유럽과 미국의 정보보호 관련 전담인력 및 법제도 동향

정보신청기관 : 한국인터넷진흥원

Ⅰ. 머리말

최근 수천만 명의 피해자들을 발생시킨 개인정보 유출 및 해킹 사례들이 빈번히 발생하면서 개인정보보호에 대한 인식이 크게 변화하고 있다.[1] 특히 우리나라는 세계 최고의 정보화 수준을 갖춘 만큼 개인정보 침해사고도 심각한 수준이다. 2008년부터 최근까지 개인정보 유출 규모만 보더라도 전체 인구에 해당하는 정보가 2회에 걸쳐 유출된 상태이다. 더욱 심각한 것은 글로벌 네트워크의 활성화로 우리나라 국민의 개인정보가 제3국으로 무단 유출됨으로써 개인정보의 오·남용 및 프라이버시 침해의 위험이 높아졌다. 최근 인도, 중국 등 개발도상국에 정보처리 관련 기업들이 증가하면서 이들 기업을 통한 개인정보의 무단 유통이 문제되고 있다.

이러한 개인정보유출의 문제점을 일찍이 인식한 주요 선진국들은 개인정보와 프라이버시를 보호하기 위한 대책을 마련해 오고 있다. EU는 이미 1995년에 정보보호지침(Data Protection Directive, 95/46/EC)을 마련하였고, 2012년 1월에는 이 지침을 더욱 강화한 「정보보호규정안(General Data Protection Regulation)」을 발표하였다. 또한 독일, 미국, 캐나다, 호주 등 선진국들도 개인정보와 프라이버시 보호를 위한 법제도 개혁안을 잇달아 내놓고 있다.

우리나라는 2011년 3월 29일 「개인정보보호법」[2]을 제정하여 시행하고 있지만 개인정보 침해 방지를 위한 전담조직과 인력이 여전히 부족하다. 특히, 공공기관과 민간 기업 모두 개인정보보호 전담인력의 확보가 시급하며, 대부분 정보화 업무와 정보보호 업무를 구별하지 않고 있다.

1) 2008년부터 2011년 상반기까지 발생된 주요 개인정보 유출사건의 규모를 살펴보면, 옥션(2008.1) 1,863만 명, GS 칼텍스(2008.9) 1,125만 명, 네이버(2009.4) 9만 명, 인천(2010.3) 2,000만 명, 대전(2010.3) 650만명, 부산(2010.4) 1,300만 명, 현대캐피탈(2011.4) 175만 명, SK컴즈, 네이트(2011.7) 3,500만 명, 한국 앱손(2011.8) 35만 명 등 무려 총 1억 657만 명에 대한 개인정보가 유출되었다. 개인정보보호 종합지원 포털 <http://www.privacy.go.kr>.

2) 개인정보보호법 제정 2011.3.29 법률 제10465호, 2011.9.30 시행.

또한 전담인력을 두고 있는 경우에도 정보보호 업무 인력의 전문성 부족 문제가 심각하다. 유럽의 주요 국가들은 이미 오래전부터 경험과 전문성을 갖춘 정보보호책임자(Data Protection Officer: 이하 DPO)를 임명하도록 법률로 강제하거나 권고하는 유인책을 마련해 오고 있다.

이하에서는 EU와 미국을 중심으로 개인정보보호 관련 전담인력 현황과 최근의 법제도 동향을 살펴보도록 하겠다.

Ⅱ. 유럽과 미국의 정보보호 관련 전담인력 현황

1. 유럽의 정보보호책임자(Data Protection Officer)

1) EU의 「정보보호규정안」

2012년 1월 유럽집행위원회가 새롭게 발표한 「정보보호규정안」은 "정보보호책임자"의 임명, 자격, 지위, 역할 등에 관한 상세한 규정을 포함하고 있다.[3] 그리고 현행 EU 규정(45/2001)에서도 정보보호책임자에 관한 사항을 규정하고 있다. 유럽집행위원회도 2001년도에 정보보호책임자를 임명한 바 있다.

정보보호책임자에 관한 규정을 살펴보면, 우선, 공공기관(단체), 250명 이상의 종업원을 고용하고 있는 사기업 또는 주된 업무가 정보에 대한 정기적이고 시스템적인 모니터링을 포함하고 있는 기관은 반드시 정보보호책임자를 임명해야만 한다(안 제32조 제1항). 그 밖의 기관 또는 단체의 경우 정보보호책임자를 반드시 둘 필요는 없지만 동 규정안에서는 그 임명을 할 수 있도록 규정하고 있다. 정보보호책임자는 정보보호법에 관한 전문지식과 실무경험 그리고 이 규정안에서 요구되는 임무를 수행할 수 있는 능력 등 전문적 자질을 갖추고 있어야 한다(동조 제3항). 또한 자신의 임무를 수행함에 있어서 이해관계의 저촉사항이 없어야 한다. 정보보호책임자의 임기는 최소 2년으로 하되 연임될 수 있으며(동조 제5항), 기업 및 단체는 정보보호책임자의 성명과 연락처를 통해서 감독기관 및 대중과 소통할 수 있다(동조 제7항).

대상기관은 임명한 정보보호책임자가 개인정보보호와 관련한 모든 이슈들을 처리하게 하고, 자신의 임무와 의무를 독립적으로 수행할 수 있도록 보장해 주어야 한다(안 제33조 제1항 및 제2항). 따라서 정보보호 업무와 관련된 정보보호책임자의 독립성을 저해하는 어떠한 지시도 하여서는 아니된다.

정보보호책임자는 이 규정(Regulation)상의 의무준수에 관한 사항을 대상기관의 대표에게 보고하고 조언하며, 개인정보와 관련된 정책과 규정의 이행 및 침해를 모니터링한다(안 제34조 제1항). 또한 정보보호책임자는 이 규정에서 요구

3) General Data Protection Regulation (29/11/2011). Section 4 Data Protection Officer §§ 32-34.

되는 개인정보보호 처리에 관한 데이터베이스 등록부를 유지·관리하며,[4] 규제당국에 대한 대외 대응과 협력, 그리고 개인정보보호 영향평가 및 정보보안에 관한 사항을 총괄한다. 이하에서 상술하는 바와 같이, 유럽 주요국들은 법률에 의해 정보보호책임자의 임명을 강제 또는 권고하고 있는바, 최근에는 정보보호책임자, 관련 기업 및 단체, 그리고 일반 공중에 대하여 법률상담, 컨설팅, 침해조사, 보안 등 서비스를 제공해 주는 회사들도 증가하고 있다.[5]

2) 독일의 연방정보보호법

독일 연방정보보호법(Bundesdatenschutzgesetz)에 따르면, 9인 이상의 개인정보를 자동처리 수단(예를 들면, 컴퓨터, 인적자원정보시스템, 고객관리데이터베이스, 기업자원계획시스템, 기타 소프트웨어시스템 또는 웹서비스)에 의해 처리하는 기업은 1개월 내에 서면에 의해 정보보호책임자(DPO)를 임명하여야 한다.[6] 또한 대상기관이 다른 수단에 의해서 개인정보를 처리하는 경우라도 개인정보처리를 위해 20명 이상의 종업원을 고용하고 있다면 정보보호책임자를 두어야 한다. 그리고 정보처리 대상의 수와 관계없이, 해당 기관이 자동화수단에 의해 민감한 개인정보를 처리하거나 개인의 특성, 능력, 성과 또는 행위 등에 관한 사항에 접근하고자 할 경우에도 정보보호책임자를 임명해야 한다. 대상기관이 마케팅, 설문조사 또는 정보이전을 위해 상업적으로 자동화처리를 수행하는 경우에도 정보보호책임자를 임명하는 것은 의무사항이다. 정보책임자는 반드시 고용(파트타임 포함)될 필요는 없으며, 용역계약에 의해서도 임명할 수 있다.

3) 노르웨이, 프랑스 등의 경우

노르웨이, 스웨덴, 네덜란드, 스위스의 경우 정보보호책임자(DPO)의 임명을 의무가 아닌 권고사항으로 규정하고 있다. 그러나 정보보호책임자를 임명한 기업에 대해서는 규제기관에 대한 복잡한 통지의무를 면제시켜 주는 혜택을 부여함으로써 정보보호책임자의 임명을 장려하고 있다. 스위스 연방정보보호법[7]을 예로 들면, 모든 사업자들은 개인정보의 정기적인 수집과 처리에 앞서 그에 관한 사항을 '연방 데이터보호 및 정보행정관(Federal Data Protection and Information Commissioner)'에게 통지(notifica-

4) 현행 EU Regulation(45/2001) 제26조에서 정보보호책임자(DPO)에게 개인정보 처리에 관한 등록부를 유지·관리하도록 요구하고 있다.

5) e.g., Data Protection Officer <http://www.dataprotectionofficer.com/About-Us.aspx>

6) Lothar Determann & Christoph Rittweger, *Data Protection Officers and Global Privacy Chiefs: Legal Requirements and Opinions*, 1048 PLI/Pat 481, 485, 2001.

7) Federal Act of June 19, 1992 on Data Protection.

tion)하여야 한다. 여기에는 사업자명과 주소, 정보파일의 명칭과 목적, 정보에 대한 접근을 주장할 수 있는 사람의 이름, 처리되는 개인정보의 범주, 정보 수령자 및 정보 수집에 참여한 자의 범주, 수집된 정보를 변경할 수 있는 제3자 등에 관한 사항이 포함되어야 하며(Art. 11a para. 5 lit. e Swiss Act), 이 모든 정보는 행정관의 웹사이트를 통해 공중에 공개된다. 실무적으로 사업자들은 이러한 의무를 회피하기 위하여 정보보호책임자를 두는 쪽을 선택하는 경우가 많다.

한편, 정보보호책임자의 임명을 의무사항으로 두고 있지 않은 다른 EU 회원국인 오스트리아, 프랑스, 스페인 등은 이러한 면제규정을 두고 있지 않다.[8]

2. 미국 IT기업의 정보보호 전담인력

미국은 앞서 살펴본 EU 주요국과 달리, 정보보호책임자(DPO)의 임명을 법적으로 강제하지 않는다. 그러나 최근 마이크로소프트(Microsoft), 구글(Google) 등과 같은 다국적 IT 기업들은 스스로의 필요에 의해 정보보호 전담조직 및 전문 인력을 두고 있다. 이는 개인정보 및 프라이버시와 관련된 미국 법률 체계의 복잡성과 세계적인 정보보호 강화 추세에 대비하기 위한 것으로 평가된다. 미국은 유럽과 같이 포괄적이고 단일한 개인정보보호 규정을 가지고 있지 않고 영역별, 목적별로 정보보호 규정을 마련하고 있다. 따라서 각 영역별로 산재되어 있는 정보보호 규정을 일일이 검토하는 데 많은 시간과 비용이 발생하고 있다.

마이크로소프트사의 경우 정보보호 전담 인력으로 40명을 두고 있으며, 정보보호 관련 업무를 하고 있는 인력이 400명에 이른다. 구글의 경우 약 60명의 엔지니어와 법무팀이 정보보호 업무를 전담하고 있다.[9] 제품 개발에 있어서 이들 엔지니어들은 정보보호에 관한 대책을 수립하고, 법무팀이 이에 대한 법적 검토를 한다. 구글은 정보보호책임자(DPO)로서 "Google+" 프라이버시 책임자를 고용한 바 있다.

Ⅲ. 유럽과 미국의 정보보호 법제 동향

1. 정보보호지침

EU 집행위원회(European Commission)는 1995년 「정보보호지침(Data Protection Directive, 95/46/EC)」을 제정하여 EU 국민의 개인정보를 보호하고 있다. 이 지침은 국가별로 상이한 개인정보보호 수준을 통일화하여 EU 역내에서 모든 회원국의 국민이 동일한 수준의 개인정

8) Id. at 486.

9) 2011년 12월 8-9일 미국 시애틀에서 Law Seminar International이 주최한 "Technology and New Media Law" 컨퍼런스에서 미국 기업들은 정보보호 전담인력에 관하여 발표하였다. <http://www.lawseminars.com/detail.php?SeminarCode=11COMWA#agenda>; 박춘식, 개인정보보호 전담인력만 MS-40명, 구글-60명 등록, 데일리시큐, 2011. 12. 12.

보보호를 받을 수 있도록 하고 있다. 동 지침은 자동화된 수단 및 구조화된 매뉴얼 파일에 의해 개인정보를 처리하는 경우에 적용된다.

이 지침은 특히 EU 기업이 EU 국민의 개인정보를 역외로 판매하는 것에 대하여 엄격한 규정을 두고 있다. 즉, EU 국민의 개인정보를 EU 역외로 이동시키기 위해서는 해당 국가가 반드시 충분한 수준의 정보보호를 제공하고 있어야 한다. EU가 인정하는 충분한 정도의 정보보호 수준을 갖춘 국가에 대해서는 특별한 제한 없이 EU의 개인정보를 이전시킬 수 있으나, 그 밖의 국가에 대해서는 개인정보를 수출할 수 없다. 다만, 예외적으로 제3국에 있는 해당 기업 등이 정보보호기준에 부합하는 충분한 보장수단을 제공할 수 있는 경우에만 개인정보를 수출할 수 있도록 하였다.

한편, 정보보호지침은 정보보호 보장수단으로서 집행위원회가 인정하는 표준계약서[10]를 사용할 경우에는 정보의 효과적인 보호를 담보해야 한다는 의무를 충족하는 것으로 보았다.

2. 정보보호규정안

1) 제정배경과 적용범위

2012년 1월 25일 유럽집행위원회(European Commission)는 온라인 프라이버시권을 강화하고 디지털경제를 촉진시키기 위하여 1995년 「정보보호지침(Data Protection Directive)」을 포괄적으로 개혁하는 「정보보호규정안(General Data Protection Regulation)」[11]을 제안하였다.[12] 이 정보보호규정안은 정보보호지침에 비해 보다 강력한 개인정보보호 규정들을 포함하고 있으므로 관련 사업을 영위하는 기업에게 비용과 인력 등의 부담을 주게 될 것으로 본다.

이 규정의 제정근거는 개인정보보호를 규정하고 있는 「EU 기능에 관한 협약(Treaty on the Functioning of the European Union)」 제16조 제2항에 두고 있으며, 금번 개정안은 "지침(Directive)"이 아닌 "규정(Regulation)"의 형태를 띠고 있으므로 EU 국민의 정보를 처리하는 자는 그

10) 국제상업회의소(ICC)를 중심으로 2001년 1차 표준계약서를 마련하여 발표하였으나 관련 업계의 반발로 수정하게 되었으며, 2005년 제2차 표준계약서를 채택하였다.

11) 규정(regulation)은 회원국의 특별한 승인 없이도 회원국 정부, 개인, 법인 등 EU 전체에 직접 적용되는 가장 강력한 EU 규범이다.

12) Commission proposes a comprehensive reform of the data protection rules, 2012. 1. 25. <http://ec.europa.eu/justice/news-room/data-protection/news/120125_en.htm> See REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data(General Data Protection Regulation), Version 56 29/11/2011 <http://www.telemedicus.info/uploads/eu-com-draft-dp-reg-inter-service-consultation.pdf>.

처리가 EU 역내에서 이루어지는지 여부와 관계없이 적용을 받게 된다. 즉 EU 역외라도 EU 국민에게 상품이나 서비스를 제공하는 자는 이 규정안의 적용을 받는다. 이하에서 「정보보호규정안」의 주요내용을 살펴보면 다음과 같다.

2) 동의요건 강화

이번 규정안은 대상기관(the controller or the processor)이 정보를 처리하기 전에 얻어야 하는 정보주체의 동의에 관한 사항을 강화하였다. 특히 개인정보 이용 동의는 반드시 사전에 옵트인(opt-in) 방식으로 획득되어야 한다. 또한 정보보호지침에서는 아동의 정보 수집에 관한 구체적인 규정을 두고 있지 않았는데, 이번 규정안에서는 18세 미만의 청소년 정보를 이용하기 위해서는 부모 등 법정대리인의 동의를 얻도록 규정하였다(안 제3조 제18항 및 제7조).

3) 개인정보 삭제권

이 규정안에서는 정보주체의 권리를 강화하였다. 예를 들면, 이용자는 자신의 정보가 불법적으로 인터넷에 공개된 경우 해당 정보를 삭제하거나 추가적으로 공개되지 않도록 사업자 등에게 요구할 수 있는데, 이를 "개인정보 삭제권(Right to be forgotten and to erasure)"이라고 한다(안 제15조). 이러한 요청을 받은 사업자 등 대상기관은 해당 정보 및 관련 인터넷 링크 등을 지체없이 삭제하여야 한다. 이 개인정보 삭제권은 최근의 소셜 네트워크 서비스(Social Network Service) 등을 통한 개인정보의 불법적인 확산을 방지하는 데 중요한 역할을 할 것으로 평가된다.

4) 정보 이동권

정보주체는 자신의 정보를 저장장치로부터 전자적 · 체계적 형식으로 복제하여 획득할 수 있으며, 해당 기관으로부터 제3자에게 이전하도록 요구할 수 있다(안 제16조).

5) 프로파일링 조치

모든 자연인은 자신에게 중요하거나 법률적 효과를 발생시키는 프로파일링[13] 조치의 대상이 되지 않을 권리를 가진다(안 제18조). 즉, 특정인의 동의 없이 그에 관한 근로, 신용, 경제적 상황, 위치, 건강, 관심사, 신용, 행위 등에 관한 사항을 분석하거나 평가할 수 없다.

6) 정보 보안

대상기관은 개인정보침해의 위험을 평가하고 이를 방지하기 위한 적절한 수준의 보안조치를

13) 프로파일링(profiling)이란 특정인의 개인정보를 수집하고 분석하여 원하는 그에 관해 정보를 획득하는 것을 말한다.

확보해야 한다(안 제27조). 이 규정안은 정보보호지침(Directive 95/46/EC) 제17조 제1항의 대상인 "controller"뿐만 아니라 "processor"까지 포함시켰다. 대상기관은 개인정보 유출 등 침해가 발생한 경우 지체 없이 24시간 이내에 그 사실을 규제기관에 보고하고, 또한 해당 이용자에게도 통지하여야 한다(안 제28 및 제29조). 따라서 대상기관은 정보유출에 대한 상시 모니터링과 함께 침해발생시 적극적이고 효과적인 대응을 할 수 있는 절차 및 체계를 갖출 것이 요구된다.

7) 정보보호 영향평가

대상기관은 개인정보처리가 이용자의 권리와 자유를 위협할 소지가 있는 경우 그 처리절차에 앞서 정보보호 영향평가(data protection impact assessment)를 수행하여야 한다(안 제30조). 규정안에서는 이러한 위협의 구체적인 경우를 제시하고 있다. 그리고 개인정보 침해의 위험이 높은 처리절차에 대해서는 반드시 감독기관과 협의하여야 하며, 또한 개인정보를 제3국으로 이전하고자 할 경우에는 감독기관의 승인을 받아야 한다(안 제31조).

8) 정보보호책임자

앞서 상술한 바와 같이, 이 규정안에서는 공공기관 및 단체, 250명 이상의 종업원을 고용하고 있는 사기업, 그리고 개인정보에 대한 정기적인 모니터링을 주된 업무로 하는 기관 및 단체 등은 정보보호책임자(Data Protection Officer)를 의무적으로 임명하도록 하고 있다(안 제32조). 정보보호책임자는 소속 기관의 개인정보보호와 관련된 모든 이슈, 정책, 조사, 보고 등에 관한 업무를 독립적으로 수행하며, 이 규정안상의 의무 이행에 관하여 보고하고 조언할 권한을 갖는다(안 제33조).

9) 벌금

각 EU 회원국의 개인정보보호 규제기관은 의무 위반의 종류와 정도에 따라 정해진 벌금을 부과할 수 있다(안 제79조). 규정안은 침해행위에 대해 부과할 수 있는 상한과 하한의 벌금을 규정하고 있는데, 예를 들면, 제5조, 제6조 및 제7조 상의 동의 조건을 따르지 않은 경우 등에 있어서 100,000~1,000,000유로 또는 사업자의 총매출액의 5%까지 부과할 수 있도록 하였다.

3. 독일

독일 사회민주당(SPD)은 2012년 2월 25일에 이용자 동의에 의해서만 쿠키(cookies)를 설정할 수 있도록 하는 「텔레미디어법(TMG)」 개정안을 연방의회에 제출하였다. 이 개정안 제13조에서는 정보통신제공자의 의무로서 쿠키정보에 대한 규제를 추가하였는데, 즉 이용자의 단말기에 데이터를 저장하거나 이용자의 단말기에 저장되어 있는 데이터에 접근하기 위해서 이용자

에게 사전 통지를 하고, 이용자가 이에 동의한 경우에만 쿠키를 설정하는 옵트인(opt-in) 규제방식을 원칙으로 채택하였다. 다만, 정보통신망에서 통신의 전달이 유일한 목적인 경우에는 이용자가 정보통신서비스를 이용하기 위해서 반드시 필요하다고 명백하게 의사를 표현한 경우에는 옵트아웃(opt-out) 규제를 할 수 있다.[14]

4. 미국

1) 정보보호법규 체계

미국은 개인정보보호에 관한 포괄적인 법률을 가지고 있지 않고, 각 영역별로 민간과 공공부문을 분리하여 개인정보를 보호하고 있으므로 각각의 개별입법을 제정하는 방식(sectoral approach)을 취하고 있다. 또한 미국의 개인정보 규제는 정부 주도적이기보다는 영역별 법률과 지침 및 자율규제(self-regulation)를 혼합적으로 적용하는 방식을 선택하고 있다.[15] 이는 미국 연방헌법이 개인정보보호를 명시적으로 규정하지 않고 연방대법원의 판례를 통해 보호하는 데 그 원인을 찾을 수 있다.[16] 따라서 EU와 비교해 볼 때 영역에 따라 일정 수준의 정보보호를 만족한다고 볼 수 있으나 전체적으로는 미흡한 부분이 존재한다.

민간 분야의 영역별 주요 정보보호 법률을 살펴보면, 1970년 Fair Credit Reporting Act, 1988년 Video Privacy Protection Act, 1992년 Cable Television Protection and Competition Act, 1998년 Children's Online Privacy Protection Act, 2010년 Massachusetts Data Privacy Regulations 등이 있다. 한편, 공공부문에 있어서는 1974년 제정된 프라이버시법(Privacy Act of 1974)[17]이 적용되어 미국 정부기관에 의해 보유되고 있는 개인정보를 보호하고 있다.

이러한 영역별 접근으로 인하여 개인정보보호기구 또한 포괄적이고 단일한 기구가 없는 실정이다. 공공부분에서는 예산관리국(Office of Management and Budget: OMB)이, 민간부문에서는 연방거래위원회(Federal Trade Commission: FTC)가 아동의 온라인 프라이버시, 소비자신용정보, 공정한 거래관행과 관련한 프라이버시를 보호하는 법률을 집행하고 감독하고 있다.[18] 아동의 정보보호와 관련하여 앞서 살펴본 EU 정보보호규정안에서는 18세 미만의 청소년

14) Entwurf eines … Gesetzes zur Änderung des Telemediengesetzes(TMG), Drucksache 17/8454, 2012.1.24. <http://dipbt.bundestag.de/dip21/btd/17/084/1708454.pdf>.

15) William J. Clinton & Albert Gore, Jr., A Framework for Global Electronic Commerce, July 1, 1997. <http://www.technology.gov/digeconomy/framewrk.htm>.

16) 김기열, 공공부문에 관한 외국의 개인정보보호 법제와 국내 입법의 검토방향, 「법제」, 2010.9, 19면.

17) 1988년에 제정된 Computer Matching & Privacy Act는 컴퓨터화된 데이터 분석 및 공유와 관련하여 법집행기관이 따라야 하는 절차규정들을 포함하고 있으며, 이 법은 1974년 프라이버시법을 개정한 것이다.

18) 한국인터넷진흥원 <http://privacy.kisa.or.kr/kor/privacy/privacy02L.jsp>.

정보를 획득하기 위해서는 부모의 동의를 얻도록 한 것과 달리, 미국 COPPA(Children's Online Privacy Protection Act)에서는 부모의 동의가 필요한 청소년의 연령을 13세로 규정하고 있다. 최근 미국의 소비자단체들은 COPPA의 적용대상을 EU와 같이 18세로 강화할 것을 주장하고 있다.[19]

2) 최근의 입법동향

(1) 캘리포니아의 온라인 개인정보보호법[20]

애플, 구글, 마이크로소프트와 같은 주요 모바일 플랫폼 기업들이 자사 제품의 애플리케이션에 개인정보보호방안을 포함하기로 동의함에 따라 애플리케이션을 다운로드 받기 전에 해당 애플리케이션이 접속, 이용, 공유하는 데이터에 대하여 이용자들은 통지를 받게 된다고 캘리포니아 검찰총장 카말 해리스(Kamal Harris)가 발표하였다. 이에 따라 미국에서 소비자 개인정보를 강력하게 보호하는 캘리포니아「온라인 개인정보보호법(Online Privacy Protection Act)」이 모바일 애플리케이션에도 적용되게 되었다. 현재 캘리포니아「온라인 개인정보보호법」은 소비자 식별정보를 수집하는 상업적 웹사이트나 온라인 서비스는 수집되는 정보 유형을 상세히 알리고 해당 정보가 공유되는 방식 및 저장된 자료를 소비자가 검토하고 수정하는 방법을 설명하는 개인정보보호 정책을 소비자가 쉽게 인지할 수 있도록 게시하도록 하고 있다.

해당 정책에 동의한 6개 모바일 플랫폼 기업들은 개별 애플리케이션에 대한 개인정보보호 정책이 스토어(store)에 게시되거나 링크할 수 있도록 애플리케이션 스토어 및 시장을 재정비하고 플랫폼 제공자들을 감독하게 된다.

(2) 비디오 프라이버시 보호법

최근 미국사법위원회는 비디오 상점의 대여(rental) 목록을 공개하지 못하도록 하는「비디오 프라이버시 보호법(Video Privacy Protection Act of 1988: VPPA)」의 개정과 관련한 청문회를 개최하였다. 현재 이 법은 이용자들의 요구가 있더라도 비디오 대여사업자들이 소셜미디어 사이트에서 이용자들의 스트리밍 콘텐츠를 공유하는 것을 금지하고 있다.

이번 개정안에 동의하는 측은 인터넷 DVD 대여 사이트 넷플릭스(Netflix)가 제안한 개정안에 따라 동법이 개정된다면 이용자가 자신의 대여정보를 용이하게 공유하도록 할 것으로 기대하고 있다. 반면, 해당 개정안에 반대하는 측은 이번 개정안은 실효성이 의문시된다고 비난하고

19) That Facebook Friend Might Be 10 Years Old, and Other Troubling News, Consumer Reports Magazine, June 2011. <http://www.consumerreports.org/cro/magazine-archive/2011/june/electronics-computers/state-of-the-net/facebook-concerns/index.htm>.

20) "Tech firms agree to privacy protections for mobile apps.", CNET, 2012. 2. 23. http://www.zdnetasia.com/tech-firms-agree-to-privacy-protections-for-mobile-apps-62303973.htm.

있다. 또한, 전자사생활정보센터(Electronic Privacy Information Center)는 이번 개정이 필요한 것은 사실이나, 오히려 기존의 법을 강화하는 방향으로 개정될 필요가 있다고 밝혔다. 즉, 동 개정안은 사업자가 개인정보를 공개할 때마다 그에 앞서 소비자의 동의를 구하도록 하는 요건을 삭제하는 것으로 이는 비디오 대여기록의 공개에 대한 통제권을 소비자가 아닌 사업자에게 이전하는 것이라고 설명하였다.[21]

(3) 소비자 프라이버시 권리장전

최근 미국 정부는 인터넷 기업들에 이용자의 개인정보 관리방침을 제시하는 지침인 '소비자 프라이버시 권리장전(Consumer Privacy Bill of Rights)'을 발표하였다. 이번 지침의 핵심은 다음의 7가지로 정리할 수 있다. 첫째, 소비자들은 기업이 자신의 정보를 수집하고 이를 어떻게 이용하는지 통제할 개별 통제권을 가진다. 둘째, 소비자는 프라이버시와 정보보안 정책과 관련하여 이해하기 쉬운 정보를 얻을 권리를 가진다. 셋째, 소비자들은 기관들이 소비자가 정보를 제공하는 조건에 적합한 방식으로 개인의 정보를 수집, 활용 및 공개할 것이라고 기대할 권리를 가진다. 넷째, 소비자들은 자신의 개인정보를 안전하고 책임감 있게 취급하도록 할 권리를 가진다. 다섯째, 소비자들은 활용 가능한 형식으로 개인정보를 접근하고 수집할 권리를 가진다. 여섯째, 소비자들은 기업들이 수집하고 보유하는 개인정보에 관한 합리적인 제한을 둘 수 있는 권리를 가진다. 일곱째, 소비자들은 기업들이 이번 지침을 엄수하는 적절한 조치에 따라 개인정보를 처리하도록 할 권리를 가진다.

백악관은 이번 지침의 일환으로 인터넷 업체가 웹브라우저상에 추적방지 기술을 도입하도록 유도할 방침이다. 즉, 이용자들이 인터넷 서비스를 이용하면서 '추적금지(Do Not Track)' 버튼을 누르면 개인정보 수집을 차단할 수 있도록 하는 것이다.

한편, 이 지침은 법적인 강제력이 없다는 한계가 있지만 백악관이 의회를 상대로 법제화를 촉구하고 있어 관련 법률안이 제출될 가능성도 있다. 그리고 상무부는 이 가이드라인을 바탕으로 인터넷 업계와 공동으로 구체적인 사생활보호 규정을 마련할 계획이다. 이 규정이 시행되면 추적방지 기술을 도입하기로 약속한 기업이 이를 위반하는 경우 연방거래위원회(FTC)로부터 제재를 당할 수 있도록 권한을 부여할 예정이다.[22]

손 승 우
(단국대학교 법학과 교수)

21) "Senate Committee Hears Testimony to Amend Video Privacy Protection Act", Heardlander Magazine, 2012. 3. 8. <http://news.heartland.org/newspaper-article/2012/03/08/senate-committee-hears-testimony-amend-video-privacy-protection-act>.

22) "White House announces new privacy 'Bill of Rights,' Do Not Track agreement", Arstechnica, 2012. 2. 22. <http://arstechnica.com/tech-policy/news/2012/02/white-house-announces-new-privacy-bill-of-rights-do-not-track-agreement.ars>.