성한 것으로 시행령(政令)으로 정하도록 하였다. 그리고 개인정보취급사업자가 열람, 내용의 정정, 추가, 삭제, 이용의 정지, 소거 및 제3자 제공의 정지를 행할 수 있는 권한을 가지는 개인데이터를 보유개인데이터라고 하여 별도로 규정하고 있으며, 개인정보 취급사업자를 개인정보 데이터베이스 등을 사업용으로 이용하고 있는 자로 규정하고 있다.

일본은 유럽의 통합법 체계와 미국의 민간자율규제 형식인 세이프하버 원칙의 중간적 입장에서

법체계를 시도하였으며, EU의 개인정보보호 강화 요구를 수용하면서도 유럽과 같이 독립 개인정보보호 감독기구를 두지 않고 고충처리를 수행하는 민간개인정보보호단체를 지정하고 있다.

행태기반 온라인광고와 관련하여 정부차원에서는 총무성을 중심으로 경제효과와 이용자 보호 관점의 균형에 대해서 논의는 되고 있으나, 개인정보보호를 위한 명확한 제도 혹은 정책은 제시되고 있지 않다. 다만, 2009년 6월에 일본인터넷광고추진협의회(JIAA)는 웹사이트에서 인터넷 이용자의 행태정보를 수집하고 그 정보를 이용하여 광고를 표시하는 행태정보 기반 온라인 광고에 관하여 광고전송사업자나 매체사[12]가 제시해야 할 내용을 정하기 위한 '행태정보 기반 온라인광고 가이드라인'을 제시하였다.

동 가이드라인에서는 행태정보를 행동이력정보라고 하는데 이는 웹사이트의 열람이력이나 전자상거래사이트 상에서의 구매이력 등을 축적한 후 이용자의 흥미 · 기호를 분석하여 제공할 수 있는 정보로서 특정한 개인을 식별하지는 않는다. 또한 행태정보 기반 온라인광고를 '행동타켓팅 광고'라고 하고 이는 행태정보로부터 이용자의 흥미 · 기호를 분석하고 이용자를 소집단으로 분류하여 소집단마다 온라인 광고를 하는 서비스로서, 행태정보의 축적을 수반하는 것으로 규정하였다. 그리고 행태정보의 취급과 관련하여 개인정보의 수집 · 이용에 대한 투명성의 확보, 이용자 관여 기회의 확보, 적정한 수단에 의한 취득의 확보, 적절한 안전관리의 확보, 교육, 불평 · 질문 대응체제의 확보를 원칙으로 제시하였다.

4) 한국

2011년 3월에 '개인정보보호법'이 제정되기 이전에 우리나라 개인정보보호 관련 법제는 크게 공공부문과 민간부문으로 나뉘어 규율되었다. 공공부문의 개인정보보호에 관한 사항은 주로 공공행정분야와 관련된 것으로, '공공기관의 개인정보 보호에 관한 법률'에서 다루어졌다. 동 법은 공공기관에서 처리되는 각종의 개인정보의 보호를 위하여 그 수집 · 처리 · 열람 · 정정 등 제반 취급에 관하여 필요한 사항을 정함으로써 공공업무의 적정한 수행을 도모함과 아울러 국민의 권리와 이익을 보호함을 목적으로 한다. 그 외에도 '공공기관의 정보공개에 관한 법률', '전자정부법', '주민등록법', '가족관계 등록 등에 관한 법률', '국정감사 및 조사에 관한 법률', '통계법' 등에서도 개인정보 보호의무를 적용하고 있다.

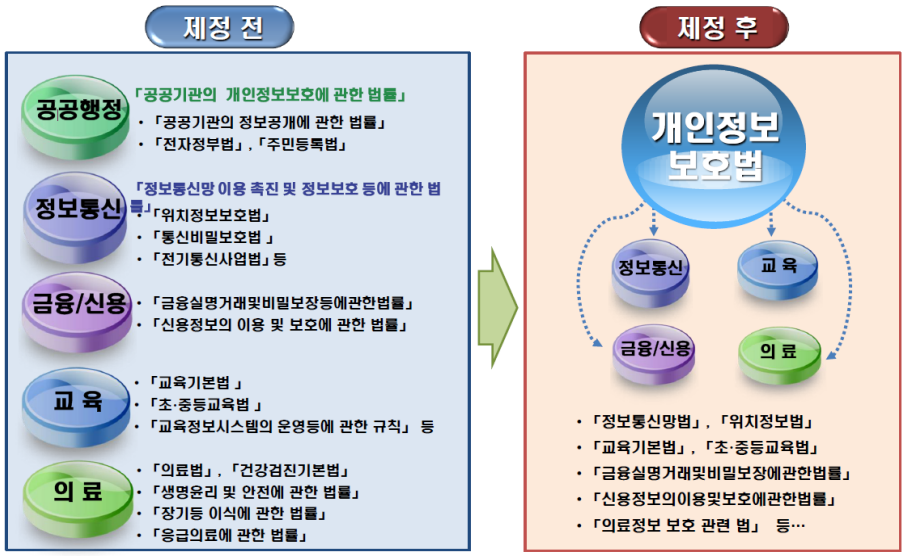
한편, 민간부문의 개인정보보호에 관한 사항은 정보통신, 금융 · 신용, 의료, 교육 등의 분야에서 각각의 개별법 내에 개인정보 보호의무가 담겨 있다. 그 가운데 정보 · 통신 분야에서는 '정보통신망이용촉진 및 정보보호 등에 관한 법률'에서 주로 다루어졌다. 동 법은 정보통신서비스 제공자에 대한 개인정보 수집 · 이용 및 제공, 개인정보의 관리 및 파기에 관한 사항을 규율하고, 개인정보보호와 관련된 정보통신서비스 이용자의 권리, 개인정보와 관련된 분쟁을 신속하고 저렴하게

12) 행태정보 기반 온라인광고를 게재하는 웹사이트를 개설하는 사업자를 말한다.

해결하기 위한 개인정보분쟁조정위원회와 조정절차 등에 관한 사항을 규정하고 있다. 그 외에도 '통신비밀보호법', '위치정보의 보호 및 이용 등에 관한 법률', '국가정보화기본법', '정보통신기반보호법', '신용정보의 이용 및 보호에 관한 법률', '보건의료기본법', '교육기본법' 등에서 개인정보보호의무를 적용하고 있다.

<그림 1>의 왼편에 정리되어 있는 바와 같이, '개인정보보호법' 이전의 개인정보보호 관련 법체계는 다양한 개별분야의 특수성을 반영한 규정들이 특별법적 성격의 법률들 내에 규율되고 있었다.

<그림 1> 개인정보보호 관련 법체계 변화



자료: 개인정보보호 종합지원 포털(http://www.privacy.go.kr).

'개인정보보호법'을 제정하면서 개인정보보호 관련 법제는 '개인정보보호법'을 중심으로 일원화하였다.[13] '개인정보보호법'은 개인정보의 수집 · 처리에 관한 일반법으로 모든 분야의 개인정보

13) '개인정보보호법'의 구성은 본문 9장, 75개조와 부칙으로 되어 있으며, 제1장 총칙, 제2장 개인정보보호정책의 수립 등, 제3장 개인정보의 처리, 제4장 개인정보의 안전한 관리, 제5장 정보주체의 권리 보장, 제6장 개인정보분쟁조정위원회, 제7장 개인정보 단체소송, 제8장 보칙, 제9장 벌칙으로 이루어져 있다. 동 법은 OECD 가이드라인에 맞추어 개인정보 보호원칙을 확립하였다. ① (수집제한의 원칙) 목적에 필요한 최소한 범위 안에서 적법하고 정당하게 수집, ② (정보정확성의 원칙) 처리목적 범위 안에서 정확성 · 안전성 · 최신성 보장, ③ (목적명확화 원칙) 처리목적의 명확화, ④ (이용제한의 원칙) 필요 목적 범위 안에서 적법하게 처리, 목적 외 활용 금지, ⑤ (안전보호의 원칙) 정보주체의 권리침해 위험성 등을 고려, 안전성 확보, ⑥ (공개의 원칙) 개인정보 처리사항 공개, ⑦ (개인참가의 원칙) 열람청구권 등 정보주체의 권리 보장, ⑧ (책임의 원칙) 개인정보처리자의 책임 준수·실천, 신뢰성 확보 노력.

처리에 적용된다. '개인정보보호법'을 제정하면서 개인정보의 수집·처리에 관한 원칙을 통일하고 중복규제를 제거하기 위해 개인정보와 관련된 개별법을 모두 폐지하는 것도 고려하였으나, 모든 개별법을 일시에 폐지하는 경우에 관련 산업에 혼란이 야기될 우려와 이 법보다 특별히 보호수준을 높이거나 낮추어야 할 경우가 존재하여 '공공기관의 개인정보보호에 관한 법률'만 폐지하고 다른 법률에 특별한 규정이 있는 경우에는 해당 개별법을 우선 적용하도록 예외를 인정하고 있다.

'개인정보보호법'과 개별법과의 관계를 살펴보면, 다음과 같다. 먼저, 공공행정분야 개인정보, 교육분야 개인정보, 의료분야 개인정보 등은 '전자정부법', '교육기본법', '의료법' 등이 우선 적용되고 보충적으로 '개인정보보호법'이 적용되어 그 보호수준이 강화될 것으로 예상된다.

그러나 금융 · 신용분야 개인정보는 다른 분야보다 먼저 체계화된 입법체계를 가지고 있어서 '개인정보보호법'은 보충적 역할을 수행할 것으로 보인다. '신용정보의 이용 및 보호에 관한 법률' 등 관련법에 신용정보의 수집 · 조사 및 처리의 제한, 신용정보 제공 및 이용의 제한, 신용정보 의무 및 보관, 신용정보주체의 권리 등이 잘 규정되어 있다(현대호, 2011: 41).

정보통신분야 개인정보는 '개인정보보호법'과 '정보통신망 이용촉진 및 정보보호 등에 관한 법률'(이하 '정보통신망법')은 상호보완적인 관계가 될 것으로 보인다. 이들은 개인정보의 수집·이용·제공, 정보주체의 권리에 대하여 유사하게 규율하고 있지만, 적용대상이나 개인정보처리자의 의무 등에 있어서 차이를 보이고 있다. '개인정보보호법'과 '정보통신망법'의 차이를 살펴보면, 다음과 같다.

첫째, 규율 대상과 관련하여 '개인정보보호법'의 개인정보처리자는 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등을 말한다(개인정보보호법 제2조 제5호). '정보통신망법'의 정보통신서비스 제공자는 '전기통신사업법' 제2조 제8호에 따른 전기통신사업자와 영리를 목적으로 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자를 말한다(정보통신망법 제2조 제3호). 즉, '정보통신망법'은 영리를 목적으로 하는 정보통신서비스 제공자를 적용대상으로 한정하며, 정보통신망을 이용한 공공영역의 서비스 등에는 그 적용을 제한하고 있다.

둘째, 개인정보 수집과 관련하여 '개인정보보호법'의 개인정보처리자가 개인정보를 수집하는 경우에 그 목적에 필요한 최소한의 개인정보를 수집하여야 하며, 최소한의 개인정보 수집이라는 입증책임을 개인정보처리자가 부담토록 하고 있다(개인정보보호법 제16조 제1항). 하지만, '정보통신망법'에서는 최소한의 개인정보 수집에 대한 별도의 언급이 이루어지고 있지 않다.

셋째, 개인정보의 처리 정지와 관련하여 '개인정보보호법'은 그 적용에 있어서 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우, 다른 사람의 생명 · 신체를 해할 우려가 있거나 다른 사람의 재산과 그 밖의 이익을 부당하게 침해할 우려가 있는 경우, 공공기관이 개인정보를 처리하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우, 개인정보를 처리하지 아니하면 정보주체와 약정한 서비스를 제공하지 못하는 등 계약의 이행이 곤란한 경

우로서 정보주체가 그 계약의 해지 의사를 명확하게 밝히지 아니한 경우 등(개인정보보호법 제37조 제2항) 폭넓은 예외를 규정하고 있다. 이로 인하여 실질적으로 개인정보 처리 정지가 이루어지는 것은 드물거나 혹은 열거하는 사항의 해석에 따라서는 상이한 결과를 초래할 여지도 있다(현대호, 2011: 27).

한편 '정보통신망법'에서는 이용자에게 정보통신서비스 제공자등에 대하여 언제든지 개인정보 수집 · 이용 · 제공 등의 동의를 철회할 수 있으며, 철회하는 경우에 정보통신서비스제공자는 파기 등의 조치를 하도록 규정하고 있다(정보통신망법 제30조 제1항).

'개인정보보호법'과 '정보통신망법' 간의 법률관계가 상호 우선 적용 규정을 두고 있어서 보충적인 지위에서 적용될 수 있다. '개인정보보호법'은 제6조에서 '정보통신망 이용촉진 및 정보보호 등에 관한 법률', '신용정보의 이용 및 보호에 관한 법률' 등 다른 법률에 특별한 규정이 있는 경우에는 이들 법률을 적용하고 해당 법률에서 특별한 규정이 없는 경우에는 일반법적인 지위에서 '개인정보보호법'을 적용하는 것으로 규정하고 있다. 한편 '정보통신망법'은 제5조에서 정보통신망 이용촉진 및 정보보호 등에 관하여는 다른 법률에서 특별히 규정된 경우 외에는 '정보통신망법'이 정하는 바에 따른다고 규정하고 있다.

5. 대안적 정책과 전략

1) Better Choices: Better Deals

소비자들의 개인정보 문제에 대해서 영국 정부는 새로운 법이나 규제에 의한 대응방식이 아닌 기업들과 소비자 단체 그리고 규제기관이 동반자적 관계를 형성하여 다양한 프로그램을 수행하는 전략을 추진하고 있다. 이 전략은 'Better Choices: Better Deals'라는 영국정부의 문서에 소개되어 있는데 이러한 전략적 변화는 크게 세 가지로 요약된다.[14] 첫째는 소비자로 하여금 재화와 서비스를 찾아내어 비교하고 구매하는 새로운 채널들을 창출하는 신기술들, 특히 인터넷과 모바일 폰 앱들의 역할 증가이다. 둘째는 기업들이 소비자를 더 잘 이해하고 맞춤형 조언을 해줄 수 있게 소비자의 거래 기록으로부터 발생하는 데이터의 활용이다. 셋째는 소비자들이 경제 전체의 차원에서 협력할 수 있는 새로운 방법의 개발이다.

영국 정부는 이러한 전략적 변화에 따라 소비자에게 더 많은 권한을 부여하여 그들이 공급자를 선택하고 개인적으로 또는 단체로 가장 좋은 거래를 성사시키고, 기업들에게 압력을 가해서 더 효율적이고 혁신적인 기업이 되도록 한다. 궁극적으로는 다음과 같은 두 개의 근본적인 변화를 기대하고 있다. 첫째는 특정 기업들이 소비자에 대한 정보를 배타적으로 관리하는 상태에서 개인 또는

14) 자세한 내용은 Better Coices: Better Deals, Department of Business Innovation & Skills, UK, 2011을 참조.

집단이 자신들의 정보를 사용할 수 있고 자기 자신의 또는 상호간 혜택을 위해 피드백을 줄 수 있는 상태로의 전환이다. 둘째는 소비자들이 어떤 식으로든 피해를 입은 다음 정부기관이 규제를 가하는 방식에서 개인 또는 집단이 기업에게 올바른 시그널을 보내어 소비자가 원하는 제품과 서비스를 확보하는 방식으로의 전환이다. 이러한 방식은 정직하고 고 품질의 기업에게 경쟁력을 부여할 것이고 혁신과 성장을 촉진할 것으로 기대되고 있다.

영국 정부는 이를 위해 다양한 프로그램들을 추진하고 있다. 그 주요 내용은 다음과 같다. 'mydata'라는 프로그램은 기업들이 가지고 있는 소비자 정보를 소비자들이 접근하고 관리하고 사용할 수 있게 하는 프로그램이다. 이를 위해 영국 정부는 금융, 유통, 전력, 통신 등의 분야에 있는 20개의 선도적 기업들과 이 프로그램에 협력하기로 협약을 맺었다.

우선 기업들이 보유하고 있는 소비자의 구매 및 라이프스타일과 관련된 적합하고도 풍부한 정보를 제공하여 현명한 선택을 하도록 한다. 예를 들면, 소비자는 최근 12개월 동안 자신의 이동통신 사용 데이터로부터 가장 유리한 요금제를 알 수도 있고, 수퍼마켓으로부터 구입하는 음식의 평균 지방량을 알 수도 있으며 돈을 절약하는 방법이나 신용카드를 사용하는 가장 좋은 방법 등도 알 수 있게 된다.

소비자들의 공동 구매, 공동 소비를 지원하여 소비자들이 집단의 위력을 통하여 더 유리한 거래를 성사시킬 수 있도록 한다. 이를 위해서 공공부문의 비교 사이트를 지원하고 민간부문에 소비자 피드백 사이트의 활성화를 지원한다. 필요시 규제기관이 보유하고 있는 데이터도 활용한다.

소비자 피드백과 온라인 비교 사이트의 무결성을 보장하기 위한 새로운 조치들을 도입한다. 예를 들면 비교 사이트를 위한 자율규제적 품질마크의 개발을 지원하고 그릇된 피드백을 생산하는 기업들을 적발한다.

거래 이후 소비자 피해를 구제하기 위해 법제 시스템 밖에서 편리하게 소비자들이 이용할 수 있는 분쟁해결 방법을 마련한다. 또한 가게 안에서도 다른 소비자들의 피드백에 접속할 수 있는 방법을 개발하여 오프라인 상태에서도 다른 소비자의 의견으로부터 도움을 얻을 수 있도록 한다.

이상에서 살펴 본 Better Choices: Better Deals의 내용에는 온라인 광고와 직접적인 관련이 있는 사항은 없지만, 프라이버시 문제에 대한 규제자로서의 정부 역할에서 탈피하여 소비자와 기업의 상생을 도모하는 조율자로서의 새로운 역할을 제시하고 있다는 점에서 온라인 광고 분야에 시사하는 바도 있다. 광고업체가 소비자의 행위 정보를 수집하는 과정이 투명해지고 가공된 정보의 사용 용도가 소비자에게 도움을 줄 수 있다면, 게다가 소비자에게 자신의 정보에 대한 주권행사를 보장한다면 소비자들은 광고 목적의 정보수집에 따른 프라이버시 침해에 대한 염려가 줄어들 수 있을 것이다.

2) 기타

영국 정부의 Better Choices: Better Deals 전략을 자문했던 시카고 경영대학원에 Richard

Thaler 교수는 2011년 4월 New York Times의 한 칼럼에서 프라이버시 보호의 차원을 넘어 기업이 활용하고 있는 소비자의 개인정보를 소비자 자신도 기업에게 그 정보를 제공할 것을 요구하여 이를 적극적으로 활용함으로써 그 혜택을 함께 누리자고 제안하였다. 또한 소비자들이 기업으로부터 자신에 대한 정보를 취득하게 되면 이를 활용하기 위한 스마트폰 앱들이 개발되어 앱 개발자들에게도 도움이 될 것이라고 주장하였다.

한편 프라이버시 보호를 새로운 서비스 산업으로 발전시키고자 하는 노력이 실리콘밸리를 중심으로 추진되고 있다. pii 2011 컨퍼런스에서는 Personal이라는 벤처기업이 주목을 받았는데 Personal은 개인의 데이터를 소유하고 관리하고 그로부터 발생하는 혜택을 누리게 해주는 플랫폼을 개발하였다. 인터넷에서 수많은 행위 추적이 이루어지고 있는 현실에서 프라이버시 보호를 국가가 법제도에 의해 보장하는 데는 한계가 있으므로 프라이버시 보호를 하나의 서비스로 개발하여 새로운 시장을 창출하자는 움직임이 최근 관련 업계에서 활발해지고 있다.

6. 주요 쟁점사항과 정책방향

1) 비식별개인정보

'개인정보보호법'과 '정보통신망법' 상의 개인정보는 생존하는 개인에 관한 정보로서 성명, 주민등록번호 등에 의하여 특정한 개인을 알아볼 수 있는 부호 · 문자 · 음성 · 음향 및 영상 등의 정보(해당 정보만으로는 특정 개인을 알아볼 수 없어도 다른 정보와 쉽게 결합하여 알아볼 수 있는 경우에는 그 정보를 포함한다)로 규정하고 있다(개인정보보호법 제2조 제1호, 정보통신망법 제2조 제6호). 즉, 비식별개인정보가 식별개인정보와 결합되지 않은 상태에서 특정 개인을 식별함이 없이 익명화되어 처리되고 있는 경우에는 현행법상 개인정보에 해당하지 않는다고 보는 것이 타당하다(정상조 외, 2010: 109).

그러나 최근에는 웹경로정보, 성향정보, 위치정보 등 다양한 형태의 비식별개인정보가 수집되고 있으며, 비식별개인정보는 그 자체로, 혹은 비식별개인정보와 비식별개인정보의 결합, 식별개인정보와의 결합 등을 통하여 개인을 유추할 수 있는 가능성이 점점 높아져가고 있다. 개인의 일련의 행태를 모두 추적 · 파악할 수 있는 위치정보 또는 이용자의 관계망과 관련된 정보, 개별 사이트에서 수집된 행태정보들의 연계, 회원의 로그아웃 상태의 웹경로 등 다양한 형태로 개인을 파악할 수 있다.

그렇다고 개인 노출과 프라이버시 침해의 가능성만으로 비식별개인정보까지 개인정보 보호 범위 내에 두는 것은 인터넷 서비스와 온라인광고의 활성화에 장애가 될 가능성이 높다. 따라서 비식별개인정보들이 무엇이 있으며 어떠한 문제점이 있는지에 대한 분석을 통하여 이용자들이 어떤 비식별개인정보가 수집 · 처리되고 있는가를 확인할 수 있고, 비식별개인정보라도 개인 유추 가능

성이 높은 비식별개인정보 등은 개인정보처리자가 이용자의 동의를 받을 시에 알려야 하는 '수집하려는 개인정보의 항목'에 포함될 수 있도록 하여야 한다.

2) 포괄적 동의

'개인정보보호법'과 '정보통신망법'에서는 이용자의 개인정보를 수집하는 경우에는 개인정보의 수집 · 이용 목적, 수집하는 개인정보의 항목, 개인정보의 보유 · 이용 기간 등을 이용자에게 알리고 동의를 받도록 하고 있다(개인정보보호법 제15조, 정보통신망법 제22조). 또한 제3자에게 개인정보를 제공하는 경우에도 개인정보를 제공받는 자, 개인정보를 제공받는 자의 개인정보 이용 목적, 제공하는 개인정보의 항목, 개인정보를 제공받는 자의 개인정보 보유 및 이용기간 등을 이용자에게 알리고 동의를 받도록 하고 있다(개인정보보호법 제17조, 정보통신망법 제24조의2).

현실적으로 대부분의 인터넷 서비스 업체들은 이용자가 서비스에 가입할 때 이용자에 관한 향후의 모든 정보 수집과 활용, 심지어 제3자에게 제공에 대해 포괄적인 동의를 요구하고 있다. 이와 같은 포괄적 동의는 이용자 동의와 관련된 위의 법조항에서 요구하는 수집 · 이용 목적, 개인정보의 항목, 보유 · 이용 기간 등을 무시할 수밖에 없어 법이 요구하는 동의 수준에 크게 못 미치고 있다.

위의 법조항을 엄밀히 해석하자면 서비스 업체들은 이용자의 정보수집 행위가 발생할 때마다 이용자에게 수집 · 이용 목적, 개인정보의 항목, 보유 · 이용 기간 등을 알리고 동의를 받아야 한다. 왜냐하면 수집하고자 하는 정보에 따라 이용 목적이나 이용기간이 달라질 수 있기 때문이다. 그러나 이처럼 엄격하게 위의 조항을 적용하면 서비스 자체가 불가능한 경우도 발생한다. 예를 들면 위치기반 서비스의 경우 한 시간에도 몇 번씩 이용자의 위치정보를 수집해야 하는 서비스들이 있다. 만일 그 때마다 이용자의 동의를 구한다면 서비스의 실시간성이 보장되지 않아 서비스 품질이 저하되고 이용자도 잦은 동의 요청에 불편함을 느끼게 되어 사실상 서비스 제공이 불가능하게 된다. 따라서 이러한 경우에는 위의 법조항을 융통성 있게 해석하여 포괄적 동의를 허용하는 것이 바람직하다.

이상의 논의를 정리하면 다음과 같다. 지금까지 관행처럼 행해진 포괄적 동의는 위의 법조항의 요구사항을 충족하지 못하는 것으로 판단되므로 시정되어야 한다. 그러나 포괄적 동의가 아니면 서비스 제공 자체가 불가능하고 각각의 정보수집 행위가 발생할 때 수집 · 이용 목적, 개인정보의 항목, 보유 · 이용 기간 등이 거의 동일하다면 예외적으로 포괄적 동의를 허용할 필요가 있다.

3) 쿠키에 의한 정보수집

'정보통신망법' 상에 정보통신서비스의 제공에 관한 계약을 이행하기 위하여 필요한 개인정보로서 경제적 · 기술적인 사유로 통상적인 동의를 받는 것이 뚜렷하게 곤란한 경우는 동의 없이 이용자의 개인정보를 수집·이용할 수 있도록 되어 있다(정보통신망법 제22조 제2항 제1호). 즉, 이용

자가 정보통신서비스를 이용하는 과정에서 생성되는 서비스 이용기록, 접속 로그, 쿠키, 결제 기록, 이용정지 기록, 페이지뷰 내역, 이용시간대, 검색사항, 사이트 방문 내역 등은 이용자의 동의 없이 수집할 수 있는 것을 의미한다(정상조 외, 2010: 113).

최근의 쿠키는 사이트 접속을 용이하게 하는 정보만을 담고 있는 것이 아니라, 이용자 행태를 모니터링할 수 있는 소지가 충분한 쿠키들이 생성되고 있다. 이에 EU의 *e*Privacy 지침에서는 사이트 접속과 관련되지 않는 쿠키에 대해서는 이용자의 사전 동의를 구하도록 하고 쿠키 거부를 이용자가 알기 쉽게 처리할 수 있도록 해야 한다고 규정하였다.

그러나 이 규정의 실효성에 대해서는 회의적이다. 앞에서 언급한 바와 같이 현실적으로 수많은 쿠키들이 존재하고 그 중 다수는 웹사이트 운영주체도 그 존재를 파악하지 못하고 있는 불법적인 쿠키들이다. EU의 사전 동의 규정은 이와 같은 불법적인 쿠키들에 대해서는 아무런 의미를 갖지 못한다. 또한 수퍼쿠키의 등장 등 쿠키기술의 발전은 지속적으로 쿠키 거부를 무력화시킬 것이다.

쿠키에 대한 문제는 법제도적으로 해결할 수 있는 문제는 아니고 어쩌면 어떤 방법으로도 해결이 불가능한 문제일 수도 있다. 우선 이용자들이 쿠키에 대한 인식을 명확히 가져야 한다. 즉 온라인상에 얼마나 많은 쿠키들이 존재하는지 그리고 자신의 개인정보가 쿠키들에게 얼마나 노출될 수 있는지에 대해 구체적으로 인지할 수 있는 기회를 제공할 필요가 있다. 이용자들은 쿠키에 대한 인지와 프라이버시 침해 위험성을 바탕으로 어떤 서비스들을 얼마나 이용할 것인지를 스스로 선택할 수 있다. 정부는 이용자들이 쿠키에 대해 구체적이고 정확한 인지의 기회를 갖도록 지원하는 프로그램을 개발하고 실행할 필요가 있다.

4) 불공정 약관

다음은 어떤 인터넷 서비스업체 ooo가 제공하는 리워드 프로그램과 관련된 약관이다.

> 제 x 조 개인정보 및 인터넷 사용정보 수집과 그 활용
>
> ooo는 사용자가 컴퓨터에서 입력한 키워드를 검색 및 결과표시를 위해서 사용자의 컴퓨터이외로 전송할 수 있으며 ooo는 이 키워드를 상업적 목적으로 사용하거나 제3자에게 익명으로 제공할 수 있습니다.

이 약관 내용은 개인정보보호법 제17조, 정보통신망법 제24조의2를 위배하고 있으나 이와 유사한 약관들은 인터넷 서비스 약관들에서 흔히 발견된다. 그러나 더 큰 문제는 대부분의 이용자들이 약관 내용을 확인하지 않고 동의한다는 것이다. 이와 같이 관련법에 어긋나는 약관들은 시정되어야 하는 것이 원칙이지만 현실적으로 관계당국이 인터넷에 존재하는 수많은 약관들을 검토하여 시정명령을 내리는 것은 불가능하다고 본다. 일각에서는 약관의 표현들이 일반인이 이해하기 어

렵기 때문에 쉬운 문장으로 바꾸어야 한다고 주장하지만 그것도 이 문제에 대한 근본적인 해결책은 아니라고 본다.

불공정 약관의 문제도 이용자의 인지가 우선되어야 한다. 이용자들이 자신이 자주 이용하는 인터넷 서비스의 약관이 자신의 프라이버시에 어떤 영향을 주는지를 객관적이고 구체적으로 인지할 수 있는 기회가 이용자들에게 주어질 필요가 있다. 예컨대 대표적인 인터넷 서비스 몇 개를 선정하여 그 약관들을 분석하고 프라이버시 영향평가를 실시하여 이용자들에게 알리고 소비자단체들이 본격적으로 문제 제기를 하면서 불공정 약관의 문제에 대한 사회적 공감대가 형성되면 관련 업계의 자정 노력도 기대해 볼 수 있을 것이다.

■ 참고문헌

김일환, "미국 개인정보보호법규에 관한 연구," 미국헌법연구 제10호, 미국헌법학회, 1999.

양지연, "온라인 맞춤형 광고: 개인정보보호와 정보이용의 균형점을 찾아서, 미국 FTC와 EU의 가이드라인에 비추어," LAW & TECHNOLOGY, 제5권 제2호, 2009.

정보통신산업진흥원, 『주간기술동향』 제1519호, 2011.

정상조, "비식별개인정보의 보호 및 활용에 관한 연구," 방송통신정책연구; 10-진흥-라-17, 2010.

현대호, "개인정보보호법과 다른 법률의 개인정보보호 규정과의 정합성 확보," 한국인터넷법학회 춘계공동학술대회 '개인정보보호법 제정에 따른 개인정보보호정책의 방향과 과제' 자료집, 2011.4.15.

Craig, T. and M. E. Ludloff, Privacy and Big Data, O'Reilly, Sebastopol, CA, 2011.

Reidenberg, J. R., "A New Legal Paradigm? Resolving Conflicting International Data Privacy Rules in Cyberspace," 52 Stan. L. Rev, 2000.