情 報 保 護 學 會 誌
第22卷 第1號, 2012. 2

미국의 개인정보보호 법 · 제도 동향

전 은 정*, 김 학 범**, 염 흥 열***

요 약

미국의 개인정보보호 정책은 시장의 자율규제에 입각하여 소비자의 권리를 보호하는 것에 초점을 맞추고 있다. 관리되는 법률로는 연방정부기관이 보유하고 있는 개인정보에 관한 보호법규인 1974년의 프라이버시법(Federal Privacy Act 1974)과 각 주단위로 규정된 프라이버시권 관련 법률들이 있다. 현재 공공과 개인을 아울러서 총괄하는 법은 존재하지 않지만 다양한 영역별로 접근 방식을 택하여 세부적으로 공공, 금융, 통신, 교육, 의료, 비디오 감시, 근로자 정보 등 각 영역별로 제정하여 시행하고 있다. 본고에서는 미국의 개인정보보호 법제 현황에 대해 살펴보았으며, 최근에 국내에서도 수행기관이 지정된 개인정보영향평가에 대한 내용을 분석하였다.

Ⅰ. 서 론

2011년 9월 30일자로 국내에서는 개인정보보호법이 발효되어 이 법의 대상이 되는 국내의 350만 업체들은 법에서 요구하는 요건들을 만족시키기 위한 노력들이 활발히 진행되고 있다.

이 법의 적용대상은 공공·민간부문의 모든 개인정보처리자로 포털, 금융기관, 병원, 학원, 제조업, 서비스업 등 72개 업종 350만 전체 사업자와 국회·법원·헌법재판소·중앙선거관리위원회 등 헌법기관, 부처, 지자체, 공사, 공단, 학교 등 2만 8천 전체 공공기관 및 사업자 협회 · 동창회 등 비영리단체이다. 이들 대상에 대한 적용범위는 전자파일 형태 외에 동창회 명부, 민원서류, 이벤트 응모권 등의 수기문서가 포함된다.

우리나라 개인정보보호법에서의 개인정보는 '생존하는 개인을 식별하거나 식별할 수 있는 일체의 정보로, 해당 정보만으로는 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 개인을 알아볼 수 있는 모든 정보를 포함하는 개념'으로 정의하고 있다[1]. 이 외에 세계 각국의 법률에서 정의한 개인정보의 개념은 [표 1]과 같다[2].

국내에서 개인정보보호법의 발효로 인하여 그 어느

〔표 1〕 각국 법률의 개인정보 개념 정의

법률	내 용
OECD 가이드라인 제1조	식별된 또는 식별가능한 개인에 관한 정보
EU 지침 제2조	정보주체의 신원이 확인되었거나 확인 가능한 정보
캐나다 프라이버시법 제3조	신원을 확인할 수 있는 개인에 대한 정보
일본 개인정보보호에 관한 법률 제2조	생존하는 개인에 대한 정보로서 특정한 개인을 식별할 수 있는 정보
호주 프라이버시법 제6조	당해 정보 또는 의견(opinion)으로부터 신원이 명백하거나 확실시 될 수 있는 개인에 관한 정보 또는 의견
영국 개인정보보호법 제1조	신원을 확인할 수 있는 생존하고 있는 개인과 관련된 데이터 또는 정보 관리자가 보유하고 있거나 앞으로 그러할 가능성이 높은 기타 정보 또는 데이터로부터 신원이 확인가능한 생존 개인과 관련된 데이터
프랑스 정보처리 축적 및 자유에 관한 법률 제4조	형식에 관계없이 직접 또는 간접으로 개인을 식별할 수 있게 하는 정보로서 자연인 또는 법인이 처리하는 정보
독일 연방개인정보보호법 제3조	신원이 확인되었거나 확인 가능한 정보주체의 인적 · 물적 환경에 관한 일체의 정보

[참조 ; 고려대, 주요 국가의 개인정보보호 동향 조사 보고서]

* 순천향대학교 정보보호학과 (junej@sch.ac.kr)
** ㈜지엔에스인증원/동국대학교 국제정보대학원 (khb0305@gns-iso.co.kr)
*** 순천향대학교 정보보호학과 (hyyoum@sch.ac.kr)

때보다도 우리나라보다 먼저 진행되고 있는 해외 국가들의 개인정보보호 관련 추진 현황에 대해서도 관심이 많아지고 있다. 따라서 본고에서는 먼저 미국의 정보보호 법·제도 현황에 대해서 상세한 내용을 분석한다. 이후에 유럽, 일본, 중국, 호주 등의 추진 내용에 대해서도 분석할 예정이다.

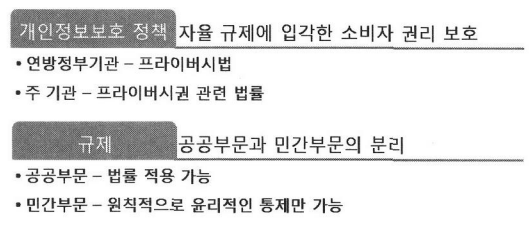
Ⅱ. 미국의 개인정보보호 정책

미국의 개인정보보호 정책은 시장의 자율규제에 입각하여 소비자의 권리를 보호하는 것에 초점을 맞추고 있다. 관리되는 법률로는 연방정부기관이 보유하고 있는 개인정보에 관한 보호법규인 1974년의 프라이버시법(Federal Privacy Act 1974)과 각 주단위로 규정된 프라이버시권 관련 법률들이 있다.

미국의 프라이버시권이 연방 대법원의 판례에 따라 보통법 상의 권리로 인정해 왔기 때문에 유럽 국가와는 달리 포괄적이고 체계적인 개별적인 법체계는 갖지 아니하고 영역별로 접근 방식을 택하여 세부적으로 공공, 금융, 통신, 교육, 의료, 비디오 감시, 근로자 정보 등 각 영역별로 제정하여 시행하고 있다[3].

미국에서의 개인정보보호는 공공부문과 민간부문으로 나누어 공공부문에만 법을 적용하고 민간부문에는 원칙적으로 윤리적인 통제만 가능하게 되어 있다. 미국의 개인정보보호제도는 1966년의 정보 공개법(Freedom of Information Act) 제정에 따라 연방정부가 보유하고 있는 정보를 원칙적으로 공개하되 프라이버시법에 의해 정부에 대한 규제를 가하고 민간부문에는 정보의 자유로운 유통을 보장하며 개별 분야에서의 개인정보보호를 목적으로 한 영역별 보호 법제를 가지고 있다는 점이 특색이다.

〔그림 1〕 미국 각 주별 개인정보유출통지 관련법 제정 현황
〔참조 : 한국인터넷진흥원 조사 자료(2009)〕(흰색은 미제정주)

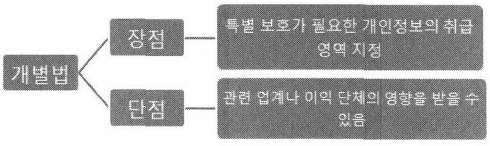


〔그림 2〕 미국의 개인정보보호 정책

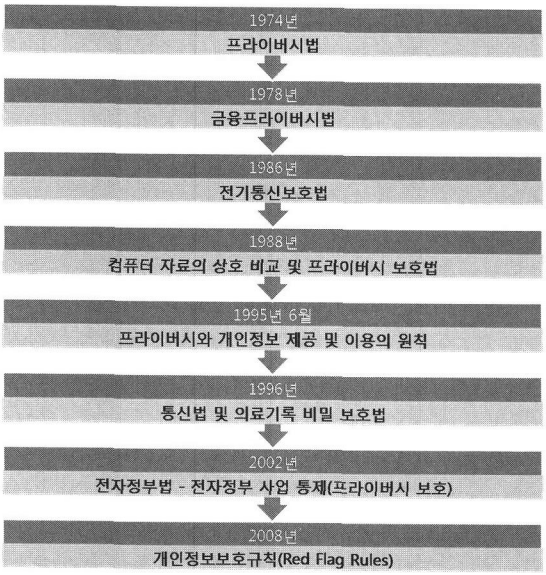
2.1 역사 및 현황

미국에서는 1974년 프라이버시법이 제정된 이래 1978년 금융프라이버시권법, 1986년 전기통신보호법, 1988년 컴퓨터 자료의 상호 비교 및 프라이버시 보호법, 1994년 전기통신 프라이버시법, 1996년 통신법 및 의료기록 비밀보호법이 각각 제정되었다. 한편 국가정보통신기반 구축을 위해 정보통신기반 전담팀에 정보정책위원회를 구성하여 세 개의 팀 중 하나인 프라이버시팀이 1995년 6월에 '프라이버시와 개인정보제공 및 이용의 원칙'을 작성했다. 동 원칙은 계약 자유에 따라 제공자의 통지와 소비자의 동의라는 두 개의 필수조건을 감안하면서 업계의 자율적인 규제가 우선이라는 것을 강조하고 있다. 미국의 개인정보보호법제의 특색인 영역별 방식에 따라 개인정보보호를 위한 많은 개별 법률이 제정되고 있는데 개별법의 장점은 특히 보호가 필요한 개인정보의 취급영역에 한정하여 법적 규제를 행하는 점이라고 하겠다. 그러나 단점으로는 개별 영역별로 법률을 제정하기 때문에 관련업계나 이익단체의 영향을 받을 수 있는 우려가 많다[4].

미국에서는 프라이버시 보호를 강화하기 위한 한 방편으로 2002년 전자정부법에서 정부기관이 전자정부사업을 추진하기 전에 반드시 당해 전자정부사업이 개인정보 및 프라이버시에 미치는 영향을 분석 및 평가하여 그 대책을 마련할 것을 의무화하는 프라이버시 영향평가 제도를 시행하고 있다. 이처럼 미국도 개인 프라이버시의 규제에 대한 중요성과 필요성을 인지하고 그에



〔그림 3〕 개인정보보호 개별법의 장단점



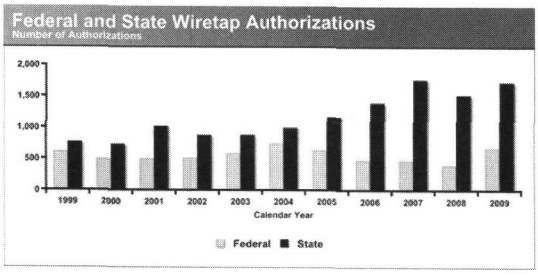
〔그림 4〕 미국의 개인정보보호법 연혁
〔참조 : KISA 정보보호 법제 동향〕

맞게 빠르게 변화하고 있는 추세이다[5].

2.2 정부와 개인정보보호법

미국의 경우 이전 부시정부는 프라이버시보다는 국가보안에 우선순위를 두는 입장을 취해왔던 관계로 IT 분야의 최고 관심사는 정보수집과 이용에 집중되었다. 따라서 주요통신망에 대한 대규모 도청, 현실세계와 사이버세계의 개인활동 내역에 대한 데이터베이스 급증을 초래했다. 또한, 2007년 수립한 사이버전략 중 하나인 리얼ID법은 전 미국인의 개인정보가 담긴 상호 연동된 데이터베이스 구축을 요구하고 있으나 어떠한 정보보호 조항도 없는 폐단을 보이기도 했다.

하지만 오바마 정부는 프라이버시와 국가보안이 균



〔그림 5〕 미국 감청 승인 현황 〔참조: 미연방법원 조사〕

〔그림 6〕 미국의 민감한 정보 정의

형 잡힌 IT 보안정책을 전개하고 있다. 오바마는 연방 CTO(Chief Technology Officer: 국가최고기술책임관)를 신설하여 대통령이 직접 IT 보안 방향을 수립하겠다고 주장함으로써 사이버보안에 우선순위를 두겠다는 의지를 표명했다. 오바마 내각과 자문 구성을 보면 국가보안에 대해 강경노선인 사람과 프라이버시 옹호자가 양립하고 있어 다양한 관점이 전략에 반영될 것으로 고려되며 실제 미국 정책을 개인정보 접근규제 및 이용 규제를 하는 유럽식 정책 형태로 만드는 한편 프라이버시와 국가보안정책과의 조화를 이룰 것으로 예상된다[6].

2.3 미국의 민감한 정보

미국의 경우 민감하지 않은 데이터에 대한 특정 정의는 내리고 있지 않으나 유럽에서와 마찬가지로 민감한 정보에 대한 정의는 내리고 있다. 미국에서 정의하는 민감한 정보로는 종교, 인종, 정치, 성 관심, 건강, Trade Union Member로, 이에 해당하는 데이터를 수집, 또는 활용을 원할 경우 데이터 제공자의 동의는 필수적으로 필요하다. 또한, FTC(Federal Trade Commission)는 데이터를 안전하게 처리 및 유통하지 않는 웹사이트, 데이터베이스 등의 매체에 대해서는 Consumer Protection Law를 적용시킨다고 명시하고 있다. FTC는 이미 오프라인과 온라인의 데이터 활용에 대해 위반한 회사에 대한 규제를 시행하였고 만약 웹사이트와 같은 매체에서 프라이버시 보호의 방침이 없을 경우 Unfair Commercial Practices의 범위 내에서 이를 처리한다[4].

III. 대표적인 개인정보 관리법과 제도

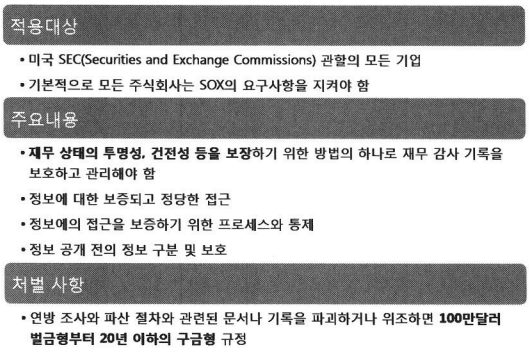
미국의 의료분야 정보보호법인 의료정보 보호법

(HIPPA)이나 전 세계적으로 기업의 내부 통제를 강화하기 위한 사베인-옥슬리법(SOX) 등은 기업의 개인정보보호에 대한 필요성 및 인식을 높이고, 이에 대한 대책을 수립하는데 중요한 동기가 되었다. 이외에도 정보유출시 기업 배상과 관련된 SB 1386법, 금융 분야 정보보호 관련법인 GLBA 등이 마련되어 있다.

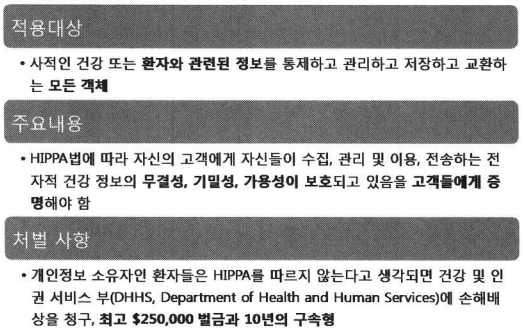
이 장에서는 개인정보보호를 위한 대표적인 법제도 현황과 주요 규정 및 처벌사항 등을 소개한다.

3.1 의료정보 보호법(HIPAA)

미국의 의료정보 보호법(HIPAA, the Health Insurance Portability and Accountability Act of 1996)은 1996년 8월 21일 빌 클린턴 정부에서 제정되었다. 이 법은 의료시스템의 효율성을 높이고 환자 건강관리 정보의 안전한 전자적 이동에 중점을 두고 있어, 건강관리 정보를 안전하게 송·수신하기 위한 시스템 보안과 정보 프라이버시에 대한 규정을 포함하고 있다.



〔그림 7〕 SOX의 적용대상과 주요내용 및 처벌 사항



〔그림 8〕 HIPAA의 적용대상과 주요내용 및 처벌 사항

3.2 사베인-옥슬리법(SOX)

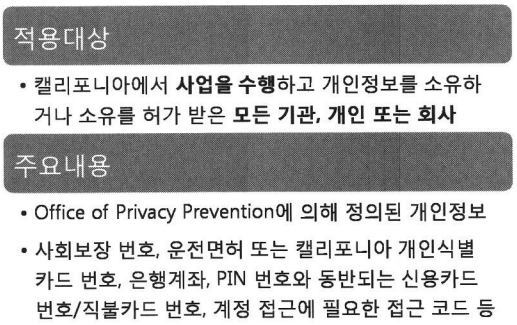
사베인-옥슬리법(SOX, Sarbanes-Oxley Act)은 2001년 엔론사 사건을 계기로 주식회사 등의 재무 상태와 투명성, 책임성을 강화하기 위해 2002년 7월에 제정되었다. SOX는 기업회계 및 재무 보고의 투명성과 정확성을 높이는 것을 목적으로 하며, 투자자에 대한 기업경영자의 책임과 의무, 벌칙을 규정한 미연방 법률이다.

3.3 캘리포니아 데이터베이스 보안침해 고지법

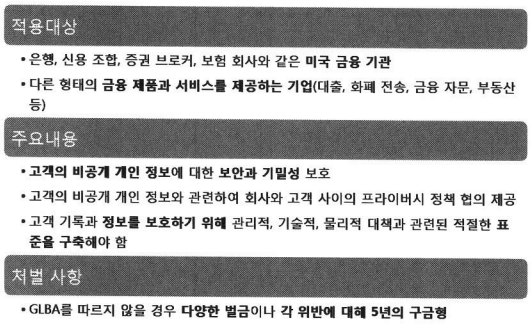
2003년 6월 발효된 캘리포니아 데이터베이스 보안침해 고지법(California Database Security Breach Notification Act)(일명, SB 1386)은 인가되지 않은 사람이 캘리포니아 주민의 암호화되지 않은 개인정보를 획득했거나, 또는 획득했다고 판단되어질 때 해당 개인정보를 관리하는 기업 또는 주 기관이 그 데이터의 보안 침해 사항을 당사자에게 공개하도록 규정하고 있다. 캘리포니아 SB 1386은 데이터베이스 보안 및 침해 고지에 관해 처음으로 다루고 있는 법으로 제정 이후 캘리포니아에서 사업을 수행하는 모든 기업뿐만 아니라 캘리포니아에 위치하지 않더라도 캘리포니아 주민의 개인정보를 보유한 기업들에게 영향을 미쳤다. 또한, SB 1386은 미국의 다른 주에도 영향을 미쳐 미국 내 반 이상의 주에서 이와 유사한 법과 규칙을 제정하였다[7].

3.4 금융정보 보호법(GLBA)

금융 관련법의 여러 변화 중에서 GLBA (Graham-Leach-Bliley Act)는 고객의 사적인 금융정보를 보호하기 위해 설계된 중요하고 새로운 규정을 포함한다.



〔그림 9〕 SB 1386의 적용 대상과 주요내용



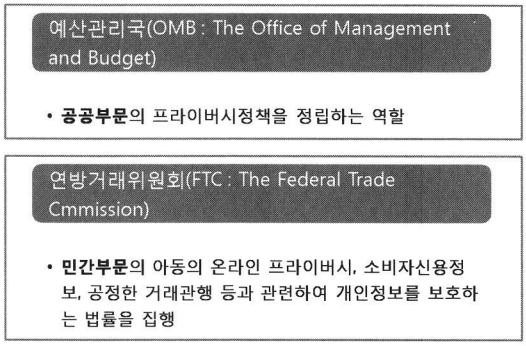
〔그림 10〕 GLBA의 적용대상과 주요내용 및 처벌 사항

GLBA는 금융기관이 비인가된 사용·접근으로부터 사적인 개인정보를 안전하게 하고 보호하도록 규정한다. 캘리포니아 SB 1386과는 다르게 GLBA는 개인의 사적인 금융정보가 암호화되었다 할지라도 조직이 오용의 가능성을 합리적으로 방지하기 위해 효과적인 암호화 기법을 사용했음을 증명할 수 없다면 고객에게 이를 고지해야 한다[7].

3.5 법과 제도를 위한 개인정보보호기구

미국은 개인정보보호에 관한 사항을 포괄적으로 규정하고 있는 개인정보보호기본법은 가지고 있지 않지만, 각 영역별로 개인정보보호를 위한 법·규범을 마련해 두고 있다. 특히 공공부문에 있어서는 1974년 프라이버시법(The Privacy Act of 1974)이 적용되어, 미국정부기관에 의해 보유되고 있는 개인정보를 보호하고 있다. 그러나 미국은 공공부문과 민간부문의 개인정보보호체계가 분리되어 있고, 민간부문에 있어서도 각 영역별로 입법이 이루어지고 규율됨에 따라 포괄적인 개인정보보호기구는 없는 상황이다.

따라서 공공부문과 민간부문을 나누어 살펴보면, 공공부문에 있어서는 예산관리국(OMB :The Office of Management and Budget)에서 프라이버시법에 따라 연방정부의 프라이버시정책을 정립하는 역할을 맡고 있다. 그러나 OMB는 예산관리차원에서의 제한적인 역할만을 맡고 있는 것으로 볼 수 있다. 한편 민간부문에 있어서는 연방거래위원회(FTC : The Federal Trade Commission)가 아동의 온라인 프라이버시, 소비자신용정보, 공정한 거래관행과 관련하여 개인정보(프라이버시)를 보호하는 법률을 집행하고 준수여부를 감독할 권한을 부여 받아 행사하고 있다. 따라서 포괄적인 개인정보보호기구는 없으나 연방거래위원회의 역할을 참고할 수 있을 것이다[8].



〔그림 11〕 대표적인 개인정보보호기구

Ⅳ. 다양한 개인정보보호 법규와 사례

이 장에서는 앞 장에서 설명한 기본적인 개인정보보호 관련법 이외에 관련된 다양한 법률과 개인정보영향평가 현황에 대해서 살펴본다.

4.1 어린이를 위한 인터넷 보호법(CIPA)

2000년 미국 의회는 학교와 공공 도서관에 필터링 프로그램을 설치하는 것을 목적으로 하는 "어린이를 위한 인터넷 보호법(Children's Internet Protection Act: CIPA)"을 제정했다. 1999년 1월 네 명의 공화당 상원의원에 의해 제안되고 이듬해 12월 노동, 건강, 인적 서비스 세출예산안의 일부로 입법된 이 법은 미국 전역의 공공도서관과 학교의 인터넷접속 컴퓨터에 필터링 소프트웨어를 의무적으로 설치하도록 하였는데, 이를 지키지 않을 경우 연방보조금을 받을 수 없게 된다. 이 법은 형사처벌을 규정하고 있었던 이전의 두 인터넷 규제법안인 CDA나 COPA(Children's Online Protection Act)와 달리 형사처벌 없이 행정적인 규제만을 규정하고 있지만, 연방보조금에 운영비의 많은 부분을 의존하고 있는 공공도서관과 학교에는 형사처벌 못지않은 강제력을 발휘하고 있다.

미국도서관협회(ALA)와 ACLU는 즉각 이법이 수정헌법 제1조가 보장하고 있는 표현의 자유를 침해하고 있다며 소송을 제기하였다. 비록 하위법원의 결정이지만, 이미 1998년 버지니아의 라우던 카운티 공공 도서

관의 사례에서 공공도서관의 필터링 프로그램 설치의 위법성이 확인되었기 때문에 CIPA의 미래도 그리 밝지는 않다. 필터링 소프트웨어들이 가지고 있는 원천적인 기술적 결함과, 사서와 이용자들에 대한 권리침해 때문에 논란이 계속되고 있다[9].

4.2 어린이 온라인 프라이버시 보호법

1998년 기업이 13세 이하 어린이의 개인 정보를 수집할 때 부모의 동의를 받도록 하는 법률인 어린이 온라인 프라이버시 보호법(Children's Online Privacy Protection Act of 1998)이 제정되었다. 현재는 13세 미만의 어린이의 가입을 제한하고 있다. 하지만 실제 페이스북에는 2011년 5월 가입자 가운데 부모의 동의를 통한 13세 미만의 가입자수가 750만명에 이른다고 발표했다. 이러한 조사를 진행한 담당자들도 부모들마저 불법인데도 불구하고 자녀들의 페이스북 가입을 도와주고 있는 상황에서 가입연령을 제한하는 COPPA는 개정돼야 한다고 말했다[10].

4.3 법 진행상의 통신지원법 혹은 범죄수사통신지원법

법원이 영장을 발부하여 합법적으로 감청 행위를 할 때 법 진행의 실효성을 위해서 통신 서비스 제공자가 감청 기술을 개발하도록 하고 있는 제도이다 (CALEA : Communications Assistance for Law Enforcement Act of 1994). 이는 국가안보나 공공이익을 위해 필요한 경우에는 법으로 정해서 제한적으로 감청을 허용하고 이를 법으로 허용한다 하더라도 감청 자체가 기술적으로 불가능한 경우에는 법 진행 자체가 무의미해지므로 이를 법으로 의무화한 것이다. VoIP와 같은 통신 서비스에 이 법을 적용해야 하느냐에 대한 범위 적용을 둘러싸고 논쟁이 끊이지 않고 있다. CALEA는 법원의 명령이 있을 때 통신 회사들이 즉각적으로 감청을 시작하도록 규정하고 있다. 하지만 회사의 시스템 업그레이드에 따른 기술적 문제로 감청을 하지 못하는 경우가 생기는 등 해당 법률을 위반하는 사례가 발생했다. 이를 해결하기 위해 정부에서는 두 가지 방안이 제기되고 있다.

하나는 통신 감청을 제대로 하지 못한 회사에 대해 벌금을 매길 가능성을 높이는 것이다. 문제가 발생했을 때 이를 수정한 뒤 벌금을 소급 적용하는 방안도 포함된다. 다른 하나는 새로운 시스템을 만들어 적용하기 전에 FBI에 그것을 보여줄 경우 그 회사에 대해 인센티브를 제공하는 방안이다. 시스템을 보여주면 문제가 발생해도 면책하는 권리를 제공하는 게 포함된다. 하지만 통신회사들은 기술 디자인과 서비스 출시에 정부가 과도하게 개입하는 것이라며 반발도 많은 상황이다[11].

4.4. 컴퓨터 사기 남용법(CFAA)

미국은 1980년대 초 컴퓨터 범죄가 급증하고 기존의 연방 형사법 규정으로는 이들을 모두 규율할 수 없게 됨에 따라 1984년 미국 연방의회는 연방법전 제 18편 제 1030조(18U.S.C.§1030)에 컴퓨터와 컴퓨터 네트워크에 대한 비인가된 접근과 이용을 규율하는 규정을 포함시켰다. 이후 1986년 이를 개정하여 컴퓨터 관련범죄를 일괄적으로 규정한 컴퓨터 사기 및 오용에 관한 법률(CFAA : Computer Fraud and Abuse Act)을 제정하여 컴퓨터 정보처리에 대한 범죄적 행위를 규제하고 있으며, 동 법은 컴퓨터 범죄가 나날이 지능화·정교화 해짐에 따라 그동안 7차례의 개정을 한 바 있다.

2006년 3월 8일 미국 제7순회 항소법원에서는 CFAA와 관련한 판결이 있었다. 국제공항센터의 전직 직원이 보안파일제거 유틸리티를 사용함으로써 CFAA를 위반했다는 내용이다. 단순히 파일을 삭제하는 것이 아니라 새로운 파일을 덮어씌움으로 완전히 삭제가 되도록 하였기 때문에, 네트워크에 연결된 컴퓨터를 허가 없이 고의적으로 고장 내는 행위에 포함된다는 것이다. 이 판결의 의미는 CFAA의 광범위한 적용 범위를 보여주고 있다[12].

4.5 기타 법규[12]

4.5.1 연방정보보안관리법(FISMA)

정보보호 위협의 심각화와 개별 위험 증가도 잠재하고 있어 이에 대응하는 정보 보안 정책도 나날이 변화가 요구된다. 이에 따라 미국에서는 연방정보보안관리법을 제정하여 연방정부의 운영 및 자산에 대한 정보보안 통제항목의 효율성을 강화하기 위한 총괄적인 프레임워크를 제공한다. 또한 연방정부 및 정보 시스템 보호를 위한 최소 통제 및 유지 방안 개발을 제공 한다. 이는 Computer Security Act of 1987을 대체한 법률이다 (Federal Information Security Management Act of 2002 : FISMA).

4.5.2 소비자 신용보고 개혁법, 공정신용정보법(CCRRA)

공공 법률 제 91-508는 정확성, 공정성, 신용보고 기관 (CRAs)에 의해 조립 개인 정보의 프라이버시를 추진하기 위해 1970년 제정되었다(Consumer Credit Reporting Reform Act of 1996).

4.5.3 스팸메일법(CAN-SPAM)

메일로 스팸을 보내지 못하도록 2003년에 만든 강력한 법안으로 고의로 권한 없이 보호되는 컴퓨터에 접근하여 고의로 다량의 상업적 전자 우편 메시지 전송을 시도하는 행위 등을 규정하고 있다 (Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act of 2003 law).

4.5.4 연방전자금이체법(EFTA)

전자상거래에서 제 3자가 권한 없이 타인의 ID번호나 패스워드, 신용카드 번호를 절취하거나 부정한 방법으로 이용할 위험성에 따라 소비자의 책임범위를 일정액으로 제한하는 법 제도이다(Electronic Funds Transfer Act of 1978).

4.5.5 공정정확신용거래법(FACTA)

신원 도용을 방지하기 위하여 소비자 분쟁의 해결책을 개선하고, 소비자의 신용 정보 접근에 대한 기록의 정확성을 향상시키기 위한 법으로 Fair Credit Reporting Act를 개정한 것이다(Fair and Accurate Credit Transactions Act of 2003).

4.5.6 운전자프라이버시 보호법(DPPA)

운전면허 정보 보호에 관한 보호법으로 운전면허를 취급하는 직원들이 취득한 운전자의 개인정보를 유출하지 못하도록 하는 법률이다(Driver's Privacy Protection Act of 1994).

4.5.7 전기통신 사생활법(ECPA)

주 또는 외국간 상업 영향을 미치는 시스템의 전체 또는 일부를 전송하는 정보 전송에 관한 법률이다 (Electronic Communications Privacy Act of 1986).

4.5.8 전자정보자유법(E-DOIA)

미국에서 정부 기록의 전자화에 대응하고 공개 청구에 대한 회답 지체를 해소하기 위해 1996년 마련한 법. 정부 기록의 전자화에 대한 대응으로 ① 정보 공개의 대상에 전자 기록도 포함된다는 점을 명시적으로 규정하였고, ② 공개 청구된 전자 기록의 공개 형태와 관련하여 청구인이 지정한 공개 형태가 청구 시에 행정 기관에 존재하지 않는 경우에도 청구인이 지정한 공개 형태로 용이하게 변환할 수 있다면, 청구인이 지정한 형태로 제공해야 함을 규정하고 있다. 또한 공개 청구에 대한 회답지체를 해결하기 위한 규정도 구체적으로 제시하고 있다(Electronic Freedom of Information Act of 1996).

4.5.9 가족 교육 권리 및 개인 정보 보호법(FERPA)

학생 교육 기록의 프라이버시를 보호하는 연방 법률이다(Family Education Rights and Privacy Act of 1974).

4.5.10 전화소비자보호법(TCPA)

고객의 요구 사항을 따르지 않고 계속 전화를 걸 경우 재판을 청구할 수 있는 법률이다(Telephone Consumer Protection Act of 1991).

4.5.11 비디오 프라이버시 보호법

비디오, DVD의 허가권 행사에 관련된 법적인 문제를 다루는 법으로 페이스북이나 유튜브와 같은 곳에 적용이 가능하다(Video Privacy Protection Act of 1988).

4.6 미국의 개인정보영향평가(PIA)

4.6.1 개인정보영향평가 정의

개인정보 영향평가(PIA : Privacy Impact Assessment)는 프라이버시와 관련하여 적용되는 법률이나 규정, 정책필요성 등에 일치하는 정보사용을 보장하기 위한 것이다, 전자정보시스템에서 신원확인이 가능한 형

태로 정보를 수집, 유지, 유포하는데 있어서 그 효과와 위험성을 결정하고 잠재적인 프라이버시 침해위험성을 완화를 위한 정보취급과정에서의 대안적인 방법이나 보호방안을 평가하고 검증하기 위하여, 정보가 어떻게 다루어지는가를 분석하는 것이다.

4.6.2 개인정보영향평가 현황

미국은 연방정부의 기능에 한정된 개인정보 영향평가 제도를 도입하고 가장 활발히 운영하고 있다. 개인정보 영향평가는 개인정보처리자가 처리하는 개인정보의 수, 제3자 제공여부, 정보주체의 권리침해 가능성 및 그 위험정도 등을 고려하여 위험요인을 분석하고 개선사항을 도출하는 일련의 평가절차로 정의할 수 있다. 점점 빠르게 진화하고 있는 정보의 대량수집능력, 빠르고 정밀한 분석 및 가공능력으로 인한 개인정보 오남용 침해에 대한 심각한 우려 때문에 최근에는 이 제도의 필요성이 더욱 높아지고 있다.

미국의 PIA 추진의 법적 근거는 전자정부법(The Electronic Government ACT) Section 208 및 프라이버시 규정 이행에 대한 OMB 지침 (M-03-22 OMB Guidance for Implementing the Privacy Provisions of the E-Government ACT of 2002)를 통해 영향평가 대상 및 절차 등을 규정하고 있다[13].

미국은 국세청(IRS)의 대규모 프로젝트에서 프라이버시 영향평가를 요구하기 시작한 것을 시발점으로 1996년 프라이버시 영향평가 지침이 제정됐고, 전자정부법 제정을 통해 프라이버시 영향평가가 추진되었다. 미국에서는 같은 해 전자정부법 제208조에 전자정부 구현 시 프라이버시 영향평가를 의무적으로 시행할 것을 명문화하여 2003년 4월 발효되었다. 영향평가 개념과 방법론을 가장 먼저 개발한 캐나다는 2002년 5월 관련 정책을 발표하고 같은 해 8월 구체적인 영향평가 지침을 고시하여 의료부문의 의무화와 나머지 부문에 대한 자율적인 시행을 권고했다. 평가대상에 있어서는 미국이 연방정부기관을 대상 수행기관으로 정하고 있는 반면 캐나다는 연방정부기관을 포함한 일부 지방정부를 대상범위로 한다. 미국과 캐나다는 각각 관리예산처(OMB)와 프라이버시감독국이 영향평가의 감독을 담당하고 있는데, 영향평가 결과를 제출받아 심의하는 역할을 수행한다. 검토결과는 웹사이트나 관보 혹은 다른 수단을 통해 공개하고 있다[14].

OMB 지침에 따른 개인정보영향평가 대상은 신규 시스템 구축 이전에는 다음과 같은 경우가 해당된다[15].

① 국민의 개인정보를 식별가능한 형태로 수집, 관리, 배포하는 IT 시스템 또는 프로젝트를 개발하거나 조달하는 경우

② 문서감축법(Paperwork Reduction Act)에 따라 식별가능한 10명 이상의 개인정보를 온라인으로 수집하는 경우

일반적으로 PIA는 절차 및 시스템 변경 시에 필요하게 되는데 다음과 같은 경우가 해당된다.

① 종이문서를 전자시스템 기록으로 변형하는 경우

② 기존에 수집한 익명정보를 식별가능한 형태의 정보로 변경하는 기능을 새롭게 적용하는 경우

③ 새로운 기술적용 등과 같은 기존 IT시스템의 신규 운용이 시스템 상의 식별가능한 정보에 중대한 변화를 일으키는 경우(예를 들면, 기관에서 다중으로 저장된 데이터에 대한 접근을 위해 새로운 관계형 데이터베이스 기술이나 웹기반의 처리를 도입하는 경우)

④ 기관에서 식별가능한 형태로 정보를 보존하기 위하여 다른 데이터베이스와 합병, 집중화 또는 매치시키기 위하여 비즈니스 프로세스를 도입하거나 변경하는 경우

⑤ 사용자 인증기술(예를 들어, 패스워드, 전자인증서, 바이오인식 등)이 공공 회원이 접근하는 전자정보시스템에 새롭게 적용되는 경우

⑥ 기관에서 시스템적으로 상거래나 공공 자원으로부터 획득하거나 구매한 식별가능한 형태의 정보 데이터베이스를 기존 정보시스템에 결합하는 경우

⑦ 동시에 여러 기관이 유사한 전자정부 사업을 개시하거나 공동으로 IT투자 개발을 수행하는 경우에 식별가능한 형태의 정보를 상호 교환하거나 신규로 정보를 사용하도록 하는 기능을 공유하는 경우

⑧ 식별가능한 형태로 시스템에 정보항목을 추가하거나 새롭게 정보를 사용 혹은 배포 결과를 유발하는 비즈니스 절차를 변경하는 경우

⑨ 식별가능한 형태의 정보 수집이 새로이 추가되어 개인 프라이버시에 위험을 야기하는 경우(예를 들어, 건강정보 혹은 금융정보의 추가)

이외에 지침에 의하여 PIA 대상에서 제외되는 경우

는 다음과 같다.

① 일반 대중회원으로부터 식별가능한 형태의 정보를 수집하거나 보관하는 IT시스템이 아닌 경우
② 피드백이나 추가정보 제공과 같은 제한적 목적만으로 사용자에게 접근하도록 선택사항을 지정한 경우 (예를 들면, 질의응답이나 코멘트)
③ 특정 국가보안시스템의 경우
④ 모든 PIA 요소가 이미 프라이버시법의 컴퓨터 매칭 조항에 의해 결정되는 매칭 조약에 의해 처리되고 있는 경우
⑤ 모든 PIA 요소가 엄격한 통계목적의 데이터 결합을 허용하는 기관간 조약에 의해 처리되고 있는 경우
⑥ 해당 기관이 식별가능한 형태의 정보를 생성하는 데이터베이스로부터 정보를 검색하거나 결합하지 않고, 개별 목적으로 식별 불가능한 정보만을 수집하거나 IT시스템을 개발하는 경우
⑦ 새로운 프라이버시 위험을 발생시키지 않는 시스템의 작은 변경이나 수집의 경우

4.6.3 평가항목 및 절차

PIA는 다음과 같은 항목을 평가하여야 한다.

① 수집되어야 하는 정보가 무엇인가? (예: 특성, 수집처)
② 정보를 수집하는 이유는 무엇인가? (예: 자격을 결정하기 위해)
③ 정보를 사용하는 의도(예: 기존 데이터를 확인하기 위하여)
④ 공유대상은 누구인가? (예: 특정 목적을 위해 다른 기관과 공유)
⑤ 제공하는 개인정보를 자발적으로 제공하거나 거절할 수 있는가?
⑥ 정보를 안전하게 보호하고 있는가?
⑦ 시스템 기록들이 Privacy Act. 하에서 생성되었는가?

위의 내용들을 평가하는 절차는 [표 2]와 같다.

국내에서도 행정안전부가 금년 12월 23일, 롯데정보통신, 씨에이에스, 안철수연구소, 이글루시큐리티, 인포섹, 한국정보기술단 등 6개 기업을 최종 개인정보 영향평가기관으로 선정하고 고시하였다.

〔표 2〕 미국의 개인정보 영향 평가 절차

항목	내용
① 사전분석	프로젝트를 위해 영향평가가 필요한가?
② 평가시기 확정	프로젝트의 계획단계에서 프라이버시 영향평가를 언제 시행할 것인가?
③ 조직 및 사업개요 분석	현재 조직의 개인정보관리정책 현황 파악과 도입되는 새로운 사업 개요 분석
④ 정보흐름 분석	프로젝트 수행 시 정보 흐름에 대한 정확한 이해
⑤ 프라이버시 분석	정보의 수집에서부터 파기에 이르기까지 제안됨
⑥ 위험관리	위험을 평가하고, 그 특성과 심각성을 판단하여 개선계획안 마련
⑦ 영향평가 보고서 작성	영향평가 결과에 대한 최종보고서 작성 과정으로 일반인이 이해하기 쉽게 작성하여 공개

개인정보 영향평가기관 지정은 개인정보보호법 제33조 및 동법시행령 제37조·제38조에 따라 지정하는 것으로, 지정된 6개 기업은 2011년 12월 23일부터 2013년 12월 22일까지 개인정보 영향평가기관으로 2년간 유지된다[16].

V. 결 론

본고에서는 1974년 프라이버시법(Federal Privacy Act 1974)을 시작으로 해서 각 주단위로 규정된 프라이버시권 관련 법률들이 있는 미국의 개인정보보호 관련 법제 현황에 대해서 살펴보았다.

최근에 미국연방통상위원회(FTC)는 2011년 11월 30일 페이스북과 개인정보보호를 실행하는데 합의했다. 페이스북은 향후 20년간 보다 엄격한 조건으로 개인정보보호를 실행하기로 하였고 매년 독립적으로 개인정보보호를 위한 실행 평가를 받기로 하였다. FTC는 2011년 구글, 트위터로 인한 사생활 침해 문제 제기 등으로 인터넷 업체들과 개인 정보 보호법을 강화해 오고 있다[17].

미국의 경우에는 공공과 개인을 아울러서 총괄하는 법은 존재하지 않지만 다양한 영역별로 접근 방식을 택하여 세부적으로 공공, 금융, 통신, 교육, 의료, 비디오 감시, 근로자 정보 등 각 영역별로 제정하여 시행하고 있다. 우리나라의 경우에도 개인정보보호법이 발효되었지만 각 분야별 보호 방안에 대하여 추가적으로 구체적인 적인 노력들이 진행되어야 할 것으로 사료된다.

참고문헌

[1] 행정안전부, 개인정보 보호법, 법률 제10465호, 2011.3.29.

[2] 고려대학교, *주요 국가의 개인정보보호 동향 조사*, 한국인터넷진흥원 연구보고서, 2009.6.

[3] 법제자료, "공공부문에 관한 외국의 개인정보보호 법제와 국내 입법의 검토 방향", 2010.9.

[4] 양용석, "해외 개인정보보호 법과 제도 동향", 주간 기술동향 통권 1443호, pp.17~29, 2010.4.28

[5] 양용석, "해외 개인정보보호 관련법과 제도의 고찰 (4)", 보안뉴스, 2008.6.

[6] 성경원, "국내외 개인정보보호 법/규제 동향", IT DAILY, 2009.3.

[7] 한국인터넷진흥원, *개인정보 DB 암호화 관리 안내서*, 2010.1.

[8] 한국인터넷진흥원 "해외개인정보 보호기구 - 연방거래위원회(FTC)".

[9] 김유승, "인터넷 내용규제, 다른 나라는 어떻게?", 민중언론 참세상, 2010.9.

[10] Children's Online Privacy Protection Act of 1998, http://www.ftc.gov/ogc/coppa1.htm

[11] 이균성, "미국 통신 감청 강화 방안 논란 확산", 아이뉴스24, 2010.10.20.

[12] "United States Privacy Laws", http://www.informationshield.com/usprivacylaws.html

[13] 김민호, "개인정보 영향평가제도의 도입 및 추진 현황", 「개인정보 영향평가에 관한 고시」제정을 위한 공청회 자료집, 2011.7.11.

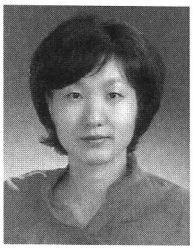
[14] 심미나, "개인정보보호 문화 정착과 체질 개선 위한 '첫 걸음마'", 보안뉴스, 2011.09.12.

[15] M-03-22 OMB Guidance for Implementing the Privacy Provisions of the E-Government ACT of 2002.12.

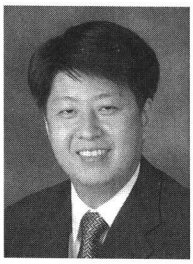
[16] 보안뉴스, "개인정보 영향평가기관 6개 기업 최종 확정", 2011.12.23.

[17] 임상수, "美서 13세미만 불법 페북가입 부모가 주로 도와", 연합뉴스, 2011.11.03.

〈著者紹介〉



전 은 정 (Eun-Jung JUN)
학생회원
2006년 8월 : 순천향대학교 정보보호학과 석사(공학석사)
2010년 3월~현재 : 순천향대학교 정보보호학과 박사과정
<관심분야> 개인정보보호



김 학 범 (Hak-Beom KIM)
정회원
1990년 8월 : 중앙대학교 대학원 전자계산학과 졸업(공학석사)
2001년 2월 : 아주대학교 대학원 컴퓨터공학과 졸업(공학박사)
1991년 10월~1996년 6월 : 한국전산원 주임연구원
1996년 7월~2001년 8월 : 한국정보보호진흥원 기술표준팀장
2001년 9월~2003년 1월 : (주)드림시큐리티 상무이사
2003년 2월~2005년 3월 : (주)장미디어인터렉티브 상무이사
2008년 4월~2009년 6월 : 인포섹(주) 수석컨설턴트
2009년 7월~2010년 12월 : 에스지에이(주) 연구소장
2001년 3월~2009년 2월 : 순천향대학교 정보보호학과 겸임교수
2005년 9월~현재 : 동국대학교 국제정보대학원 겸임교수
2011년 7월~현재 : 한국정보보호학회 이사
2011년 9월~현재 : (주)지엔에스인증원 ISMS본부장
<관심분야> ISO 27001, 클라우드 컴퓨팅 보안, 개인정보보호

염 흥 열 (Heung-Youl YOUM)
정회원
1981년 2월 : 한양대학교 전자공학과 학사 졸업
1983년 9월 : 한양대학교 대학원 전자공학과 석사 졸업
1990년 2월 : 한양대학교 전자공학과 박사 졸업
1982년 12월~1990년 9월 : 한국전자통신연구소 선임연구원
1990년 9월~현재 : 순천향대학교 정보보호학과 정교수
1997년 3월~2000년 3월 : 순천향대학교 산학연컨소시엄센터 소장
1997년 3월~현재 : 한국정보보호학회 총무이사, 학술이사, 교육이사, 논문지편집위원 위원장, 수석부회장(역), 학회장(현)
2005년~2008년 : ITU-T SG17 Q9 Rapporteur(역)
2006년 11월~2009년 2월 : 정보통신연구진흥원 정보보호전문위원
2009년 5월~현재 : 국정원 암호검증위원회 위원
2009년~현재 : ITU-T SG17 부의장/SG17 WP2 의장
<관심분야> 인터넷보안, USN 보안, IPTV 보안, 홈네트워크 보안, 암호 프로토콜