글로벌 법제전략 연구 13-22-④-2
글로벌 법제와 정책연구 | 정보통신

유럽연합(EU)의 잊힐 권리 법제화에 대한 평가와 전망

손 현

한국법제연구원
KOREA LEGISLATION RESEARCH INSTITUTE

글로벌 법제전략 연구 13-22-④-2

글로벌 법제와 정책연구	정보통신

유럽연합(EU)의 잊힐 권리 법제화에 대한 평가와 전망

손 현

한국법제연구원
KOREA LEGISLATION RESEARCH INSTITUTE

유럽연합(EU)의 잊힐 권리 법제화에 대한 평가와 전망

The Assessment and outlook of EU Legislation on the Right to be Forgotten

연구자 : 손 현(부연구위원)

Son, Hyun

2013. 9. 30.

한국법제연구원

KOREA LEGISLATION RESEARCH INSTITUTE

요 약 문

Ⅰ. 연구의 배경과 목적

□ 개인정보의 중요성에 대한 공감대는 전세계적으로 형성되고 있으며, 특히 EU는 2012년 1월 세계 최초로 정보주체가 온라인상에서 자신과 관련된 모든 정보에 대한 삭제 및 확산 방지를 요구할 수 있는 권리인 “잊힐 권리(Right to be forgotten)”를 법제화하는 등 개인정보보호 강화를 주요 내용으로 하는 일반정보보호규정(안) 및 개인정보보호지침(안)을 제안하고, 2014년 발효 예정에 있음.

□ EU의 이러한 법제화 움직임에 대해, EU 산하의 유럽네트워크정보보호원(ENISA, European Network and Information Security Agency)에서도 최근 관련 규정의 실효성 및 구체성에 대한 문제 제기와 함께 기술적 한계를 극복하기 위한 권고를 담은 평가 분석 리포트를 발표함.

□ ‘프라이버시 라운드’라는 말에서도 볼 수 있듯이 개인정보보호문제는 글로벌 웹 환경을 기반으로 하기 때문에 단순히 국내 문제로 한정할 수 없을 뿐만 아니라, 향후 국가간의 합의로 EU처럼 국제 규범화를 통해 국가간 공동 대응을 전제로 함.

□ 이러한 점에서 개인정보 정책과 관련한 글로벌 동향에 대한 조사·연구의 일환으로 EU의 일반 정보보호규정(안) 및 '잊힐 권리'에 관한 주요 규정 및 최근 미국의 개인정보 보호 정책 동향에 대한 소개를 통하여 바람직한 국제 통일 규범화 방향을 모색함.

Ⅱ. 주요 내용

□ EU의 일반정보보호규정(안)의 주요 내용

○ EU 일반정보보호규정(안)은 개인정보의 처리에 관한 개인의 보호와 관련한 규범과 개인 정보의 자유로운 이동에 관한 규범을 정함을 목적으로 전체 11장 91조로 구성되어 있음.

○ 제1장 일반 규정, 제2장 개인정보 처리의 원칙, 제3장 정보주체의 권리, 제4장 관리자 및 처리자, 제5장 제3국 또는 국제기구로의 개인 정보 전송, 제6장 독립적 감독기관, 제7장 협력 및 일관성, 제8장 구제, 책임 및 제재, 제9장 정보 처리 상황 관련 규정, 제10장 위임 입법 및 실행 법령, 제11장 부칙상의 주요 내용을 소개함.

□ 잊힐 권리에 관한 규정(안)의 내용

○ 잊힐 권리 및 삭제권(Right to be forgotten and to erasure)은 일반정보보호규정(안) 제17조에 규정되어 있으며, 정보주체는 개인정보처리자를 대상으로 자신의 개인정보의 삭제 및 확산 방지를 청구할 수 있는 권리를 가짐.

○ 그 외 개인정보 공개시의 책임, 적용예외, 개인정보 처리의 제한, 위임 입법 권한에 관한 구체적인 내용을 담고 있음.

□ EU의 '잊힐 권리' 법제화에 관한 ENISA의 평가

○ ENISA는 잊힐 권리의 실현 가능성과 관련하여 EU 규정(안)에는 개인정보의 범위, 데이터 삭제 요청 권리자의 범위, 잊혀질 데이터의 항목 등이 명확하게 제시되어 있지 않다는 문제를 제기함.

○ 이에 개인정보는 한번 공개되고 나면 기술적 수단만으로는 '잊힐 권리'의 실현이 불가능하기 때문에 기술적·법적 조치가 동시에 필요하며 이를 위해 권고사항을 제안함.

□ 미국의 개인정보보호 정책 관련 최신 동향

○ 소비자 프라이버시 권리장전의 주요 내용 소개

- 개인정보통제
- 사생활보호 및 보안정책의 공개
- 개인정보 제공 목적에 부합하는 수집·이용·공개
- 개인정보의 적절한 관리
- 개인정보의 접근가능성 및 정확성
- 필요한 정보만을 수집
- 책임성

○ FTC의 프라이버시 정책 프레임 워크 및 실행 권고

- 최종 범위

- 디자인에 의한 프라이버시
- 소비자 선택의 단순화
- 투명성
- 입법적 권고
- 5개 영역에서의 이행 지원(추적 방지, 모바일, 데이터 프로커, 대형 플랫폼 제공자, 강제 집행력 있는 자율 규제 강령의 촉진)

Ⅲ. 기대효과

□ 개인정보보호 정책 및 입법에 관한 최근 국제 사회의 논의 동향을 국내에 소개함으로써 향후 개인정보의 국외 이전 등의 문제에 대비하여 국제 수준의 개인정보보호 정책 및 입법 방향 모색에 기여함.

주제어 : 잊힐 권리, EU 일반정보보호규정, 미국 소비자프라이버시 권리장전, 프라이버시, 개인정보

Abstract

Ⅰ. Background and Objectives

□ World-wide consensus about the importance of privacy has been formed, in particular, EU suggested EU General Data Protection Regulation and EU Data Protection Directive including “the Right to be Forgotten” which granted the data subject to request deleting or avoiding the possibility of spreading all the related information about himself/herself.

□ According to the movement of EU legislation, ENISA(European Network and Information Security Agency) published an assessment report including questions on the effectiveness and the details of the provisions, and recommendations to overcome the technical limitations.

□ The word 'Privacy round’ implies that privacy issues based on the global web environment should be dealt by international norm not by domestic legislation.

□ This study introduces the proposed EU General Data Protection Regulation and main provisions on “the Right to be Forgotten”, and the recent trends of privacy policies in the United States, as part of the research on privacy policies and related global trends.

Ⅱ. Main Contents

□ Main Contents of the proposed EU General Data Protection Regulation

o It aims to treat rules on an individual's personal information protection and the free movement of personal data. It consists of 11 chapters and 91 provisions.

o This study introduces summaries of: General Provisions(Chapter 1), Principles of Data Processing(Chapter 2), Rights of the Data Subject (Chapter 3), Controller and Processor(Chapter 4), Transfer of Personal Data to Third Countries or International Organizations(Chapter 5), Independent Supervisory Authorities (Chapter 6), Co-operation and Consistency(Chapter 7), Remedies, Liability and Sanctions (Chapter 8), Provisions relating to Specific Data Processing Situations (Chapter 9), Delegated Acts and Implementing Acts (Chapter 10), and Final Provisions (Chapter 11).

□ Main Contents of “Right to be Forgotten”

o Right to be Forgotten and to erasure are provided in the article 17 of the General Data Protection Regulation, data subjects have the right to be forgotten to request data processors to delete or avoid the spreading of their personal data.

o It includes the liability due to the personal data disclosure, exemptions, limitations on data processing, and so on.

□ Assessment on EU legislation of “Right to be Forgotten”

o ENISA challenged that provisions such as the scope of personal data, the scope of erasure right holders were not clearly defined.

o It recommended that technical and legal protection would be needed because the “Right to be Forgotten” is hardly implemented after disclosure.

□ Recent Privacy Policy Trends in the US

o It introduces main contents of Consumer Privacy Bill of Rights:

- Individual Control on personal data
- Transparency on Policy of privacy and security
- Collect · Use · Disclosure of personal data respect for context
- Proper security
- Access and Accuracy of personal data
- Focused Collection
- Accountability

o Privacy Policy Framework and implementation Recommendation of FTC

- Final Scope
- Privacy by Design
- Simplification of Consumer Choice

- Transparency

- Legislative Recommendation

Ⅲ. Expected Effect

□ As introducing international trends of privacy policies and legislations, it contributes to give directions to national legislation responding to international transfer of personal data.

Key Words : the Right to be Forgotten, EU General Data Protection Regulation, Consumer Privacy Bill of Rights, Privacy, Personal Data

목 차

제 1 장 서 론

제 1 절 연구의 목적

소셜 네트워크 서비스(SNS)·클라우드 서비스의 이용 증가, 검색 기술 등 ICT 기술의 발전, 빅 데이터(Big Data)의 활용 증가 등으로 인해 글로벌 웹기반의 온라인 공간에 대한 개인정보 및 프라이버시 침해 문제가 전 세계적인 이슈가 되고 있다.

이러한 시점에서 EU는 2012년 1월 세계 최초로 정보주체가 온라인상에서 자신과 관련된 모든 정보에 대한 삭제 및 확산 방지를 요구할 수 있는 권리인 "잊힐 권리(Right to be forgotten)[1)]"를 법제화하는 등 개인정보보호 강화를 주요 내용으로 하는 일반정보보호규정(안) 및 개인정보보호지침(안)을 제안하고, 2014년 발효 예정에 있다. EU의 이러한 법제화 움직임에 대해, EU 산하의 유럽네트워크정보보호원(ENISA, European Network and Information Security Agency)[2)]에서도 최근 관련 규정의 실효성 및 구체성에 대한 문제 제기와 함께 기술적 한계를 극복하기 위한 권고를 담은 평가 분석 리포트를 발표하기도 하였다. 또한 구글, 페이스북 등 다국적 인터넷 기업은 정보삭제 청구와 관련한 향후 소송에 대한 영향을 분석하는 등 전·세계적인 관심이 고조되고 있다. 우리나라의 경우도 방송통신위원회 등 정부부처를 중심으로 '잊힐 권리' 법제화 방안에 대한 논의가 활발해지고 있다.

"잊힐 권리"는 이를 새로운 독자적 권리로 인정할 수 있을 것인가에 대한 원론적인 논의부터, 표현 및 언론의 자유, 프라이버시 및 인

1) 국내에서는 'right to be forgotten'을 '잊혀질 권리'로 번역·사용되고 있으나, 국어 맞춤법 표기상 '잊히다'를 활용한 '잊힐 권리'가 맞는 표현으로 본 보고서에서는 '잊힐 권리'라는 표현을 사용한다.

2) 사이버 범죄와 관련된 유럽 각국의 정보가 효과적으로 공유될 수 있도록 조정하고, 사이버 범죄에 효과적으로 대응하기 위한 정책개발을 위해 정보 통신망 및 정보보호 안전에 관한 전문가들로 구성된 기관((http://ww.enisa.europa.eu)

격권 보호 등 개인정보의 이용과 보호라는 양립할 수 없는 두 이념적 가치를 어떻게 균형·조화롭게 제도화 할 수 있는가의 문제 등 쉽지 않은 난제를 전제로 하고 있다. 또한 구체적으로 “사망한 자의 정보의 공개를 허용할 것인지의 문제에서 시작하여 사망한 자에 관한 정보를 적극적으로 어떻게 처리할 것인지의 문제(소위, 디지털 유산의 문제), 현재 살아있는 자에 관한 개인정보의 삭제를 청구할 수 있는지에 대한 문제(개인정보자기결정권의 문제), 언론에 게재된 개인에 관한 기사의 삭제를 청구할 수 있는가의 문제(기사삭제요구권의 문제), 또는 인터넷 게시판에 게시된 타인의 글에 대한 삭제를 청구할 수 있는가의 문제(게시글 삭제 요구권의 문제)”[3]의 해결을 필요로 한다.

‘프라이버시 라운드’라는 말에서도 볼 수 있듯이 개인정보보호문제는 글로벌 웹 환경을 기반으로 하기 때문에 단순히 국내 문제로 한정할 수 없을 뿐만 아니라, 향후 국가 간의 합의로 EU처럼 국제 규범화를 통해 국가간 공동 대응을 전제로 한다. 이에 본 연구는 EU의 일반 정보보호규정(안) 및 ‘잊힐 권리’에 관한 주요 규정 내용에 대한 분석과 평가, 미국의 최근 개인정보보호 정책 동향 분석 등을 바탕으로 하여, 개인정보보호 및 ‘잊힐 권리’에 대한 바람직한 국제 통일 규범화 방향을 모색함을 목적으로 한다.

제 2 절 연구의 범위 및 방법

본 연구는 EU의 일반 정보보호규정 및 ‘잊힐 권리’에 관한 주요 규정 내용과 이러한 EU의 ‘잊힐 권리’ 법제화 움직임 이후에 나온 각종 평가 보고서의 분석에 기초한다. 또한 ‘잊힐 권리’를 둘러싼 각종 법적 이슈, 개인정보보호와 관련한 ‘온라인 프라이버시 프레임워크’

3) 이에 대한 문제제기는 최경진, “잊혀질 권리 - 개인정보 관점에서”, 정보법학 제16권 제2호, 2012; 한국정보화진흥원, “‘잊혀질 권리’의 법적 쟁점과 개선 방향”, 법제연구 2012-10. 2012 참조.

등 최근 미국 정부 등에서 나온 보고서 등을 통해 '잊힐 권리' 법제화를 위한 국제 통일 규범화 방향을 모색해본다. 주요 분석 대상 Paper는 다음과 같다.

o Proposal for a 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)

o Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data

o ENISA, "The right to be forgotten - between expectation and practice", 2012.11.20.(http://www.enisa.europa.eu)

o THE WHITE HOUSE, Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy, 2012.1

o FTC, "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers", 2012.3.(http://www.ftc.gov/opa/2012/03/privacyframework.shtm)

o 기타 국・내외 문헌

제 2 장 유럽연합(EU)의 '잊힐 권리'에 관한 주요 내용 분석 및 평가

제 1 절 배경 및 의미

최근 2011년 7월 6일에 유럽의회가 "유럽연합에서의 개인정보보보에 관한 종합적 접근"을 의결하면서 잊힐 권리의 입법 필요성을 강조하였다. 이러한 잊힐 권리의 내용은 2012년 1월 25일 EU 일반정보보호규정(안) 및 개인정보보보지침(안)을 발표하면서 구체적으로 드러나게 되었다. EU 차원의 개인정보보호를 위한 입법 노력은 1995년 EU가 개인정보보호지침을 제정한 이후 16년 만의 일로 이번 입법 발표에서 주목할 만한 점은 지침의 전면 개정에 머물지 않고, EU 회원국의 국내에 직접 법적 효과가 발생하는 규정(regulation)을 함께 추진한다는 점이다. EU 법체계하에서 규정은 회원국이 자국의 사정에 맞게 국내법으로 전환을 해야 하는 유럽연합의 지침(Directive)와 달리 회원국 국내법으로의 전환 없이 곧바로 회원국에 적용되는 매우 강력한 규범이다. 다만, 개정안이 발효되려면 27개 회원국 정부 대표로 구성된 이사회와 유럽의회의 승인을 받아야 한다. 이법 입법안이 통과되면 2014년 발효를 목표로 하고 있다.[4)]

제 2 절 EU의 일반정보보호규정(안)의 주요 내용

1. 구 성

EU 일반정보보호규정(안)은 개인정보의 처리에 관한 개인의 보호와 관련한 규범과 개인 정보의 자유로운 이동에 관한 규범을 정함을 목

4) 최경진, "'잊혀질 권리'에 관한 해외 법제 동향", 잊혀질 권리와 디지털 자유 대토론회 자료집, p.21

적으로 전체 11장 91조로 구성되어 있다. 제1장 일반 규정(제1조 목적, 제2조 물적 적용범위, 제3조 영역적 적용범위, 제4조 정의), 제2장 원칙(제5조 개인정보 처리의 원칙, 제6조 처리의 합법성, 제7조 동의의 조건, 제8조 아동의 개인정보의 처리, 제9조 특정한 범주의 개인정보의 처리, 제10조 식별을 허용하지 않는 처리), 제3장 정보주체의 권리(제11조 투명한 정보와 통신, 제12조 정보주체의 권리 행사의 절차 및 체계, 제13조 수령인 관련 권리, 제14조 정보 주체에 대한 정보, 제15조 정보 주체의 접근권, 제16조 수정할 권리, 제17조 잊힐 권리와 삭제할 권리, 제18조 정보 이동에 관한 권리, 제19조 반대할 권리, 제20조 프로파일링에 근거한 조치, 제21조 제한), 제4장 관리자 및 처리자(제22조 관리자의 책임, 제23조 고정적·계획적 정보 보호, 제24조 공동관리자, 제25조 유럽연합 내 고용되지 않은 관리자의 대표, 제26조 처리자, 제27조 관리자와 처리자의 권한 내 처리, 제28조 문서화, 제29조 감독기관과의 협력, 제30조 처리의 보안, 제31조 감독기관에의 개인 정보 의무 위반 통지, 제32조 정보주체에의 개인정보 의무 위반 통지, 제33조 정보보호 영향 평가, 제34조 사전 승인 및 사전 자문, 제35조 정보보호 담당관의 지정, 제36조 정보보호 담당관의 지위, 제37조 정보보호 담당관의 임부, 제38조 행동 강령 및 인증, 제39조 인증), 제5장 제3국 또는 국제기구로의 개인 정보 전송(제40조 전송의 일반 원칙, 제41조 적절한 결정에 따른 전송, 제42조 적절한 안전책에 따른 전송, 제43조 구속력있는 기업 규정에 의한 전송, 제44조 수정, 제45조 개인정보 보호를 위한 국제 협력), 제6장 독립적 감독기관(제46조 감독기관, 제47조 독립성, 제48조 감독기관 구성원의 일반적 조건, 제49조 감독기관 설립의 원칙, 제50조 직업적 비밀 유지, 제51조 권능(competence), 제52조 의무, 제53조 권한, 제54조 활동보고), 제7장 협력 및 일관성(제55조 상호지원, 제56조 감독기관의 공동 수행, 제57조 일관성 체계, 제58조 유럽 정보위원회의 의견, 제59조 유럽위원회

의 의견, 제60조 조치 초안의 중지, 제61조 긴급 절차, 제62조 실행 법령, 제63조 집행, 제64조 유럽 정보보호위원회, 제65조 독립성, 제66조 유럽 정보보호위원회의 임부, 제67조 보고서, 제68조 절차, 제69조 위원장, 제70조 위원장의 임무, 제71조 사무국, 제72조 기밀유지), 제8장 구제, 책임 및 제재(제73조 감독기관에 이의를 제기할 권리, 제74조 감독기관을 상대로 한 사법적 구제를 받을 권리, 제75조 관리자 및 처리자를 상대로 한 사법적 구제를 받을 권리, 제76조 법원 절차에 관한 공통 규칙, 제77조 배상을 받을 권리 및 책임, 제78조 벌칙, 제79조 행정적 제재), 제9장 정보 처리 상황 관련 규정(제80조 개인정보의 처리와 표현의 자유, 제81조 건강 관련 개인정보의 처리, 제82조 고용관계 내의 처리, 제83조 역사적, 통계적 그리고 과학적 목적의 처리, 제84조 기밀 유지 의무, 제85조 교회 및 종교적 단체의 기존 정보보호 규칙), 제10장 위임 입법 및 실행 법령(제86조 위임의 실행, 제87조 위원회 절차, 제88조 지침 95/46/EC의 폐지, 제89조 지침 2002/58/EC와의 관계 및 의의 개정, 제90조 평가, 제91조 시행 및 적용) 으로 규정되어 있다.

한편, EU 개인정보보호지침(안)은 형사범죄의 예방, 조사, 수사와 기소 또는 형사벌칙금의 집행을 목적으로 하는 적법기관에 의한 개인정보의 처리와 관련하여 개인의 보호에 관한 규범을 정함을 목적으로 한 지침으로 총 9장 64조로 구성되어 있다. 제1장 총칙(제1조 목적, 제2조 적용범위, 제3조 용어의 정의), 제2장 원칙(제4조 개인정보 처리 원칙, 제5조 다양한 범주의 정보 주체간의 구별, 제6조 개인정보의 정확성과 신뢰성의 상이한 정도, 제7조 처리의 적법성, 제8조 특정한 범주의 개인정보 처리, 제9조 프로파일링이나 자동화된 처리에 근거를 둔 조치) 제3장 정보주체의 권리(제10조 정보주체의 권리를 실행하는 형식, 제11조 정보주체에 관한 정보, 제12조 정보주체를 위한 접근권, 제13조 접근권에 대한 제한, 제14조 접근권 실행을 위한 형식, 제15조

수정에 대한 권리, 제16조 삭제에 대한 권리, 제17조 형사조사와 절차 진행 중의 정보주체의 권리), 제4장 관리자와 처리자(제18조 관리자의 책임, 제19조 디자인과 초기설정에 의한 정보보호, 제20조 공동 관리자, 제21조 처리자, 제22조 관리자와 처리자 승인하의 처리, 제23조 문서화, 제24조 기록의 보존, 제25조 감독기관과의 협력, 제26조 감독기관의 사전협의, 제27조 처리 보안, 제28조 감독기관에 대한 개인정보 침해의 고지, 제29조 정보주체에 대한 개인정보 침해의 통보, 제30조 정보보호 담당자의 지정, 제31조 정보보호 담당자의 지위, 제32조 정보보호 담당자의 임부), 제5장 개인저보의 제3국 또는 국제기구로의 이전(제33조 개인정보의 이전을 위한 일반 원칙, 제34조 정확성 결정에 따른 이전, 제35조 적절한 보호조치에 의한 이전, 제36조 일탈, 제37조 개인정보 이전을 위한 구체적 조건, 제38조 개인정보보호를 위한 국제적 협력), 제6장 독립 감독기관(제39조 감독기관, 제40조 독립, 제41조 감독기관의 구성원을 위한 일반 조건, 제42조 감독기관의 설치에 관한 규칙, 제43조 직업상 비밀 유지, 제44조 권능, 제45조 의무, 제46조 권한, 제47조 활동보고서), 제7장 협조(제48조 상호지원, 제49조 유럽 정보보호위원회의 임무), 제8장 구제, 책임 그리고 제재(제50조 감독기관에 관한 불만제기 권리, 제51조 감독기관을 상대로 한 사법구제에 관한 권리, 제52조 관리자와 처리자에 대한 사법규제 권리, 제53조 법적 절차에 대한 일반 규칙, 제54조 책임과 보상에 대한 권리, 제55조 범칙금), 제9장 대리행위와 시행(제56조 대리의 실행, 제57조 위원회 절차, 제58조 폐기, 제59조 형사사건의 사법협조와 경찰협조를 위한 유럽연합의 이미 채택된 법령관의 관계, 제60조 형사문제에 관한 사법협조와 경찰협조 분야에 있어서 이미 체결된 국제 협정과의 관계, 제61조 평가, 제62조 이행, 제63조 발효와 적용, 제64조 수령인)이다.

2. 주요 내용

(1) 일반 규정(총칙)

제1조는 지침 95/46/EC 제1조와 같이 이 규정의 두 가지 목적을 규정한다. 제2조 및 제3조는 각각 이 규정의 물적 적용범위, 영역적 적용범위에 관하여 규정하고 있다. 제4조는 이 규정에서 사용된 용어를 정의하고 있는데, 일부 정의는 지침 95/46/EC에서 차용하고, 일부 용어는 기존의 정의를 개정하거나 부수적 요건을 추가하여 또는 새롭게 정의하고 있다. e-프라이버시 지침 2002/58/EC[5] 제2조 제h호에 근거한 '개인 정보의 의무불이행(personal data breach)'은 지침 2009/136/EC[6]의 개정에 의한 것이고, '유전 정보(genetic data)', '생체 정보(biometric data)', '건강 관련 정보(data concerning health)', '주요 근거지(main establishment)', '대표(representative)', '경제 주체(enterprise)', '활동(group of undertakings)', '구속력 있는 기업 규정(binding corporate rules)', 그리고 UN 아동권 협약에 근거한 '아동(child)', '감독기관(supervisory authority)' 등에 대한 용어 정의가 있다. '동의(consent)'를 정의함에 있

5) 전기 통신 부문에서의 개인 데이터 처리 및 프라이버시 보호에 관한 2002년 7월 12일 유럽의회 및 이사회 지침 2002/58/EC (Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)), OJ L 201, 31/07/2002, p. 37.

6) 소비자 보호 법령상의 국가별 책임 부처간 협력에 관한 규칙 (EC) 2006/2004 및 전기 통신 부문 내 개인 데이터의 처리 및 프라이버시 보호에 관한 지침 2002/58/EC, 국가별 전기 통신 네트워크 및 서비스 관련 보편적 서비스와 이용자 권리에 관한 지침 2002/22/EC의 개정을 위한 2009년 11월 25일 유럽의회 및 이사회 지침 2009/136/EC (Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users'' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws Text with EEA relevance); OJ L 337 , 18.12.2009, p. 11.

어서는, '모호하지 않은' 동의와의 혼동을 피하고, 정보 주체의 인지를 보장하기 위한 단일한 정의를 위하여 '명시적인'이라는 표현이 추가되었다.

(2) 개인정보 처리의 원칙

제5조는 지침 95/46/EC 제6조에 규정된 원칙에 부합하는 것으로, 개인 정보의 처리에 관한 원칙들을 규정하고 있다. 새로이 추가된 요소로는 투명성의 원칙, 개인정보처리자의 포괄적 책임, 개인 정보 최소화 원칙의 명확화 등이 있다. 제6조는 지침 95/46/EC 제7조에 따라, 이익형량 및 법적 의무의 준수, 공익을 고려한 합법적 처리의 기준을 규정하고 있다. 제7조는 합법적 처리의 법적 근거로서 유효한 동의의 조건을 규정한다. 제8조는 아동에게 제공된 정보 사회 서비스와 관련하여 아동 개인 데이터의 합법적 처리 조건을 규정한다. 제9조는 지침 95/46/EC 제8조에 따라 특정 유형의 개인 정보 처리에 관한 일반적 금지 및 이러한 규칙의 예외를 규정한다. 제10조는 개인정보처리자가 단지 이 규칙을 준수할 목적으로 정보 주체를 확인하는데 필요한 부수적 정보를 획득할 의무는 부담하지 않음을 명시한다.

(3) 정보주체의 권리

1) 투명성 및 세부 원칙

제11조는 개인 정보 및 프라이버시 보호 국제 기준에 관한 마드리드 해결(the Madrid Resolution)[7]에 따라, 개인정보처리자에게 정보의 투명성, 접근 용이성, 그리고 이해가능성을 제공할 의무를 부여한다. 제12조는 전자적 요청 수단을 포함하여, 만료 기간 내 정보 주체의 요청에 답변할 것, 거부가 가능하도록 할 것 등 정보 주체의 권리 실

7) 2009년 11월 5일 개최된 정보 보호 및 프라이버시 위원회 국제 컨퍼런스에서 채택되었다. 유럽 일반 매매법에 관한 규칙안 제13조 제3항 참조(COM(2011)635final).

현을 위하여 개인정보처리자가 절차와 체계를 마련해야 한다는 의무를 부여한다. 제13조는 지침 95/46/EC에 근거하여, 수령인의 범위를 공동 통제자 및 처리자를 포함한 모든 수령인으로 확대한다.

2) 정보에의 접근

제14조는 지침 95/46/EC 제10조 및 제11조에 따라, 국제 전송 및 근원지와 관련하여, 보관 기간, 이의를 제기할 권리를 포함한 정보 주체에 대한 개인정보처리자의 정보 의무를 구체화한다. 여기에는 지침 95/46/EC의 변경이 가능하다. 기록 또는 공개가 법률에 의하여 명시적으로 규정된 경우 위와 같은 의무를 지지 않는다. 예를 들면 경쟁 관련 부처, 조세 또는 관세 행정, 또는 사회 보장 서비스 등에 의한 절차가 있다. 제15조는 지침 95/46/EC 제12조 제a호에 따라 정보 주체가 자신의 정보에 접근할 권리, 그리고 보관 기간, 수정・삭제・이의를 제기할 수 있는 권리에 대한 통지 등을 새로이 추가하여 규정하고 있다.

3) 수정 및 삭제

제16조는 지침 95/46/EC 제12조 제b호에 따른 정보 주체의 수정 권리를 규정한다. 제17조는 정보 주체의 잊힐 권리와 삭제권을 규정한다. 이는 지침 95/46/EC 제12조 제b호에 규정된 삭제권을 보다 상세화하고 특정한 것으로, 정보 주체가 자신의 개인 정보에의 링크, 복사 또는 복제를 요청한 경우 발생하는 개인정보처리자의 의무를 포함하여 잊힐 권리의 요건을 규정하고 있다. 이 조항은 또한 “블로킹”이라는 모호한 단어 정의를 피하기 위해 특정한 사례 내로 제한된 처리에 관한 권리를 통합하고 있다. 제18조는 정보 주체가 개인정보처리자의 간섭 없이 정보를 하나의 전자 처리 시스템으로부터 다른 전자 시스템으로 전송할 수 있다는 정보 이동성 (portability)을 규정한다. 이에 대한 전제 조건으로, 그리고 자신의 정보에 대한 접근을 개선하기 위

하여 이 조항은 개인정보처리자로부터 구조화되고 통상적으로 사용되는 전자적 형태로 이루어진 정보를 획득할 수 있는 권리도 규정하고 있다.

4) 반대할 권리 및 정보 수집

제19조는 정보 주체의 반대할 권리를 규정한다. 이 조항은, 입증책임 및 직접적 마케팅에의 적용을 포함한 일부 변경에 관한 지침 95/46/EC 제14조에 근거를 둔다. 제20조는 정보 주체가 정보 수집(profiling)에 기인한 조치의 대상이 되지 않을 권리를 규정한다. 이 조항은 자동화된 개인의 결정에 관한 지침 95/46 제15조 제1항을 수정하고 안전책을 추가하였으며, 정보 수집에 관한 유럽이사회의 권고에 따른 것이다.

5) 제 한

제21조는 유럽 연합 또는 회원국이 제5조에 따른 원칙, 제11조 내지 제22조, 그리고 제32조에 규정된 정보 주체의 권리에 대한 제한을 유지하거나 설정할 권한을 명확히 하고 있다. 이 조항은 지침 95/46/EC 제13조에 따라, 유럽 인권 법원 및 EU 법원이 해석한 바와 같이, 기본권 헌장과 인권 및 기본적 자유 보호에 관한 유럽 협약에 따른 요건에 근거를 둔다.

(4) 관리자 및 처리자

1) 일반 의무

제22조는 "책임성의 원칙"에 대한 논의를 고려하여 이 규칙을 준수하기 위한 관리자의 책임 의무를 상세화하고, 내부 정책의 채택 및 이 규칙을 준수를 확보하기 위한 체계 마련 등을 포함한 준수 수단을 열거하고 있다. 제23조는 데이터의 계획적(by design)·자동적(by default)

보호 원칙에 따른 관리자의 의무를 규정한다. 제24조는 공동 관리자의 내부적 관계 및 정보 주체와의 관계에 있어 책임을 명확화한다. 제25조는 유럽 연합 내 설립 기반을 두지 않은 관리자들이 처리 활동을 함에 있어 이 규칙의 적용을 받는 경우, 특정 조건 하에서 유럽 연합 내에 대표를 지정해야 할 의무를 부여한다. 제26조는 지침 95/46/EC 제17조 제2항에 부분적 근거를 두고, 관리자의 지시 범위 내에 속하지 않으면서 정보의 처리를 행하는 처리자를 공동 관리자로 보는 등 새로운 요소를 추가한 처리자의 지위 및 의무를 규정하고 있다. 제27조는 지침 95/46/EC 제16조에 따라 관리자 및 처리자의 권한 하에 이루어진 처리에 관하여 규정한다. 제28조는 지침 95/46/EC 제18조 제1항 및 제19조에 규정된 감독기관에의 일반적 통지 의무 대신, 관리자와 처리자가 그들의 책임 하에 처리 운영 문서를 보관할 의무를 규정한다. 제29조는 관리자 및 처리자의 감독기관에의 협조 의무를 규정한다.

2) 정보 보안

제30조는 지침 95/46/EC 제17조 제1항에 따라, 관리자 및 처리자가 처리 보안을 위한 적절한 조치를 취해야 한다고 규정하며, 처리자는 관리자와 계약과 관계없이 이러한 조치를 취해야 하는 것으로 의무를 확대한다. 제31조와 제32조는 e-프라이버시 지침 2002/58/EC 제4조 제3항의 개인 정보 의무불이행 통지 규정에 따라, 개인 정보 의무불이행 통지 의무를 규정한다.

3) 정보 보호 영향 평가 및 사전 승인

제33조는 관리자 및 처리자에게 위험한 처리를 행하기 전 정보 보호 영향 평가를 수행할 것을 의무화하고 있다. 제34조는 지침 95/46/EC 제20조의 사전 확인 개념을 근거로, 처리 전 의무적으로 감독기관의 자문과 사전 승인이 이루어져야 하는 경우를 규정한다.

4) 정보보호 담당관

제35조는 공공 부문, 민간 부문, 그리고 규모가 큰 경제 주체에 대하여, 정기적·체계적으로 모니터링이 요구되는 처리 활동을 수행하는 관리자 또는 처리자의 핵심적 활동에 관한 의무적 정보 보호 담당관을 두어야 한다고 규정한다. 이 조항은 일반 통지 요건을 대신하여 회원국이 위와 같은 요건을 정할 수 있음을 규정한 지침 95/46/EC 제18조 제2항에 따른 것이다. 제36조는 정보 보호 담당관의 지위를 규정한다. 제37조는 정보 보호 담당관의 주요 임무를 규정한다.

5) 행위 규범 및 인증

제38조는 지침 95/46/EC 제27조 제1항의 개념에 따라, 규범의 내용과 절차를 명확히 하고 유럽위원회에게 행위규범의 일반적 유효성을 결정할 수 있는 권한을 부여한다. 제39조는 정보보호의 인증 체계, 씰 및 인증마크 제도를 도입할 수 있음을 규정한다.

(5) 제3국 또는 국제기구로의 개인 정보 전송

제40조는 미래의 전송을 포함하여, 개인 정보의 제3국 또는 국제 기구에의 전송에 관한 의무 이행을 일반 원칙으로 명시하고 있다. 제41조는 지침 95/46/EC 제25조에 따라, 유럽위원회의 적절성 결정을 채택하기 위한 기준, 조건 및 절차를 규정한다. 유럽위원회의 보호 수준에 대한 적절성 평가에서 고려되어야 할 기준에는 법치주의, 사법적 공평 및 독립적 감독이 명시적으로 포함된다. 이 조항은 유럽위원회가 제3국 내 처리 부문 또는 지역별로 유지되는 보호의 수준을 평가할수 있는 가능성을 명확히 확인하고 있다. 제42조는 유럽위원회가 적절성 결정을 채택하고 있지 않은 경우, 제3국에의 전송에 있어, 적절한 안전책, 특히 표준 정보 보호 조항, 구속력있는 기업 규정 및 계약 조항

등을 추가할 것을 요구한다. 유럽위원회의 표준 정보 보호 조항의 활용 가능성은 지침 95/46/EC 제26조 제4항에 근거한다. 새로운 요소로서, 이러한 표준 정보 보호 조항은 감독기관에 의해 채택될 수도 있으며, 유럽위원회가 일반적 유효성을 선언할 수도 있다. 구속력있는 기업 규정은 법적 문맥에 따라 특별히 언급되고 있다. 계약 조항은 관리자 및 처리자에게 일정한 유연성을 부여하나, 감독기관의 사전 승인 대상이 된다. 제43조는 현재의 관행 및 감독기관의 요건에 따라, 구속력있는 기업 규정에 의해 전송되는 세부 조건을 규정한다. 제44조는 지침 95/46/EC 제26조의 규정에 따라 정보 전송에 관한 변경을 명시하고 있다. 이 조항은 경쟁 관련 부처, 조세 또는 관세 행정, 사회 보장 서비스 또는 어수면 관리 등과 같이 특별히 공익을 중요한 이유로 보호가 요청되거나 필요한 정보 전송에 적용된다. 또한, 정보 전송은 제한된 상황 하에서 관리자 또는 처리자의 합법적 이익을 위하여 정당화될 수 있으나, 이는 그러한 전송이 발생하게 된 상황을 평가 및 문서화한 이후에만 가능하다. 제45조는 유럽위원회와 제3국의 감독기관과의 개인 정보 보호에 관한 국제 공조 체계, 특히 보호의 적절한 수준 마련, 2007년 6월 12일 프라이버시 보호 법령의 시행에 따른 국경간 협력에 관한 OECD 권고의 고려 등을 명시적으로 규정한다.

(6) 독립적 감독기관

1) 독립적 지위

제46조는 지침 95/46/EC 제28조 제1항에 따라 회원국이 독립기관을 설립하여야 하며, 각 회원국 및 유럽위원회와의 공조를 위하여 그 업무를 확대할 것을 규정하고 있다. 제47조는 유럽연합 법원에 의한 판례법과 EC 규정 45/2001 제44조에 따라, 감독기관의 독립성 확보를 위한 조건을 명확히 하고 있다. 제48조는 EC 규정 45/2001 제42조 제

2항 내지 제6항 및 관련 판례법에 따라, 감독기관의 구성원에 관한 일반 조건을 규정한다. 제49조는 회원국이 법률에 따라 행할 감독기관의 설치에 관한 규칙을 규정한다. 제50조는 지침 95/46/EC 제28조 제7항에 따라 감독기관의 구성원·직원의 직업적 비밀 유지에 관하여 규정한다.

2) 의무 및 권한

제51조는 감독기관의 권한을 규정한다. 이 일반적 원칙은, 지침 95/46/EC 제28조 제6항(각 회원국의 내부 권한)에 따라, 적용의 단일성 보장을 위해 관리자 및 처리자에 대한 주무기관으로서의 권한을 갖는다. 각 회원국의 사법기관은 그 사법적 권한을 행사함에 있어 감독기관의 모니터링을 받지 않으나 데이터 보호에 관한 실질적 규칙의 적용의 대상에는 포함된다. 제52조는 공공의 위험, 규정, 안전책 및 권리에 대한 인식 제고, 이의 제기로 인한 청문회 및 조사 등을 포함한 감독기관의 의무를 규정한다. 제53조는 EC 규정 45/2001 제47조 및 지침 95/46/EC 제28조 제3항에 부분적으로 근거를 두고, 행정적 범죄에 대한 제재 권한을 포함한 새로운 요소를 추가하였다. 제54조는 지침 95/46/EC 제28조 제5항에 따라, 감독기관에게 연간 활동 보고서를 작성할 의무를 부여한다.

(7) 협력 및 일관성

1) 협 력

제55조는 지침 95/46/EC 제28조 제6항 제2목에 따라, 다른 감독기관의 요청 비준수로 인한 결과를 포함하여 의무적 상호 지원의 원칙을 명시하고 있다. 제56조는 유럽이사회 결정 2008/615/JHA 제17조에 따라, 감독기관의 공동 운영에의 참여권을 포함한 공동 운영에 관한 규칙을 규정한다.

2) 일관성

제57조는 일부 회원국내 정보 주체에 대한 처리 방안과 관련한 적용의 단일성 확보를 위해 일관성 확보 체계를 규정한다. 제58조는 유럽 정보 보호 위원회의 의견과 관련한 절차와 조건을 규정한다. 제59조는 일관성 체계 내에서 다룰 수 있는 사안으로, 유럽위원회가 유럽 정보 보호 위원회의 의견을 지지하거나 그와 다른 의견을 표명할 수 있는 사안, 그리고 감독기관의 초기 조치에 관한 사안을 규정한다. 제58조 제3항에 따라 유럽 정보 보호 위원회가 제기한 사항에 대하여는, 유럽위원회가 필요한 경우 그 재량을 행사하고 의견을 개진할 수 있다. 제60조는 이 규칙의 정확한 적용을 보장하기 위해 필요한 경우 유럽위원회의 결정으로 권한 기관에게 초기 조치의 중지를 요청할 수 있음을 규정한다. 제61조는 비상 절차로, 개별 조치의 채택이 가능함을 규정한다. 제62조는 일관성 체계에 따른 유럽위원회 이행 법령 요건을 규정한다. 제63조는 관련 모든 회원국 내 감독기관의 조치를 강화할 의무, 일관성 체계의 적용이 법적 유효성 및 향후 조치 집행을 위한 전제 조건임을 규정하고 있다.

3) 유럽정보보호위원회

제64조는 유럽 정보 보호를 감독하고, 각 회원국 감독기관의 수장인 유럽 정보 보호 위원회의 설립을 규정한다. 유럽 정보 보호 위원회는 지침 95/46/EC 제29조에 따라 설립된 개인 정보 처리 관련 개인 보호 실무반을 대체한다. 이 조항은 유럽위원회가 유럽 정보 보호 위원회의 구성원은 아니나, 그 활동에 참여하고 대표될 권리가 있음을 명시하고 있다. 제65조는 유럽정보 보호 위원회의 독립성을 강조하고 명시적으로 규정한다. 제66조는 지침 95/46/EC 제30조 제1항에 따른 유럽 정보 보호 위원회의 임무를 규정하고, 유럽연합 내에서 그리고 그

범위 이외에서의 유럽 정보 보호 위원회의 확대된 활동 범위를 반영하여 추가적 요소를 규정한다. 비상 상황에 대응할 수 있도록 유럽위원회는 특정 기간 범위 내에서 의견을 요청받을 수 있다. 제67조는 지침 95/46/EC 제30조 제6항에 따라 유럽 정보 보호 위원회는 그 활동에 관한 연례보고서를 제출하여야 한다고 규정한다. 제68조는 절차 규칙의 채택 의무를 포함한 유럽 정보 보호 위원회의 결정 절차를 규정한다. 제69조는 유럽 정보 보호 위원회의 장 및 부서장에 관한 규정을 포함하고 있다. 제70조는 위원장의 임무를 규정한다. 제71조는 유럽 정보 보호 감독관이 유럽 정보 보호 위원회의 사무국을 구성한다는 것을 규정하고, 해당 사무국의 임무를 구체화한다. 제72조는 비밀 유지에 관한 원칙을 규정한다.

(8) 구제, 책임 및 제재

제73조는 지침 95/46/EC 제28조 제4항에 따라 정보 주체가 감독기관에 대하여 이의를 제기할 수 있는 권리가 있음을 규정한다. 이 조항은 정보 주체를 대신하여 이의를 제기할 수 있거나, 정보 주체의 이의 제기와는 별도로 개인 정보의 불이행의 경우 이의를 제기할 수 있는 주체, 기구 또는 협회를 구체화한다. 제74조는 감독기관에 대한 사법적 구제를 받을 권리를 규정한다. 이 조항은 지침 95/46/EC 제28조 제3항의 일반 규정에 따른 것으로, 감독기관이 설립된 경우, 회원국의 법원이 갖는 권한을 명시하고, 감독기관에 이의를 제기하는 경우 받을 수 있는 사법적 구제책에 관한 내용을 규정한다. 이 조항은 또한 정보 주체가 거주하는 회원국의 감독기관이, 권한 있는 감독기관이 설립된 다른 회원국의 법원에 정보 주체를 대신하여 소를 제기할 수 있음을 규정하고 있다. 제75조는 지침 95/46/EC 제22조에 따라, 관리자 또는 처리자를 상대로 사법적 구제를 요청할 권리가 있으며,

피고가 거주하는 회원국 내 법원 또는 정보 주체가 거주하는 회원국 내 법원을 선택할 수 있음을 규정한다. 동일한 사안에 관한 절차가 일관성 체계 내에 계류 중인 경우, 해당 법원은 비상 상황을 제외하고 그 절차를 중지할 수 있다. 제76조는 다른 회원국 내 병행되는 절차에 관한 법원 정보, 법적 절차와 관련한 감독기관의 권리, 정보 주체를 대표하는 주체, 기구 및 협회의 권리, 그리고 그러한 절차를 중지할 수 있는 법원의 권한 등 법원 절차에 관한 일반적 원칙을 규정한다.[8] 회원국은 신속한 사법 처리를 보장할 의무를 진다.[9] 제77조는 배상을 받을 권리와 책임을 규정한다. 이 조항은 지침 95/46/EC 제23조를 근거로, 처리자가 일으킨 손해까지 권리를 확대하고, 공동 관리자와 공동 처리자의 책임을 명시하고 있다. 제78조는 이 규칙상 규정된 침해에 제재를 가하고, 규칙의 이행을 보장하기 위하여 각 회원국이 벌칙에 관한 규칙을 정하도록 의무화한다. 제79조는 각 감독기관이 동 조항에서 열거한 행정적 범죄를 제재할 의무를 규정하고, 각 개인별 상황에 따라 최대 금액 이하의 벌금형을 과하도록 규정한다.

(9) 특정 정보 처리 상황 관련 규정

제80조는 각 회원국이 표현의 자유와 개인 정보 보호의 조화를 위하여 필요한 경우 이 규정의 특정 규정에 대한 예외 및 수정을 도모할 것을 의무로 규정한다. 이는 EU 법원이 해석한 바와 같이, 지침 95/46/EC 제9조에 근거한다.[10] 제81조는 회원국이 보건 후생을 목적으

8) 형사절차에서의 관할 분쟁의 방지 및 조정에 관한 2009년 11월 30일 유럽이사회 프레임워크 결정 제5조 제1항에 근거한다.

9) 정보 사회 서비스의 특정 법적 관점에 관한 2000년 6월 8일 유럽의회 및 이사회 지침 2000/31/EC 제18조 제1항에 근거한다.

10) EU법원 (Court of Justice of the EU), 2008년 12월 16일 판결 (judgment of 16 December 2008) 참조, Satakunnan Markkinapörssi and Satamedia (C-73/07, ECR 2008 p. I-9831).

로 정보를 처리할 경우 안전책을 보장하기 위하여, 정보의 특정 유형별 조건을 상세화할 의무를 부여한다. 제82조는 고용 관점에서 각 회원국이 개인 정보 처리를 위한 특별 법령을 채택할 수 있는 권한을 규정한다. 제83조는 역사, 통계 및 과학적 연구를 목적으로 하는 개인정보 처리를 행할 경우에 대한 구체적 조건을 규정한다. 제84조는 회원국에게 관리자가 비밀 유지 의무의 대상이 된 경우, 감독기관의 개인 정보 및 그 영역에의 접근에 관한 구체적 규칙을 채택할 권한을 부여한다. 제85조는 이 규정과 저촉되는 경우 유럽 연합의 역할에 관한 협약 제17조에 따라 기존 교회의 포괄적 정보 보호를 위한 지속적 적용을 허용한다.

(10) 위임 입법 및 실행 법령

제86조는 TFEU 제290조에 따라 위임 행사를 위한 기준 규정을 포함한다. 이 조항은 입법상 비본질적 요소의 보완 또는 개정을 위하여 입법자가 유럽위원회에개 행정입법을 채택할 수 있는 권한을 부여한다. 제87조는 TFEU 제291조에 따라 유럽 연합의 법적으로 구속력있는 입법을 이행하기 위하여 필요한 경우 유럽위원회에 권한을 부여하는데 따른 위원회 절차를 규정한다. 조사 절차가 적용된다.

(11) 부 칙

제88조는 지침 95/46/EC를 폐지한다. 제89조는 e-프라이버시 지침 2002/58/EC와의 관계를 명확히 하고 이를 개정한다. 제90조는 유럽위원회에게 이 규칙을 평가하고 관련한 보고서를 제출할 의무를 부과한다. 제91조는 이 규칙의 효력 발생일을 규정하고 이 규칙의 적용을 위한 이행과도기를 규정한다.

3. 잊힐 권리에 관한 규정(안)의 내용

잊힐 권리 및 삭제권[11]은 일반정보보호규정(안) 제17조에서 규정하고 있다.

(1) 기본 내용

정보주체는 개인정보처리자를 대상으로 자신의 개인정보의 삭제 및 확산 방지를 청구할 수 있는 권리를 가진다. 특히 아동인 정보주체의 개인정보에 대하여 그러한 권리가 보장되어야 한다. 다만, ① 정보가 정보의 수집 또는 처리되는 목적과 관련하여 더 이상 필요하지 않는 경우, ② 제6조(1)(a)에 따라 정보주체가 동의를 철회하였거나 동의한 정보의 보관 기관이 만료한 경우, 그 밖에 정보 처리를 위한 법적 근거가 없는 경우, ③ 제19조에 따라 정보 주체가 개인 정보의 처리에 반대하는 경우, ④ 그 밖에 다른 이유로 정보의 처리가 이 규정에 부합하지 않는 경우에 잊힐 권리가 인정된다.

(2) 개인정보 공개시의 책임

개인정보처리자가 개인정보를 공개한 경우 개인정보처리자는 공개한 정보와 관련하여 기술적 조치를 포함하여 그 정보를 처리하는 제3자에게 정보주체가 그 개인정보에의 링크나 복사 또는 복제를 삭제할 것을 요청한다는 사실을 통지하기 위한 모든 합리적인 조치를 취하여야 한다. 개인정보처리자가 제3자의 개인 정보 공개를 허용한 경우 그 개인정보처리자는 해당 정보의 공개에 대한 책임이 있는 것으로 본다.

---

11) Article 17(Right to be forgotten and to erasure)

(3) 적용 예외

개인정보처리자는 ① 제80조에 따라 표현의 자유에 대한 권리를 행사하는 경우, ② 제81조에 따라 공공 보건의 영역에서 공익을 위한 경우, ③ 제83조에 따라 역사적, 통계적 그리고 과학적 연구 목적을 위한 경우, ④ 유럽 연합 또는 개인정보처리자가 속한 회원국 법률에 의해 개인 정보의 보관에 관한 법적 의무를 준수해야 하는 경우[12]와 같이 개인 정보의 보유가 필요한 경우를 제외하고는 지체없이 개인정보를 삭제하여야 한다.

(4) 개인정보 처리의 제한

개인정보처리자는 다음의 경우에는 삭제 대신 개인정보의 처리를 제한하여야 한다. ① 개인정보처리자가 정보의 정확성을 검증할 수 있는 기간 동안 정부 주체가 정확성에 이의를 제기하는 경우, ② 개인정보처리자가 업무 수행을 완료하여 개인 정보를 더 이상 필요로 하지 않으나 입증을 목적으로 보관하는 경우, ③ 정보처리가 불법이어서 정보 주체가 정보의 삭제가 아닌 사용 제안을 요청한 경우, ④ 정부 주체가 제18조 제2항[13]에 따라 다른 자동화 처리 시스템으로 해당 개인 정보의 전송을 요청한 경우가 해당된다.

개인 정보는 예외적으로 보관이 인정됨에 더하여 입증의 목적, 정보주체의 동의, 공익 목적 또는 다른 자연인이나 법인의 권리 보호를 위하여 처리될 수 있다. 또한 개인 정보의 처리가 제한된 경우 개인정보처리자는 처리 제한이 해제되기 전 정보주체에게 이러한 사실을

12) 이 경우 회원국 법률은 공익 목적에 부합하고, 개인정보보호 권리의 주요 내용을 존중하고, 추구하는 합법적 목적에 적합하여야 한다(Article 17(3)(d).)

13) Article 18(정보의 이동성에 관한 권리) (2) 정보주체가 동의 또는 계약에 근거하여 개인 정보를 제공한 경우, 정보주체는 개인 정보 및 정보주체가 제공한 그 밖의 다른 정보로 자동화된 처리 시스템에 의하여 유지되는 정보를 관리자의 방해없이 전송할 수 있는 권리를 가진다.

통지하여야 한다. 개인정보처리자는 개인 정보의 삭제에 필요한 기간 제한 및 정보 저장의 필요성에 대한 정기적 심사를 보장하기 위한 메커니즘을 도입하여야 한다. 삭제가 이루어진 경우 개인정보처리자는 삭제된 개인 정보를 다른 방법으로 처리해서는 안 된다.

(5) 위임 입법 권한

집행위원회는 ① 특정 정보의 처리 상황 및 부문에 관하여 제1항의 적용 기준 및 요건, ② 제2항에 규정된 공중이 사용가능한 통신 서비스로부터 개인 정보의 링크, 복사 또는 복제를 삭제하기 위한 요건, ③ 제4항에 규정된 개인 정보의 처리 제한 기준 및 요건을 구체화하기 위한 위임 입법을 채택할 권한을 가진다.

제 3 절 EU의 '잊힐 권리' 법제화에 관한 유럽네트워크정보보호원(ENISA)의 평가[14]

EU 개인정보보호 규정안이 2012년 공개된 이후 잊힐 권리가 과연 어느 정도로까지 보장될 수 있고 또한 현실적으로 보장가능한가에 대하여 다양한 의문이 제기되어 ENISA에서는 이에 대한 검토를 진행하였고, 그 결과 잊힐 권리에 관한 보고서[15]를 공표하였다.[16] 이 보고서에서 제시된 시사점들 우리가 EU의 규정안에 대하여 어떠한 시각으로 접근해야 하는가를 보여주는 좋은 자료로서 의미가 있기 때문에 이하에서는 보고서의 전문을 번역・소개한다.

14) 이하의 내용은 ENISA, "The right to be forgotten - between expectation and practice", 2012.11.20.(http://www.enisa.europa.eu)에 소개된 내용을 번역한 것임.

15) 이 문서는 유럽네트워크정보보호원(ENISA)에 의하여 2011년, 2012년에 발표된 "유럽에서의 데이터 저장 및 수집에 관한 연구(Study on data collection and storage in the EU)"와 "온라인 행태추적(online behavioral tracking)에 대한 사생활보호 고찰"에 관한 논문의 보완이다.

16) 최경진, "'잊혀질 권리'에 관한 해외 법제 동향", 잊혀질 권리와 디지털 자유 대토론회 자료집, p.25

1. 잊힐 권리의 해석

잊힐 권리는 무엇이 개인 정보를 구성하는 요소이며, 누가 특정 데이터 항목에 대하여 삭제를 요청할 권리를 가지며, 또한 무엇이 이 권리의 이행 수단으로 수용될 만한 것인가에 대하여 정확한 정의를 제공하는 것이 아니라, 그 해석에 관한 것이다.

(1) 개인정보의 범위

새로운 유럽연합 규정은 개인 정보와 관련하여 다음과 같이 규정하고 있다. ① '정보 주체(data subject)'는 직접적으로 또는 간접적으로 식별될 수 있는 관리자 또는 다른 자연인 혹은 법인, 특히 식별 숫자, 위치 정보, 온라인 식별자(online identifier)에 그 사람에 대하여 물리적, 생리적, 유전자적, 정신적, 경제적, 문화적 또는 사회적 정체성을 정하는 하나 또는 그 이상의 요소들에 의하여 합리적으로 이용되기 쉬운 수단에 의하여, 확인가능한 자연인(identified natural person)을 의미한다. ② '개인 정보(personal data)'는 정보 주체와 관련한 어떤 정보를 뜻한다.

정보보호규정 제2조의 규정은 "(a) '개인 정보(personal data)'는 식별되거나 식별가능한 자연인('정보주체(data subject)')과 관련된 어떤 정보이다. 식별가능한 자연인은 직접 또는 간접적으로, 특히 식별 숫자 또는 하나 또는 그 이상의 그의 물리적, 생리적, 정신적, 경제적, 문화적, 또는 사회적 정채성에 대하여 특정된 요소들과 관련하여 식별 될 수 있는 이를 말한다."고 되어 있다.

이러한 정의는 개인 정보를 그 자체로 혹은 다른 유효한 정보들과의 조합에 의해서, 자연인을 고유하게 확인할 수 있도록 링크될 수 있는 정보라는 것으로 광범위하게 규정하고 있다. 그러나 이러한 정

의는 예를 들자면, 그 사람의 사진이나 그의 역사들, 연기 행위와 같이 그것이 높은 가능성은 있지만 확실성은 없이 자연인을 식별하는데 이용될 수 있는 정보를 포함하는지 아닌지에 대해서는 명확하게 규정하고 있지 않다. 개인을 고유하지 않게, 가족처럼 회원 혹은 그 이상 혹은 그 이하의 개인들의 집합으로 인식하는 정보를 포함하는지 아닌지에 관해서도 명확하지 않다. 이와 관련된 문제는 합쳐지거나 파생된 정보(예를 들면, 통계)의 형태를 통계가 만들어 낸 (처리되지 않은) 미가공 데이터의 일부가 잊혀 졌을 때 영향을 받게 할 것인가이다. 모든 합쳐지거나 나누어진 형태의 잊혀진 정보를 제거하는 것은 중요한 기술적 도전이 될지도 모른다. 반대로, 합쳐지거나 나누어진 형태의 정보를 제거하지 않는 것은 그것이 합쳐진 다른 형태들과 연관 지음으로써 잊혀진 미가공 정보로 추정될 가능성이 있기 때문에 위험하다.

이러한 어려움은 유럽연합(EU) 규정과 법률들이 의도적으로 광범위하고 일반적이며, 많은 다른 상황에 대하여 적절한 해석의 범위를 허락하려는 경향 때문이다. 그러나 잊힐 권리를 보장하기 위한 기술적 수단은 잊혀지기 위한 권리에 적요되어야 할 그 데이터 및 상황들에 대하여 정확한 정의가 요구되어야 한다.

(2) 누가 데이터 항목 삭제 요청을 하는 권리를 갖는가?

다음의 문제는 누가 데이터 항목에 대하여 삭제를 요구할 권리를 갖느냐는 것이다. 많은 사례에서, 이것에 대한 답은 어떤 사람이 데이터베이스로부터 그들 자신의 이름, 생일 및 거주지 주소를 제거하는 것을 요구하는 사람의 경우와 같이 모호하다. 그럼에도 불구하고, 이와 다른 경우에, 누가 이 항목들이 잊혀지도록 요구하는 권리를 갖느냐에 대한 문제는 해석의 문제로 다뤄지게 된다.

예를 들어, 어떤 시간과 장소에서 어떤 활동으로 이루어진 Alice와 Bob을 묘사한 사진을 생각해 보자. Alice는 이 사진이 잊혀지기를 바라고, Bob은 이것이 계속해서 유지되기를 바란다고 가정해보자. 누구의 바람이 존중되어야만 하는가? 만약 다수의 사람들이 단체 사진에서 보여지고 있다면? 누가 이 사진이 잊혀질지 말지 그리고 언제 그렇게 되어야 할지에 대한 결정을 하는가? 또 다른 예를 들어보자면, Bob이 그가 Alice로부터 받은 트윗의 부분을 보다 길이가 긴 자신의 블로그 포스트에 추가한다. Alice가 이후에 그녀의 트윗을 제거하는 그녀의 권리를 행사하게 되었을 때, Bob의 블로그 포스트의 지위에 관하여 이것은 어떠한 영향을 미치게 되는가? Bob이 그의 블로그 전체를 제거해야한다면? 그가 Alice의 트윗을 블로그로부터 제거하거나 그의 포스트를 그에 따라 다시 써야만 한다면? 어떤 기준이 결정에 사용되어야만 하는가?

이와 관련한 문제는 어떻게 잊힐 권리가 책임성(accountability), 언론(journalism), 역사(history), 과학적 연구(scientific inquiry)에 있어서 공공의 이익과 조화를 이루게 하느냐이다. 정치인 또는 정부는 이러한 당황스러운 보고서의 제거를 요구할 수 있어야만 하는가? 과학적 연구의 입안자는 발표(publication)의 철회를 요구할 수 있어야만 하는가? 어떤 원칙이 결정에 사용되어야만 하고, 누가 결정에 대한 권한을 갖는가?

(3) 무엇이 "잊혀지는" 데이터 항목이라고 여겨지는가?

다음 과제는 무엇이 "잊혀지는(forgetting)" 정보에 대하여 수용가능한 방법이냐에 대한 문제이다. 엄격한 해석은 알려진 기술적 수단 등으로 정보의 복구를 불가능하게 하는 정도로 나뉘거나 합쳐진 표현물들로부터 정보의 모든 사본들을 삭제하고 제거하는 것을 요구하는 일이 될 것이다. 보다 약한 그리고 실질적인 가능성이 보다 높은 해석

은 권한 없는 당사자들에 의하여 암호가 풀릴 수 없도록, 남아 있는 정보의 암호화 복제를 허용하는 일이 될 것이다. 훨씬 더 약한 그리고 보다 실질적인 해석은 정보가 공적인 색인목록, 정보베이스 계층 클러스터링, 또는 검색엔진의 검색결과에 나타나지 않는 한, 남아 있는 깨끗한 문서 복제물들을 허락하는 것이다.

2. 기술과 과제

잊힐 권리를 집행하는데 있어서 처해진 근본적인 도전 과제들은 ① 개인을 식별하고 개인정보 항목들에 관하여 저장된 위치가 어디인지를 알게 하는 것, ② 정보 항목의 복제물 및 데이터 항목으로부터 파생된 모든 종류의 항목에 대한 복제물을 추적하는 것, ③ 개인 정보 항목의 제거를 요구할 수 있는 권리를 갖는지의 여부를 결정하는 것, ④ 권한 있는 자가 이러한 권리가 행사된 경우의 사례에 있어서, 모든 일치하거나 파생된 복제물의 삭제 또는 제거를 효율적으로 만드는 것이다.

오늘날 월드 와이드 웹의 어마어마한 공공의 비율과 같이 완전하게 개방된 시스템에서는, 누군가가 공공의 데이터 항목의 복제물을 만들고 그것들을 임의적인 장소에 저장하는 것이 가능하다. 게다가, 이러한 시스템은 그러한 복제물의 숫자, 소유자 또는 위치를 확인하지 않는다. 이러한 개방 시스템에서 어떤 사람이 그들에 관하여 저장된 모든 개인 데이터 항목들의 위치를 정하는 것은 일반적으로 불가능한 것이다. 어떤 사람이 특정 데이터 항목에 대하여 삭제 요청을 하는 권리를 갖는지의 여부를 결정하는 것은 어렵다. 어떤 개인 하나 혹은 전체가 모든 복제물의 삭제에 효력을 미치는 권한 또는 관할을 갖는 것도 가능하지 않다. 그러므로 잊힐 권리를 집행하는 것은 개방형, 글로벌 시스템에서는 일반적으로 불가능하다.

"잊힐 권리(right to be forgotten)"를 집행하기 위한 능력은 결정적으로 근본적인 정보 시스템의 수행능력에 달려 있다. 간단히 말해서, 이 수행능력은 모든 정보에 대하여 저장과 보급이 확실하게 처리되고, 삭제가 시행될 수 없는 곳에 대하여 정보의 파급을 막을 수 있는, 기술적으로 "폐쇄적인(closed)" 시스템에서만 가능한 것이다. 이러한 시스템에서, 모든 참여 기업들은 잊혀 질 권리가 집행되는 관할에 속하며, 모든 정보 요청은 권한이 존재해야만 하고, 로그 되어야만하며, 이 원칙들은 현실 세계의 사람들과 조직체들과 연결되어 있어야만 한다.

원칙적으로, 유럽연합 회원국들의 관할권 내에서 전반적인 몫을 차지하고 있는 네트워크 협력 및 네트워크 공유 사용권한에의 접근과 같은 시스템들은 이러한 요건들에 부합할 수 있다. 그러나 그러한 연결망들은 예외 없이, 전자적 식별의 형식을 사용함으로써 모든 주체들(사용자 및 공급자들)이 자연인과 연결될 수 있다는 것을 강력하게 증명할 것을 요구하게 될 것이다.

반면에, 인터넷과 같이 공적인 비중을 가진 개방형 시스템에서는, 공공의 데이터는 자연인과 확실하게 연결지어 질 수 없는 온라인 식별들로써 이용주체들에 의하여도 접근이 가능하다. 이러한 주체들은 정보를 신뢰할 수 없는 당사자들에게 보다 더 확산시키고, 이로 인하여 엄청난 양의 데이터 복제의 결과가 나올 가능성이 있다. 이러한 시스템에서, 잊힐 권리를 집행하기 위한 일반적으로 적용가능하고 기술적인 접근은 존재하지 않는다. 개인 정보가 사회적 네트워킹 사이트, 홈페이지, 블로그, 트윗 등에 포함되는 이러한 경우는 인터넷에서 흔한 일이다. 다음의 세부 항목에서, 우리는 양쪽의 가능성에 대하여 보다 세부적으로 논의하게 될 것이다.

정보화 체계(information system)의 형태에 상관없이, 사람의 관찰에 의한 권한 없는 정보의 복제를 기술적 수단에 의하여 방지하는 것이

영구적으로 불가능하다는 것을 이해하는 일은 매우 중요하다. Alice가 그녀가 그렇게 하도록 허락되는 동안(즉, Bob이 그의 잊힐 권리를 적용하기 전에) Bob의 개인 정보를 컴퓨터 화면으로 보는 것을 생각해 보자. Alice는 카메라를 사용하여 화면의 사진을 찍을 수 있고, 그 정보를 적어두거나 기억할 수 있다. Alice가 그렇게 하는 것을 막거나, 혹은 그녀가 Bob의 개인 정보의 복제물을 얻었다는 사실을 인지하는 것조차도 기술적으로는 불가능하다. 이후에, Bob이 그의 잊힐 권리를 적용하게 되면, 이 시스템 안에서 모든 알려진 그의 정보에 대한 복제물은 삭제될 것이다. 그러나 Alice는 이 정보의 복제물을 가지고 있고, 그녀는 이 정보를 의지로 배포하거나 다시 실을 수도 있다.

(1) 비공개 시스템

이 논의의 목적을 위하여, 폐쇄적 시스템(closed system)은 개인 정보를 처리하고, 이전하거나 혹은 저장하는 구성요소들의 하나이며, 개인 정보에 접근하는 모든 사용자와 운영자들은 또한 신뢰할 수 있거나 이 개인 정보의 사용과 관련한 적절한 법률과 규정들에 대한 기대에 책임을 질 수 있어야한다.

데이터 처리 하드웨어 및 소프트웨어가 기업에 의하여 소유되고 운영됨으로써 개인 정보가 독점적으로 처리되고, 이전되고 저장되며, 개인 정보에 접근하는 모든 사용자 및 운영자들이 고용인들로 이루어진, 내부 네트워크는 하나의 좋은 예이다. 이러한 연결망에서 '잊힐 권리(right to be forgotten)'를 이행하는 것은 장애만 없다면, 기술적으로는 가능하다. 예를 들어, 개인정보의 항목의 소유자가 그의 잊힐 권리를 행사한다면, 확인하고 제거하는 모든 정보의 복제물(직원의 컴퓨터 로컬 디스크에 저장된 은닉한 복제물, 기록보관소 저장 매체에서 저장된 복제물의 예비파일 등을 포함하는)과 어떠한 파생 정보는 기술적으로 어려움을 겪을 수 있고, 상당한 운영상의 비용이 요청될 수 있다.

보다 복잡한 폐쇄형 시스템(closed system)의 형태는 개인정보를 공유하고 이러한 정보의 이용과 관련하여 정부에 의하여 규제되는 산업이다. 예를 들어, 미국의 의료산업(의료정보제공자, 보험회사들, 의료결제 회사들)은 고용인이 환자들의 기록을 공유할 뿐만 아니라, 연방 의료보험통상책임법(the Health Insurance Portability and Accountability Act, HIPAA)의 Title Ⅱ와 관련한 이러한 정보를 다룸에 있어서 공동으로 책임을 진다. 기업과 조직들의 참여는 그들이 적절한 개인정보에 대하여 신뢰받고 책임감 있는 것이 된다. 이 시스템은 개인정보에 접근하는 모든 당사자들이 그들이 법률을 준수하는 것에 대하여 책임을 지며, 모든 개인 정보가 미국의 관할권으로 남기 때문에 폐쇄적인 것이 된다. 원칙적으로, "잊힐 권리"는 이러한 시스템에서 이행될 수 있다. 그러나 실제에서, 의료정보 부문에서 사생활이 침해되는 일은 드문 일이 아니며, 금융 산업에서 신용카드 정보가 손실되는 일도 그러하다. 이것은 잊힐 권리가 폐쇄적 시스템 안에서도 어려운 일이라는 것을 말해주는 것이다.

폐쇄적인 시스템(closed system)에서조차도, 기술적 수단 혼자만으로는 법의 준수를 보장하기가 매우 어렵기 때문에, 개인 정보에 접근하는 모든 이용자는 적절한 사생활보호 법률을 존중할 것이라고 신뢰받아야 한다. 예를 들어, 직원이 그의 사무실 컴퓨터 화면에서 개인 정보에 대한 사진을 스마트 폰을 이용하여 찍어서 그들이 잊힐 권리에 대하여 어떠한 기술적인 집행도 닿을 수 없는 곳인, 회사 밖으로 디지털화된 정보를 이전시키는 것을 막는 것은 어려운 일이 될 것이다.

(2) 공개 시스템

인터넷과 같은 개방된 네트워크에서 전형적으로 공공에게 접근이 가능한 정보는 그 정보의 근원이 되는 사용자의 지배하에 유지될 수가 없다. 정보가 디지털로 복제될 수 있고, 국부적으로 저장될 수 있

으며, 종종 다른 장소와 다른 목적을 위하여, 인터넷으로 다시 재입력 될 수 있다는 것이 그 이유이다. 그러한 디지털 복제 및 임의적 데이터의 재입력은 디지털저작권관리(Digital Rights Management, DRM)에서와 같이, 근본적으로 소프트웨어 혹은 하드웨어에 관한 매우 강력한 통제들을 가능하게 하지 않는 한, 일반적으로 기술적인 수단들에 의해서는 방지될 수 없다. 그러한 강력한 통제들은 추가적인 기술적 경제적 도전과제들을 생겨나게 하며, 종종 공공에 수용에 있어서 한계에 부딪히기도 한다. 게다가, 이러한 강력한 수단들이 전반적으로 이 문제들을 풀 수 있을지 없을지에 대해서 불분명한 점을 남기기도 한다. 예를 들어, 디지털저작권관리는 훌륭한 콘텐츠를 보호하기 위하여 암호 기반(cryptographic infrastructure)을 요구하며, 소프트웨어 프로그램 담당자는 디지털저작권관리를 지지하도록 맞춰야만 한다. 그럼에도 불구하고, 전문 공격자들은 쉽게 디지털저작권관리을 피해가기도 한다.

권한 없는 데이터 복제를 피하기 위하여 가능한 방법은 저작권 보호를 집행하는 실행 가능한 프로그램으로 데이터의 양을 늘리는 것이 될 수 있을 것이다. 에를 들어, 이미지들은, 예를 들자면, 이미지들이 보이는 동안에, 그리고 그 이후로도, 이미지의 화면 샷을 못하게 하는 (이전에 암호화 되었던) 데이터를 적절하게 표시하기 위한 믿을만한 서버로의 통신과 같은, 해당 디스플레이 프로그램을 갖추는 것이 될 수 있다. 이러한 기술들은 정보의 복제를 제한하는데 사용될 수 있다. 그러나 이러한 해법은 실제에서 중요한 한계들에 부딪히게 된다. ① 사실상 거의 모든 서비스들은 JPG와 같은 표준 파일 형식을 따르며, 이러한 이유로 그들 자신의 판독으로부터 비롯된 소유주의 형식은 받아들여지지 않게 될 것이다. ② 그러한 해법들은 종종 추가적인 보안 문제들을 일으키는, 외부 서버들과의 추가적인 토신을 요구하게 될 것이다. 예를 들어, 그런 프로그램들은 개별주체들의 컴퓨터나 장치들

에 있는 트로이 목마나 바이러스들이 유입되는 새로운 통로를 제공하게 될 것이다. 적절하게 기능하기 위하여, 이러한 프로그램들은 관대한 허가로 처리해야 하며, 이것은 악성 코드로 이용될 수 있는 가능성이 잠재적으로 존재한다. 따라서 이러한 해법은 사업, 보안 전문가 및 공공에 의하여 회의론으로 생각되기 쉬울 수 있다. 그러므로 디지털 복제는 일반적으로 개방형 네트워크에서는 방지될 수 없다는 말은 타당한 말이다. 그럼에도 불구하고 직접적인 디지털 복제가 기술적 수단에 의하여 차단될 수 있다는 것을 가정한다면, 방지하기가 훨씬 더 어려울 수 있는 데이터 복제에 효과를 미칠 수 있는 추가적인 방법이 존재한다는 것을 지적하는 것은 의미 있는 일이다. 예를 들자면, 개인 정보가 보여지는 사진을 찍거나, 또는 모든 청자들의 물리적인 화상통신 없이 사적인 대화가 그것이 재생되는 동안 마이크를 이용하여 녹음되는 것을 방지할 수가 없는 것들이다. 그런 식으로 탈취된 정보는 인터넷에서 재입력될 수 있다. ③ 사실상 중요한 뉴스와 같이 공적인 정보는 비디지털(non-digital) 신문, 라디오 등과 마찬가지로, 전형적으로 다양한 다른 형식, 다양한 디지털 소재들 모두에서 존재한다. 이 정보를 잊혀지게 만드는 기술적인 방법은 존재하지 않는다.

(3) 폐기 또는 오프라인 기억장치에 대한 개인정보의 보호

개인 정보가 개방형에서 처리되는지 혹은 폐쇄형 시스템에서 처리되는 지의 여부와 상관없이, 실제적인 주의는 예컨대, 스마트폰, 노트북, 데스크탑 컴퓨터 및 USB 장치(대용량 이동 저장장치)와 같이 폐기되거나 재활용되는 자기 디스크나 플래시 디스크 장치들과 같은 폐기된 저장 장치에 의하여 저장된 정보에 두어야 한다. 그러한 장치에서 파일들을 간단하게 삭제하는 것은 제3자가 단순하고 널리 유용한 기술적 수단을 사용하는 폐기 장치들로부터 그러한 정보를 회복시키는 것을 막는데 비효율적이다. 2013년 4월에 있었던, 영국정보보호위

원회(Information Commissioner's Office-UK, ICO)에서 발표한 연구에 따르면, 폐기된 저장 장치들에 대한 개인 정보의 누출은 실질적으로 중요한 문제이며, 소비자들은 이를 피하기 위하여 보다 더 큰 주의를 해야만 한다. 이 문제는 물리적으로 저장 매체를 파괴하거나, 신뢰할 만한 전문적인 서비스에 의하여 처리하거나, 하드디스크 데이터 완전 삭제 툴(Darik's Boot And Nuke, DBAN)과 같은 보안 삭제소프트웨어의 이용함으로써 피할 수 있는 것이다. 이것과 연관된 문제는 온-오프라인 저장 매체에서 저장된 정보의 제거와도 관련이 있다. TAR(Tape Archive)[17] 또는 USB 스틱(대용량 이동 저장장치)과 같은 온・오프라인 데이터 복제물 저장은 일반적이며, 재해복구(disaster recovery)를 필요로 한다. 그럼에도 불구하고, 개인의 그들의 잊힐 권리를 행사할 때, 제거 운영의 일부로써 그러한 복제를 위치시키는 것은 특히 어려운 일이 될 수 있다. 온・오프라인 매체에 저장한 제거된 데이터 항목들은 매체에 접속하자마자 삭제될 수 있기 때문에, 무기한으로 제거 요청을 분산하거나 유지하는 것이 필요할 것이다.

(4) 데이터의 만료에 대한 현행 기술들

현재의 정보화 시스템에서 가상으로 퍼져 있는 메모리의 폭넓은 결과들을 논의하고 있다. 만료 데이터로 민감한 정보를 표시하고 모든 서버들이 그러한 데이터를 그 날짜에 따르게 처리하도록 요구할 것을 제안하고 있다. 그러한 권한은 많은 법인 정보 서비스 공급자들의 사업상 이익 및 정부의 이익과 모순된다. 반면에, 정보의 만료날짜를 존중하는 전 세계적인 법적 권한은 가까운 미래에는 힘이 미치지 않을 것 같이 보인다. 게다가, 모든 서버들이 사실상 이 데이터를 삭제하고

17) 지정된 여러 개의 파일들을 아카이브라고 불리는 하나의 파일로 묶는 혹은 반대로 하나로 묶인 파일을 원래의 파일들로 풀어주는 유닉스 유틸리티온-오프라인 매체데이터 복제물

비행 서비스 공급자들에게 책임을 지게 하는 것을 확인하는 것은 기술적으로 어려운 일이다. 최근 몇 년간, 많은 수의 연구 프로젝트들이 이 문제에 관하여 다양한 관점으로 다루는 것을 노력해 왔다.

이 작업의 최우선 선상에서, 개인정보와 관련한 만료 기간은 대칭키 암호화 시스템(symmetric encryption key)과 이러한 키에 대한 접근을 제한함으로써 암호화된 데이터 자체에 의하여 이행되어 진다. 불행히도, 이러한 시스템의 어떤 것도 공개된 데이터가 이후에 조정이 되는 경우의 상황, 예컨대, Facebook과 같은 소셜 네트워크에서 일반적으로 행해지는 것과 같은 JPEGs의 재인코딩과정(re-encoding)을 다룰 능력을 갖추지 못하였다. 이와 유사하게, 암호키들을 그들의 유효 기간 동안 안전하게 저장 및 분배하는 것의 문제들이 이제까지 고려되어 왔다. 결국, 권한 없는 복제를 막고, 모든 암호 키 보유자들이 그들의 키를 삭제하는 것을 통지하고, 제거 요청을 확인하는 것은 열린 문제로 남아 있다.

첫번째 과제는 법인 정보 시스템 그리고 단일한 관할권에 제한되는 시스템들과 같은, 폐쇄형 시스템을 효과적으로 하는데 그 목적이 있다. 여기서 모든 서버들은 암호화된 데이터의 본질을 파악하고 있으며, 이후 데이터의 처리는 지지되지 않으며, 일반적으로 데이터가 유효한 동안 암호화키를 획득한 상대방을 취급하는 것은 고려되지 않는다. 이러한 시스템에서 우리가 우선적으로 알아야 할 것은 다음에 서술되며, 이것은 기본적인 원칙들을 제공하고 있다. 또 다른 중요한 시스템은 나중에 서술할 개선된 형태인 Ephemerizer이다. Vanish는 P2P 네트워크의 기저를 이루는 데이터 구조인, 분산 해시 테이블(distributed hash table, DHT)에서 암호 키들을 공유를 저장하는, 훨씬 최신의 접근법이다. 분산 해시 테이블(DHT)은 특정 시간 이후에 암호키를 확실하게 제거하도록 설계되어, (암호화되지 않은) 일반텍스트(cleartext) 데이터를 사용할 수 없게 만든다(암호화된 복제물이 존재함

에도 불구하고). 분산 해시 테이블(DHT)에서의 Sybil 공격[18]을 사용하는, 이행 제안에 대한 공격이 최근에 발표되었었다.

X-pire![19]는 사용자들에게 이를 테면, Facebook이나 Flickr와 같은 소셜 네트워크상에서, 이들 웹페이지로써 추가적인 상호작용의 어떠한 형식도 요구하지 않는 정적 방식 웹사이트(static websites)[20]에서, 이미지에 대한 유효기간을 설정하도록 하는 시스템이다. 기술적으로, X-pire! 는 이미지들이 웹 서버에 업로드 되기 전에, 그리고 열심히 일하는 암호 키 서버에서 상대의 기들을 저장하기 전에, 이미지를 적당한 방식으로 암호화한다. 예를 들어, Alice의 Facebook 프로파일을 방문하는 때, 만약 사용자 Bob이 이러한 이미지를 보기를 바란다면, 브라우저는 Bob의 기계에 대한 실행 연결은 키 서버로부터 상대방의 해독키(decryption)를 요청하게 된다. 만약 이 키가 아직 만료되지 않았다면, 이 이미지는 해독되어 Bob의 화면에 보여 지게 된다. 이러한 모든 시스템에서와 같이, 공격자는 권한 없는 이미지에 대한 복제물을 화면에 스냅 샷(snapshot)을 찍거나 문서 이미지가 화면상에 보여 지고 있을 때 카메라로 사진을 찍음으로써 얻을 수 있다.

EphCOM 시스템은 Vanish와 유사하지만, 일반화된 호스트명의 표시에 기반 한, DNS 서버의 은닉에서 키들을 저장하는 편법을 사용하지 않는다. Vanish 와 X-pire! 와 유사하게, 그것들의 유효기간 동안 데이터 보호의 후처리(post-processing)와 검색 키(retrieving key)의 처리를 고려하지 않는다. 특정 시간에 유효한 데이터를 발표하는 것은 같은 TTL을 갖는 수많은 도메인들을 알아야 할 필요가 있다. 이 연구는 이러한 접근의 실질적 한계가 있기 때문에, 7일 이상의 TTLs은 다소 흔

18) 어떤 한 공격자가 여러 개의 식별자를 가지고 시스템이나 네트워크를 공격하는 방법의 총칭

19) 익스-피레, 폐기라는 의미를 가진 독일 회사

20) 사용자의 환경이나 회사의 정책, 접속 시점 등의 환경 변화를 고려하지 않고 무조건 클라이언트로 동일한 HTML 페이지를 전송하는 방식의 사이트와 페이지를 의미

한 것이 아니라는 것을 보여준다.

이 작업의 두 번째 선상은 소셜 네트워크에서 발표된 사생활에 민감한 내용을 보호하는 목적에 있다. 가장 핵심적으로 다른 점은 앞서 언급했던 접근들이 이러한 데이터를 목적을 삼은 서버들, 사실상 소셜 네트워크 그 자체인 것에서 취하는 반면에, 이러한 접근들이 모든 데이터를 외부의 신뢰할만한 서버에 대하여 저장한다는 점이다. 그 하나의 예가 FaceCloak 이다. 이러한 접근들에 있어서 문제점은 매일 매일 발행되는 이미지와 비디오 다중 매체를 포함하는, 어마어마하게 많은 양의 정보가 주어지는, 중앙집권적인 서버의 확장성이다.

개인 정보에 대한 접근을 막는 유사한 동기들에 따라서, 소유자 중심의 컴퓨터 시스템 구성(owner-centric architecture, OCN)은 최근 핵심적인 원칙에 따라 콘텐츠 소유권을 고려하는 것이 제안되었다. 콘텐츠 분배 및 통제에 관한 한, 소유자 중심의 컴퓨터 시스템 구성(OCN)은 그 데이터의 적법한 소유자만이 접근할 권한을 갖는, 모든 데이터들을 위하여 헌신하는 저장 위치들을 설립하는 것을 목적으로 한다. 그러한 데이터에서 콘텐트 접근은 이러한 저장 공간들과 연결을 제공함으로써 사용자들에게 주어지게 된다. 이 구성은 사용자가 권한 없는 복제물을 만들지만 않는다면, 적법한 데이터의 소유자에 의한 데이터의 지배를 보장한다. 앞서 언급했던 접근들과 유사하게, 복제 및 통제되지 않은 데이터의 전파는 이러한 구성에 의하여 제공된 보장들을 무효화 할 수도 있다. 그리하여 전술한 부분에서 논의했던 바와 같이, 이러한 해법들은 잊힐질 권리를 현실화시키기에는 불완전한 기술적 해법만을 제공한다.

데이터 복제를 방지하는 또 다른 가능성 있는 해법은 디지털저작권관리(DRM)로부터의 기술들을 채택하는 것이다. 기술적으로 디지털저작권관리(DRM)는 다양한 상업 기업들이 권한이 없이 디지털 콘텐트를 사용하는 것을 억제하는데 사용되어 온, 접근 통제를 위한 기술이

다. 디지털저작권관리(DRM)는 콘텐츠 발행인, 하드웨어 제조업체, 저작권 소유자, 그리고 판매 후 그들의 상품의 전파에 제한을 바라는 개별주체들을 위하여 설계되었다. 실제로, 디지털저작권관리는 다양한 문제 상황들에 직면해 있는데, 특히 기술적 수준에서 그러하다. 디지털저작권관리 기술들은 종종 적당한 시도로 우회 될 수도 있다. 예를 들어, 디지털저작권관리 오디오 보호는 오디오 CD에서 오디오 파일들을 복제하고, 그 후에 디지털저작권관리・무료 오디오 파일로 들어감으로써 우회될 수 있다. 이와 유사하게, 이미지와 비디오에 있는 워터마크(watermarks)는 종종 쉽게 제거될 수 있다. 그 결과, 디지털저작권관리에 기반을 둔 해법들은 일반적으로 데이터 복제를 피할 가능성이 별로 없다.

데이터가 발간된 때 인터넷으로부터 이것이 제거되는 것이 일반적으로 불가능하다지만, 그것의 접근에 제한을 두는 것은 가능할지도 모른다. 이러한 접근은 전형적으로 검색 엔진에서 이슈가 된 질문들에 의하여 또는 소셜 네트워킹, 공유 또는 표지 사이트를 사용하거나, 인터넷에서 사용자들이 정보를 알아내는 관찰에 의존한다. 검색 엔진이나 Twitter와 같이 공유되는 경우 서비스에 의하여 확인되지 않는 데이터는 찾기가 어렵다. 그러므로 "거의 잊는" 데이터에 대한 자연스러운 방법은 검색 엔진의 결과들에서 그것의 등장을 방지하고 Twitter와 같은 공유 서비스 공유로부터 그것을 여과하는 것이다. 유럽연합 회원국들은 검색엔진 운영자 및 공유 서비스들에게 잊혀진 데이터와 관련하여 여과를 요구할 수 있었다. 결과적으로, 예컨대 유럽연합 관할권 밖에서, 복제물이 여전히 존재함에도 불구하고, 잊혀진 데이터는 찾기가 매우 어려울 지도 모른다.

요약하자면, 잊힐 권리를 보장하기 위한 모든 현행 기술적 접근들은 그 날짜가 공적으로 접근가능하고 그러한 권한 없는 복제물의 재 전파가 기간이 만료하는 동안, 권한 없는 복제에 취약하다. 그러므로 잊

힐 권리는 기술적 수단 단독으로는 보장될 수 없다. 가능성 있는 부분적인 해법은 예컨대, 만료된 개인 정보는 그 검색의 결과에서 나타나지 않도록 검색엔진에 요청함으로써, 만료된 개인 정보를 찾기 어렵게 만드는 것을 목적으로 하는 법적 권한이 존재하는 것일지도 모른다.

3. 권고 사항

개인 정보가 발간된 때, 그것은 기술적 수단에 의해서는 이 정보의 권한 없는 복제의 창출을 방지하거나 혹은 목격하는 것조차 불가능한 것이다. 인터넷과 같은 개방형 시스템에서, 잊힐 권리는 기술적 수단 단독으로는 집행될 수 없다. 집행은 기술적이면서도 국제적인 규정들의 조합에 기초해야만 한다. 권고사항들은 다음과 같다.

① 잊힐 권리의 집행을 원조하는 기술적 수단들은 개인정보의 범위와, 어떤 상황에서 누가 개인 정보의 삭제를 요구할 권리를 갖는지에 대한 설명, 그리고 무엇이 데이터의 제거에 영향을 미치는 수용될 수 있는 방법인가를 요구한다. 제29조 실행그룹(WP29), 유럽 정보보호 자문위원회(the European Data Protection Supervisor) 등의 정보 보호권한자들(Data Protection Authorities)은 이러한 이슈들을 명확하게 하기 위하여 공동으로 노력해야만 한다.

② 앞서 언급했던 정의들을 제공하는 때, 정의들에 대하여 주어진 선택에 있어서 잊힐 권리를 집행함에 필요한 기술적 도전과제들은 주의 깊게 고려되어야만 한다. ③ 잊힐 권리에 대한 어떠한 합리적인 해석에 있어서, 이 권리를 집행하기 위한 순수하게 기술적이고 포괄적인 해법은 일반적으로 불가능하다. ④ 잊힐 권리의 집행을 원조하기 위한 가능성 있는 실용적인 접근은 유럽연합(EU) 내의 검색엔진 운영자 및 공유서비스들에게 유럽연합(EU) 지역 안 밖에서 저장되는

잊혀 진 정보에 관하여 여과하도록 요구하는 것이다. ⑤ 폐기되고 오프라인 저장 장치들에서 저장된 개인정보의 삭제와 관련해서는 특별한 주의가 행해져야만 한다. ⑥ 데이터 관리자들은 사용자들에게 그들이 저장한 개인정보로의 쉬운 접근을 제공해야만 하고, 사용자들에 대하여 지체나 비용 없이 정보를 업데이트하고, 정정하며, 삭제할 방법들을 제공해야 할 필요가 있다. ⑦ 원치 않은 정보의 수집이나 전파를 방지하기 위한 목적의 기술들(예를 들어, 로봇배제표준(robot.txt), 개인추적장치(do not track), 접근 통제(access control))을 발전시켜야 될 것이다.

또한 나아가 ① 정책 입안자들은 온라인에서 수집되고 저장된 개인정보의 양을 최소화하기 위한 최소 노출의 원칙을 지원하는 기술들의 사용을 보장해야만 한다. ② 우리는 또한 개인정보의 저장과 이전을 위하여 암호화의 사용을 모든 당사국들에게 권유한다. ③ 특별한 주의가 온라인의 추적 및 자료수집에 초점이 맞춰져야만 하며, 정책 입안자들은 비행 기업들을 막고, 개인 정보 보호에 관한 규칙과 규정들의 준수를 집행하기 위해서 집행을 위한 명확한 제재와 수단들을 규정해야만 한다. ④ 정보보호권한자들과 이 분야의 관련 이해관계인들은 사용자들이 이 정보 보호 입법으로부터 그들의 권리를 다지는 것과 개인 정보의 과잉 수집 및 저장의 경우에 항의하는 것을 포함하여, 이러한 권리들을 행사하기 위한 법적 시스템에 의하여 그것들이 제공될 가능성에 대하여 이와 관련한 인식을 개선하는 것을 목적으로 해야만 한다. ⑤ 동시에, 정보보호권한자들, 제29조 실행그룹(WP29), 유럽 정보보호 자문위원회(the European Data Protection Supervisor) 등은 회원국들이 규정들의 충돌을 감소시켜야 하는 반면에(개인 정보의 수집과 저장이 항상 보 보호 법제에 의하여 통제되지는 않는다), 실질적 이행과 관련한 미결된 정의 이슈들을 명확히 하기 위하여 공동으로 작업해야만 한다.

제 3 장 미국의 개인정보보호 정책 관련 최신 동향

최근 2012년 2월 오바마 대통령은 “네트워크세계에서의 소비자정보 프라이버시 : 글로벌 디지털 경제에서의 프라이버시 보호 및 혁신 촉진을 위한 기본 구상[21]”을 발표하면서 소비자 프라이버시 권리장전을 제시하였다. 이에 의하면 소비자에게 보장되는 권리 중에서 특히, 목적 제한적 수립(focused collection)에 따라 기업은 개인정보를 폐기하지 말아야 할 의무가 없는 이상 개인정보가 더 이상 필요하지 않은 경우 확실히 폐기하거나 비식별 처리하여야 한다고 천명하였다[22]. 이하에서는 해당 내용을 요약・소개하기로 한다.

제 1 절 미국 소비자 개인정보 보호체계 강화의 기반 구축[23]

미국에서 소비자 개인 프라이버시 강화는 중요한 행정적 우선사항이다. 미국인들은 사생활에 가치를 두며, 민간 및 정부의 프라이버시

21) 네트워크 세계에서의 소비자 개인 정보(Consumer Data Privacy in Networked World)는 상무성(the Department of Commerce) 인터넷 정책 전담팀의 2010년 12월 보고서, “Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework, Privacy and Innovation Green Paper""의 권고들을 기반으로 하고 있다. 인터넷 정책 전담반은 사생활 보호 및 혁신 녹색 보고서(Privacy and Innovation Green Paper)에서의 권고들을 이해관계자들 - 기업, 무역 그룹, 민간 사생활 보호 지지자, 학계, 주 법무장관들, 연방 민・형사법 집행부 대표들 및 국제적 동반자들 - 의 공공 토론회, 논평, 공개 연설 및 발표회, 비공식 회의들을 통한 참여로 발전시켰다. 100명 이상의 이해관계인들은 사생활 보호 및 혁신 녹색 보고서에 대하여 서면의 논평을 제출하였다. 이러한 논평들은 네트워크 세계에서의 소비자 개인 정보를 전개하는 동안 매우 유용한 반응들을 행정부에게 제공하였다.

22) 최경진, 앞의 자료집, p.26

23) 이하의 내용은 THE WHITE HOUSE, Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy, 2012.1에서 발췌한 내용임.

침해로부터의 보호를 기대한다.[24] 강력한 사생활 보호는 또한 인터넷 상거래를 양성하고 혁신을 위한 신뢰를 유지한다는 점에서 중요하다. 인터넷 경제에서 신뢰를 보호하는 것은 상당한 양의 경제 활동을 보호하고 향상시키는 일이다. 지역에서 적절한 사생활 및 보안 장치들에 의하여 보호되는 개인 정보의 새로운 이용은 중요한 비즈니스 기회를 창출할 수 있는 것일 지도 모른다. 또한, 미국은 클라우드 컴퓨팅[25] 수출, 지역기반 서비스 및 기타 혁신적인 서비스에 있어서 세계의 지도적인 역할을 수행하고 있다. 이러한 경제적 이익을 보존하기 위하여, 소비자들은 네트워크화 기술에 대한 신뢰를 계속해서 가져야만 한다. 소비자 개인정보 보호의 강화는 이러한 목표를 이루는데 일조하게 될 것이다.

신뢰를 유지하는 것은 또한 네트워크화 기술에 대한 전체 사회 및 문화의 이익을 인식하는 것이 필요하다. 그러나 기업들이 소비자들이 공개한 정보하의 상황에 모순되는 방식으로, 개인 정보를 사용할 때, 그들은 아마도 신뢰기반을 약화시킬지도 모른다. 예를 들어, 웹과 온라인 사회 연결망 사이트를 통하여 그들의 친구, 가족 및 동료 및 공공 일반과 함께 정보를 활발하게 공유하는 개인들은 그러한 서비스들의 방식과 제3자들을 모를 수도 있고, 그들 자신의 동료들과 그들에 관한 정보를 사용할지도 모른다. 민감한 정보에 대한 권한 없는 노출은 개인들의 권리를 침해할 수 있고, 손해 혹은 민감한 개인적 특성을 이유로 한 차별을 발생시킬 수도 있으며, 오해의 소지가 있거나

24) 이 체제(framework)는 오로지 어떻게 상업적 환경에서 민간부문 기업들이 개인정보를 처리할 것인가에 대한 것에 관련한다. 별개의 헌법과 법률적 보호는 정부가 개인 당사자의 소유권의 범위 내에 있는 정보에 접근하는 것에 적용되는 것이다. 게다가 1974년 사생활보호법(the Privacy Act of 1974, Pub. L. No. 93-579(5 U.S.C. § 552a))과 미연방 기획예산처(the Office of Management and Budget)의 이행 지침은 연방정부가 개인의 신원정보(personal identifiable information)를 통제하도록 하고 있다.

25) Cloud Computing이란, 인터넷 기반(Cloud)의 컴퓨터기술(Computing)을 의미하는 것으로, 여기에서 구름(Cloud)은 컴퓨터 네트워크 상에 숨겨진 복잡한 인프라 구조, 인터넷을 뜻함

부정확한 정보에 대하여 책임을 져야할 행동과 결정을 발생시키고, 많은 비용이 들고 잠재적으로 일상에 지장을 주는 신원도용을 야기할 수도 있다. 신원도용을 금지하고 신원도용에 대하여 기소하는 미국의 사생활 보호는 행정부에 중요한 초점이 맞춰져 있다.

현존하는 미국의 소비자 개인 사생활보호 체계는 디지털 시대에서 몇몇의 소비자 개인정보 보호를 유연성 있고 효과적으로 다루고 있다. 이 체제는 산업 성공사례(industry best practice), 연방통상위원회(FTC)의 집행, 그리고 최고 개인정보책임자들(chief privacy officers)의 연결 및 기술, 비즈니스 모형을 적용시키고, 기업 내에서 사생활보호의 문화 인식의 확대를 창출하여 사생활보호 정책을 발전시키는 기타 사생활보호 전문가들로 구성되어 있다.

그럼에도 불구하고, 인터넷상의 많은 양의 개인 정보들이 포괄적인 연방법률 상의 보호에 부합하지 않고 있는데, 그것은 대부분의 연방 프라이버시보호 법률들(Federal data privacy statutes)이 단지 온라인 정보 수집의 경우에 있어서의 공중 보건, 교육, 통신 및 금융 서비스, 혹은 아동에 대한 것과 같은 특정 분야들에만 적용되고 있기 때문이다. 행정부는 개개인이 네트워크화 기술에 대한 접근성을 가지며, 광범위한 기업들이 개인 정보를 수집하고 이용하는 넓은 범위에 걸쳐 있는 환경 속에서, 현존하는 체계의 빈틈을 메우는 것이야 말로 사생활 보호 관련 문제들에 대한 보다 일관성 있는 책임들을 촉진시킬 것이라고 믿고 있다. 그러나 행정부는 특정 부문에만 적용되는 현존하는 연방 법규들을 그들이 관련 기술들에 대한 기준에 모순되지 않는 한 수정할 것을 권고하지는 않는다. 대신에, 행정부는 기존 체제를 보완할 수 있고, 현재 연방법규들이 포괄하지 못하는 영역에 대한 보호에 대한 기준을 확대하는 법률 제정을 지원하고 있다.

여기에 놓여 있는 포괄적인 소비자 개인정보 체계는 소비자들에게 보다 명백한 보호들을 제공하게 될 것이다. 그것은 또한 혁신을 촉진

하고 규정 준수 비용(compliance costs : 행정명령 제13563(Executive Order 13563), “규제개혁 및 규제검토(Improving Regulation and Regulatory Review)”의 목표에 부합하는)을 최소화하면서, 기업들에 대해서도 보다 큰 확실성을 제공하게 될 것이다.

이 체제는 보다 나은 수단으로써의 디지털 경제에서, 개인정보의 흐름을 이해하고 통제하기를 원하는 소비자들을 위해 마련되었다. 그 목적은 앞 다투어 소비자들의 기대에 부합하려는 기업들이 소비자 및 정책자들을 참여시키는데 보다 효과적인 방식을 갖는 것을 보장한다. 이것은 기업들이 소비자들이 받아들일 만하고, 그들이 침해를 알아차릴만한 개인정보 정책들을 결정하는데 도움을 주게 될 것이다. 마지막으로, 행정부의 소비자 개인정보 체제는 소비자 및 기업들이 실제로 네트워크화 기술들을 어떻게 사용하는 지를 반영하는 국제적 정책 체제들을 촉진시킴으로써, 우리의 전 세계적인 경쟁력을 개선하게 될 것이다.

행정부의 소비자 개인정보에 대한 체계는 이러한 목표를 성취하기 위한 길을 제시하고 있다. 이것은 다음과 같은 핵심 요소들에 기초한다. ① 개인정보와 관련 있는 개인들의 권리 및 기업들의 관련 의무들을 마련한 소비자 프라이버시 권리장전(Consumer Privacy Bill of Rights)[26], ② 소비자 프라이버시 권리장전(Consumer Privacy Bill of Rights)이 특히 비즈니스 상에서 요구하는 사항들을 특정하기 위한 기초를 형성하기 위한, 다양한 이해관계인의 합의(multistakeholder processes)를 바탕으로 한 실효성 있는 법규의 제정(Enforceable codes of conduct), ③ 공정하지 못하거나 기만적인 법률과 정책을 금지하는 권한을 통한, 소비자 개인사생활 보호 권리들에 대한 연방통상위원회(FTC)의 집행, 그리고 ④ 미국의 소비자개인정보 보호 체계와 다른 국가들의 체계

26) 이러한 소비자 권리들은 인터넷 시대의 역동적인 환경을 제공하는 측면에서 연계되어 있는 발전적이며 전 지구적으로 인식되고 있는 공정정보규정(Fair Information Practice Principles, FIPPs)에 그 기반을 두고 있다.

간의 상호인정(mutual recognition)이다. 다양한 이해관계인들의 합의를 통한 법규명령의 발전 및 협력 강화(enforcement cooperation)를 통한 국제적 상호운용성(Global interoperability)의 증대는 정보의 흐름에 대한 장애를 줄일 수 있을 것이다.

제 2 절 소비자 프라이버시 권리장전의 주요 내용

1. 정의

미국의 공정정보규정(Fair Information Practice Principles, FIPPs)은 1970년대에 시작되었고, 이것은 전 세계적으로 소비자 개인정보보호에 대한 기본 원리로 오랫동안 인식되어 오고 있다. 소비자 프라이버시 권리장전은 이러한 공정정보규정(FIPPs)을 개인들에 관한 정보의 처리가 공정정보규정이 최초에 시작되었을 때에 비하여 훨씬 더 고도화되고 만연된 오늘날의 상황에서도 적용시킨다. 기업과 정부 기관들이 더 이상 전통적인 개인정보 수집자 혹은 처리자가 아니게 되었다. 세계는 훨씬 더 다양해지고 역동적이게 되었고, 기업은 늘어가는 광범위한 목적의 개인정보를 처리한다. 소비자들을 개인정보를 온라인 사회 연결망과 개인 블로그들(blogs)과 같은 유통 체계들을 통한 방식으로 점점 더 적극적으로 교환하고 있다. 개인정보의 구제는 소비자들에게 이익을 가져다 줄 뿐만 아니라 사생활 보호에 관한 어려운 문제들을 제기하는 혁신의 중요한 원천이 될 수 있다. 이러한 환경의 중심이 되는 도전과제는 기업에 대하여는 그들이 쇄신을 계속할 필요가 있다는 것에 대한 확실성을 제공하는 것이 되는 것인 반면, 소비자들에게는 그들의 사생활보호 기대의 보호가 될 것이다.

이러한 과제에 부합하기 위하여 소비자 프라이버시 권리장전은 다음의 두 가지 방식으로 공정정보규정을 수행하고 있다. 첫째, 소비자

들이 그들의 개인정보를 다루는 기업들에 대하여 그들이 기대해야만 하는 것을 소비자들에게 알려야하는 일체의 소비자 권리를 확인한다. 소비자 프라이버시 권리장전은 소비자들이 네트워크 사회에 대한 참여가 증가함에 따라, 기업들이 소비자들의 사생활을 보호하는 어떤 책임을 갖는다는 것을 확인하고 있는 것이다. 둘째, 소비자 프라이버시 권리장전은 그 적용에 있어서 개인정보 제공 목적 부합성(context)의 중요성을 강조하는 방법으로 공정정보규정(FIPPs)을 반영하고 있다. 개인정보 제공 목적의 부합성의 핵심요소는 소비자들이 기업의 상품 또는 서비스를 이용함으로써 얻을 것이라고 기대할 수 있는 목표나 목적들, 즉 기업들이 실제로 제공하는 서비스들, 이러한 서비스들을 제공하는데 필요한 개인정보의 교환들, 기업의 고객에 어린이와 청소년을 포함할 것인지 말 것인지를 포함한다. 개인정보 제공 목적의 부합성은 소비자 사생활보호 권리장전에서의 균형 및 상대적으로 특정한 원칙들을 구성해야만 한다.

소비자 사생활보호 권리장전은 소비자들이 다음에 관하여 갖는 권리를 유지시킴으로써 이러한 목적들을 발전시킨다.

- 개인정보통제(Individual Control)
- 사생활보호 및 보안정책의 공개(Transparency)
- 개인정보 제공 목적에 부합하는 수집・이용・공개(Respect for Context)
- 개인정보의 적절한 관리(Security)
- 개인정보의 접근가능성 및 정확성(Access and Accuracy)
- 필요한 정보만을 수집(Focused Collection)
- 책임성(Accountability)

소비자 사생활보호 권리장전은 개인정보의 상업적인 사용에 대하여 적용된다. 개인정보라는 이 용어는 특정 개인에 연결되어 있는 정보

의 집합을 포함하는 어떠한 정보를 말한다. 따라서 개인정보는 특정 컴퓨터나 다른 장치기구(device)와 연결된 정보를 포함하는 것일 수도 있다. 예를 들어, 스마트폰에 대한 식별자(identifier on a smartphone) 혹은 사용 내역(usage profile)이 작성되어 있는 가족의 컴퓨터는 개인정보에 해당한다. 이러한 정의는 영리기업들(commercial entities)이 수집・이용・공개하는, 소비자들에 관한 여러 가지 종류의 정보를 수집하는데 필요한 유연성을 제공하게 된다.

2. 주요 내용

(1) 개인정보통제

개인정보통제(Individual Control): 소비자들은 기업들이 그들로부터 어떤 개인정보를 수집하고, 그것을 어떻게 사용할 것인지에 대하여 통제를 행사할 권리를 갖는다. 기업들은 소비자들에게 소비자들이 다른 사람들과 공유하는 개인정보에 대한, 혹은 기업들이 개인정보를 어떻게 수집하고, 이용하거나 혹은 공개하는 지에 대한 적절한 통제를 제공해야만 한다. 기업들은 그들이 수집, 이용, 또는 공개하는 개인정보의 규모, 범위, 그리고 민감성(sensitivity)을 그들이 개인정보라고 생각하는 것을 이용하는 것에 대한 민감성과 함께 반영하여, 이용하기에 쉽고 접근 가능한 체계를 소비자들에게 제공함으로써, 이러한 선택들을 가능하게 해야만 한다. 기업들은 소비자들이 개인정보의 수집, 이용, 공개에 관하여 중요한 결정들을 소비자들이 내릴 수 있는 명확하고 간단한 선택들을 적절한 시기와 방법으로 제공해야만 한다. 기업들은 우선 첫째로, 접근가능하고 이용하기에 쉬운 승인의 방법 만큼이나 승인의 철회(withdraw) 및 제한(limit)에 대한 수단을 소비자들에게 제공해야만 한다.

개인정보통제(Individual Control) 원칙은 두 가지 차원이 있다. 첫째, 수집하는 시기에, 기업들이 정보를 공유, 수집, 이용 및 규모와 범위,

문제가 될 수 있는 개인정보의 민감성에 적합한 공개에 관하여 선택을 표현해야만 한다. 예를 들면, 개인 인터넷 사용 내역, 이를 테면 검색 엔진, 무선 네트워크(ad networks), 그리고 온라인 사회연결망과 같은 중요한 부분에 관하여 평가를 갖는 기업들은 시간이 지남에 따라 개인들의 행위양식(behavior)에 대한 상세한 개요(profiles)를 만들 수 있다. 이러한 개요들은 범위에 있어서 넓고, 규모에 있어서 클 수도 있고, 개인의 건강 또는 금융 정보와 같은 민감한 정보를 포함하게 될는지도 모른다. 이러한 경우들에 있어서, 단일하고 분명하고, 매끄러운 개인정보의 이용과 공개를 제공하는 선택 체계(choice mechanisms)는 적절한 것이 될 것이다. 반대로, 개인과 합리적인 연관을 가진 정보를 수집하지 못하게 하는 서비스들은 제한적인 선택들을 제공하게 될 것이다.

어떠한 경우에도, 소비자 정보를 직접 다루는 기업은 기업이 그 정보를 그 자체로 쓸 것인지 또는 그것을 제3자에게 공개할지의 여부에 상관없이, 기업들이 수집하는 개인정보가 무엇인지에 관하여 그들에게 적절한 선택을 주어야만 한다. 소비자를 직접 대하는 기업들(consumer-facing companies)이 소비자들로부터 직접적으로 개인정보를 모으는 제3의 당사자들과 계약을 행할 때, 그들은 그러한 제3자들이 개인 정보를 어떻게 이용하고, 수집・이용・공개에 관하여 소비자들에게 적절한 선택을 제공할지의 여부에 관하여 성실한 요구가 행해져야만 한다. 행정부는 또한 그들 자신 그리고 그들의 사업 파트너들과 수집하는 개인정보에 대하여 승무원들과 같은 역할을 하는 소비자 직접 상대 기업들을 원조하고 있다. 소비자 직접상대 기업들은 소비자들의 관점에서, 단일하고, 지속적이고, 측정 가능한 체계들(mechanisms)을 통하여 소비자 선택(consumer choices)을 인식할 수 있는 방법을 찾아야만 한다.

제3자들 역시 규모, 범위, 및 그들이 수집하는 정보의 민감성에 대하여 적절한 개인정보 수집에 관한 선택들을 제공해야만 한다. 최근 몇 년 동안, 제3자 개인정보 수집에 관한 논의의 초점은 온라인 광고 행위(online behavior advertising)[27]에 있었다. 이러한 광고체계는 개별적인 소비자들을 끌어들일 수 있는 무선 네트워크를 중심으로 다른 웹 사이트를 거쳐서 돌아간다. 이러한 정보가 독특한 식별자들(identifiers)에 따라 구조화되었을 때, 이것은 잠재적으로 광범위한 개인의 인터넷 사용의 관점을 제공할 수 있다. 이러한 개별적인 행위의 개요들은 인터넷 사용에 의하여 드러난 것에 따라, 광고업체들로 하여금 개인의 취향에 관한 영향에 기반을 둔 무선 네트워크를 목표로 하는 것을 가능하게 한다. 특정 대상이 된 수신 광고(targeted ads)들은 일반적으로 문맥 광고(contextual ads)에 비하여 보다 가치가 높고 효율적이며, 다수의 무료 온라인 콘텐츠나 서비스들을 지지하는 수입(revenue)을 제공한다. 그럼에도 불구하고, 많은 소비자 및 민간 지지자들은 그들의 사생활보호에 대한 기대를 침해할 수 있는 추적(tracking)과 광고(advertising)를 찾고 있다.

행정부는 무선 네트워크와 같은 제3자가 수집한 개인정보의 궁극적인 사용이 사생활 보호 이익에 중대한 영향을 미치고 있음을 인지하고 있다. 결과적으로, 이러한 개인정보의 사용은 적절한 개인정보통제(individual control) 선택의 범위를 형성하는데 틀림없이 도움을 주게 될 것이다. 예를 들어, 소비자들이 그 서비스를 어떻게 사용하는지에 관하여 단지 통계만을 계산한 개인정보를 사용하는 회사는 중요한 소비자의 사생활 이익에 누를 끼치지 않을 것이며, 이러한 목적을 위하여 수집된 정보를 보호하는 방식들로써 소비자들에게 제공할 필요도 없을 것이다. 기업이 몇 가지 사용에 관하여 어떤 개인정보를 수집하

27) 소비자들을 대상으로 광고하기 위해서 온라인상 소비자들의 관심에 대한 정보를 수집하는 행위들

고 저장하였다 하더라도, 수집에 관하여 정교한 방식의 선택을 소비자들에게 제공할 필요가 없을 것이다. 예를 들어, 온라인 광고의 경우를 보자면, 광고전달(ad delivery)을 다양화하고 소비자들에게 같은 광고를 여러 차례에 걸쳐 보는 것을 금지하는 것은 얼마간의 개인정보 수집을 요청하는 것일 수도 있다. 그러나 단지 통계적 목적으로만 수집된 개인정보는 대규모의 장기적인 개별 정보의 개요들의 총체를 요구할 필요가 없을 것이며, 통제를 위하여 광범위한 선택들을 요구하지도 않을 것이다.

혁신적인 기술은 사용자의 통제의 범위를 확장시키는 것을 도울 수 있다. 소비자들과 직접적인 관계를 맺는 인터넷 회사들이 개인들이 기업이 수집하는 개인정보가 무엇이며 언제 수집하는지에 대한 보다 넓은 통제를 실행하는 것을 가능하게 하는 상세한 사생활 정보들을 제공하는 것은 점점 일반화되어 가고 있다. 게다가, “개인정보 추적(Do Not Track)” 장치와 같은 개인정보 강화 기술들은 소비자들로 하여금 제3자가 개인정보를 어떻게 사용할 것인지 혹은 전혀 받지 못하게 할지의 여부에 대한 어떤 통제를 실행하는 것을 가능하게 한다. 예를 들어, 연방통상위원회(FTC)에 의하여 촉구된, 제3자 광고들의 온라인 광고 산업의 회원들은 공정정보규정(FIPPs)에 기반을 둔 자체 법규 원리들(self-regulatory principles), 존재에 대하여 소비자들에게 알려주고 관련 광고 네트워크에 관한 더 많은 정보를 가르쳐주는 공용 인터페이스(common interface) 및 개별 광고 네트워크에 의하여 소비자들이 타깃 광고 밖으로 빠져나올 수 있도록 하는 일반 기제(common mechanism)를 발전시켰다. 브라우저 업체들(browser vendors), 소프트웨어 개발자(software developers), 그리고 기술표준 기구(standards-setting organizations)을 포함하는 다양한 다른 행위자들은 소비자들에게 제3자가 개인정보를 받을지의 여부에 관하여 어느 정도의 통제를 행할 수 있게 하는, “개인정보 추적(Do Not Track)” 체계를 발전시켜 나가

고 있다. 이러한 모든 기제들(mechanisms)은 장래성이 있는 것이다. 그러나 그들을 쉽게 이용하고, 개인정보의 혁신적인 사용들과 균형을 유지하고, 보안 이익을 고려하며, 개인정보 수집의 잠재적 비용에 대한 명백한 상을 제시하고 이를 제한하는 이익을 보장하기 위해서는 더 나은 발전을 필요로 한다.

제3자가 소비자들과의 직접적인 상호작용으로부터 제거되면, 그들이 수비자들에게 정보 수집에 대한 중요한 통제를 제공하는 것이 보다 더 어렵게 된다. 예를 들어, 데이터 브로커(data broker)[28]는 다양한 소스로부터 개인정보를 모으며, 종종 이것은 소비자들과 어떠한 상호작용조차 없이도 일어난다. 그러한 기업들은 소비자들이 이러한 제3자들의 존재를 모를 수도 있는 까닭에 개인정보통제에 대한 효과적인 기제들을 제공하는 것에 대한 도전에 직면하고 있다. 게다가 일부 데이터 브로커들은 법원 기록, 뉴스 리포트, 재산 기록 및 다른 공공 기록에 있어서의 정보를 수집한다. 이러한 문서들을 수집하고 사용하는 것을 포함하는 언론과 출판의 자유에 대한 권리는 어떻게 그것들이 수집되고 이용되고 확산되는지에 대한 개인들에 대한 사생활 보안정책의 공개의 필요와 이미 수집된 정보들에 대하여 접근하고 정정하는 개인들의 기회 사이의 균형이 있어야만 한다.

여전히, 데이터 브로커들과 개인정보를 소비자들과 직접 상호작용이 없거나 혹은 합리적으로 소비자들을 직접 대면하는 탐지 가능한 존재가 없이 개인정보를 수집하는 기업들은 소비자들에게 개인정보통제을 제공하는 혁신적인 방법을 찾아야만 한다. 만약 개인정보통제를 제공하는 것이 현실적으로 어렵다면, 이들 기업들은 그들이 소비자들의 사생활을 보호하기에 적정한 방식으로 소비자 프라이버시 권리장전의

28) 데이터 베이스 서버에 접근해서 데이터를 처리하는 중개자 혹은 어떤 업무에 필요한 비즈니스 로직들을 따로 별도의 애플리케이션에 넣어 두는 애플리케이션 서버(application server), 클라이언트 프로그램과 데이터베이스 서버 사이에 위치해서 필요한 일들을 대신 처리해준다고 하여 이러한 명칭으로 불리 운다.

다른 요소들을 준수한다는 것을 보장해야만 한다. 예를 들어, 충분한 사생활 보호를 하기 위해서, 이러한 기업들은 소비자들과 직접적인 관계의 부재를 보충하기 위한 원칙인, 개인정보의 접근가능 및 정확성 확보와 책임성원칙들 하에서 수집된 정보에 대한 통제를 적절히 제공함과 동시에 그들이 개인 정보의 상업적인 이용을 하는 역할에 대한 명백하고 공적인 설명들을 제공함으로써 개인 사생활 및 보안정책의 공개와 같은 다른 원칙들을 준수하기 위하여 추가적인 노력을 할 필요가 있을 것이다.

개인정보통제의 두 번째 차원은 소비자 책임(consumer responsibility)에 있다. 온라인 사회연결망이 늘어감에 따라, 개인정보의 사용은 비공개설정을 선택할지 개인정보를 다른 사람들과 공유할 것인가의 개별적인 결정들로 시작된다. 이러한 상황에서, 소비자들은 그들의 선택을 평가하고, 그들이 결정한 것에 대하여 책임을 져야만 한다. 원래의 공유 행위에 대한 통제는 매우 중요하다. 소비자들은 그러한 결정들에 대하여 책임을 져야만 하는 데, 이것은 마치 단지 이러한 공유에 참여하고 이익을 얻는 기업들이 이용 가능한 수단과 분명한 설명들을 소비자들이 중요한 결정을 하는 것을 가능하게 제공해야만 하는 것과 같다.

개인정보통제원칙은 또한 개인정보에 존재하는 소비자들의 사생활 보호 이익이 그들의 기업들과 맺는 관계를 통하여 유지된다는 것을 확인하고 있다. 따라서 이 원칙은 기업이 지배하는 개인정보 사용에 대한 포괄적인 동의를 포함하는 권리이다. 기업들은 그들이 동의를 얻는 방식과 대등한 방식으로 포괄적인 동의의 수단을 제공해야만 한다. 예컨대, 소비자들이 그들의 컴퓨터에서 단일 행위를 통하여 동의를 보장한다면, 그들은 또한 비슷한 형태로 포괄적인 동의를 가능하게 해야만 한다.

포괄적 동의를 위한 권리에는 세 가지의 실질적인 한계가 있다. 첫째, 그것은 소비자들이 기업들과 계속해서 관계를 지속할 것으로 간주한다. 이러한 관계는 소비자들이 단발의 거래를 삼는 것과 같이 최소한의 것일 수가 있다. 혹은 그것은 몇 년에 걸쳐서 일어나는 많은 금융적 거래와 같이 대규모의 것일 수도 있다. 그럼에도 불구하고, 기업은 이 기업이 개인들과 연결이 계속되고 유지되는 정도의 동의에 관하여 포괄성에 영향을 끼치는 방법을 가지게 될 것이다. 반대로, 기업이 합리적으로 개인들과 연결될 수 없는 정보는 포괄적 동의의 권리의 주제가 되지 않는다. 둘째, 소비자들의 포괄적 동의에 관점에서의 의무는 단지 기업이 이러한 통제 하에서 가지는 정보에 대한 것에만 미친다. 셋째, 개인정보통제 원칙은, 만약 그들이 그 정보의 수집 당시에 그러한 계약을 하지 않았다면, 기업들이 소비자 사생활보호 권리장전의 시행 이전에 수집했던 개인 정보에 대하여, 포괄적 동의를 허락받을 것이 요구하지 않는다.

(2) 사생활보호 및 보안정책의 공개

사생활보호 및 보안정책의 공개(TRANSPARENCY): 소비자들은 사생활보호 및 보안정책들에 관한 정보를 쉽게 이해하고 접근할 권리를 가진다. 사생활의 위험에 대한 중요한 이해와 개인정보통제(Individual Control)을 행사할 수 있는 능력을 얻는 것을 최대한 가능하게 하는 시간과 공간에서, 기업들은 어떠한 개인정보를 그들이 수집하며, 그들이 그 정보가 왜 필요하고, 어떻게 그것을 이용할 것이며, 언제 그 정보를 삭제(delete) 혹은 소비자들로부터 그것을 익명화시킬(de-identify) 것인지, 그리고 그들이 제3자에게 개인정보를 제공할 것인지 아닌지 무엇을 위해서 할 것인지에 대한 명확한 설명(descriptions)을 제공해야만 한다.

개인정보의 수집, 이용, 공개 및 유지에 관한 일반적인 설명은 소비자들이 상업적 상호 작용의 주변 용어들을 이해하는 것을 돕는다. 기업들은 그것들이 현저한 사생활 보호의 위험에 관련성이 큰 것인 경우, 이러한 설명들을 소비자들이 알아 볼 수 있도록 해야 하며, 알아볼 수 있도록 해달라는 요청이 있을 때에는 쉽게 이용이 가능하게 해야만 한다. 기업 대 소비자들의 상호작용, 혹은 관계라는 맥락에 부합하지 않는 개인정보 이용은 필수적이거나 그러한 맥락을 일반적으로 받아들인 개인정보 이용에 비하여 보다 더 중요한 노출을 받게 되기 마련이다. 이러한 방법으로 개인정보를 구별하는 개인정보 처리방침은 일반적으로 모든 개인정보 이용에 대하여 동일한 정도로 강조하는, 소비자들이 참여하지 않았거나 최근 여러 가지의 개인정보 처리방침과 비교해 보지 않은 개인정보 이용에 비하여 소비자들에게 더 나은 정보를 주게 될 것이다. 이러한 개인정보 처리방침은 사생활보호에 민감한 소비자들이 그것들과 관련한 정보로의 접근을 보다 용이하게 할 것이다. 이것은 또한 기업들에 의하여 공개에 있어서 보다 더 많은 일관성을 촉진하게 되고, 일상적으로 개인정보 처리방침을 무시하며, 잠재적으로 사생활 보호를 다른 상품과 서비스 사이의 경쟁에서 훨씬 더 핵심적인 것으로 만드는 소비자들의 관심을 끌게 될지도 모른다.

게다가, 기업들은 소비자들이 실질적으로 그들의 서비스에 접근하는데 사용하는 장치들을 읽기 쉬운 형식으로 개인정보 처리방침을 제공해야만 한다. 특히, 모바일 장치들은 개인정보 처리방침 전문을 효과적으로 읽는 것이 불가능한 작은 액정을 가지고 있다. 따라서 기업들은 모바일 소비자들에게는 작은 사이즈의 디스플레이나, 모바일 장치들에 특수한 사생활 보호의 위험들과 같은 모바일 장치의 특성을 참작하는 방식으로 가장 적절한 정보를 표시하려는 노력을 해야만 한다.

마지막으로, 소비자들과 직접적으로 상호작용하지 않는 기업들, 말하자면 앞서 논의했던, 데이터 브로커들과 같은 경우 그들이 개인정보를 습득하고, 이용하고, 공개하는 방법에 대한 유효하고 명쾌한 설명을 해야 할 필요가 있다. 이러한 기업들은 예컨대, 그들의 웹사이트 혹은 다른 공개적인 접속처에 대하여 게시함으로써, 이러한 설명을 유효하게 만드는 경우, 직접적 관계의 부재를 보충할 수 있을 것이다. 게다가 소비자들과 일차적인 관계를 가지는 기업들은 특히 그들이 개인정보를 제3자에게 제공하는 목적을 공개해야만 하고, 소비자들에게 그러한 제3자의 행위들의 본질 및 이들 제3자들이 그러한 목적을 성취하기 위하여 그들의 데이터 사용에 한계를 가지고 있다는 점을 이해시키려고 노력해야만 한다. 이것은 제3자들이 어떤 개인정보를 취하고 또 그것을 어떻게 사용하는지를 이해하려고 노력하는 것에 비하여, 소비자들에게 단일 기구로 계약 할지의 여부를 평가하는 것이 보다 쉬운 일이 되게 한다. 이와 유사하게 1차 당사자들은 그들이 제3의 당사자들인 제3자들로부터, 그들이 어떠한 종류의 개인정보를 공개하는지, 또 이 정보를 어떻게 사용하는지를 공개함으로써 보다 큰 개인 사생활 및 보안정책의 공개를 창출할 수 있을 것이다. 이러한 보안정책의 수준은 또한 혁신적인 개인 사생활보호 강화 기술 및 소비자들이 그들의 사생활을 보호하기 위하여 이용할 수 있는 지침에 대한 민간부분에 있어서의 발전을 용이하게 할 수 있을 것이다.

(3) 개인정보 제공 목적에 부합하는 수집・이용・공개

개인정보 제공 목적에 부합하는 수집・이용・공개(RESPECT FOR CONTEXT) : 소비자들은 기업들이 소비자들이 정보를 제공한 목적에 부합한 방식으로 개인정보를 수집하고, 이용하고, 공개할 것으로 기대할 권리를 가진다. 기업들은 그들의 개인정보의 이용 및 공개에 관하여, 법적으로 다르게 이용해야하는 것이 요청되지 않는 한, 기업이 소비자들과 가지는 관계

> 및 소비자가 본래 개인정보를 공개했던 목적 모두에 부합하는, 그러한 목적에 대한 한계를 가져야만 한다. 만약 기업들이 개인정보를 다른 목적으로 이용하거나 공개한다면, 그들은 정보를 수집한 때 소비자들에 의하여 준수되고 소송이 가능한 방식으로 이러한 다른 목적들을 공개함으로써, 강화된 사생활 보호 및 보안정책의 공개 그리고 개인의 선택을 제공해야만 한다. 만약 정보 수집 후에, 기업들이 정보들이 공개된 목적에 부합하는 목적들을 위하여 개인정보를 이용 또는 공개하는 것을 결정하게 된다면, 그들은 강화된 사생활 보호 및 보안정책의 공개 그리고 개인의 선택의 수단을 제공해야만 한다. 마지막으로, 기업과 관계한 소비자들의 기술에 대한 연령과 친숙함은 목적에 대하여 중요한 요소가 된다. 기업들은 이러한 원칙하에 소비자들의 연령과 교양수준에 대하여, 적절한 방식으로 소비자들에 대한 의무를 다해야만 한다. 특히, 소비자 사생활보호 권리장전의 원칙들은 어른들에 대한 것보다는 어린이나 청소년들로부터 획득한 개인정보에 대하여 보다 많은 것을 요구하고 있을지도 모른다.

개인정보 제공 목적에 부합하는 정보의 수집・이용・공개는 소비자들이 비즈니스 과정에서 이 서비스나 애플리케이션을 제공해야할 필요와 더불어 서비스 또는 애플리케이션을 사용하기 위한 목적에 어떻게 하면 최대한 부합할 것인가에 기초한 개인정보의 사용을 구분 짓는다. 이 원칙은 공정정보규정(FIPPs)의 규정들에서부터 일반적으로 발견되는 두 가지 원칙을 파생시킨다. 첫 번째 원칙인 목적의 특정(purpose specification)은 기업들이 그들이 개인 정보를 수집하기 위한 목적을 수집 당시에 특정해야한다는 것을 정하고 있다. 두 번째, 이용제한 원칙(the use limitation principle)은 기업들이 정해진 목적들을 수행하기 위해서만 개인정보를 사용해야한다는 것을 포함하고 있다. 정보 제공목적 부합성의 원칙은 두 가지 방식으로 이러한 안정된 원칙들을 적용하고 있다. 정보 제공목적 부합성은 회사들이 그들의 기초적인 개인정보 정책들에 관한 결정을 실질적 기준으로 이끄는 것을

가능하게 한다. 일반적으로 말해서, 기업들은 개인정보의 사용에 소비자들이 개인정보를 공개에 부합하는 목적을 이행하는 것으로 한계를 가져야만 한다. 또한 이러한 원칙이 소비자가 정보를 공개할 당시의 소비자와 기업 사이의 관계의 중요성을 강조하는 반면, 이것은 또한 이러한 관계가 시간이 지남에 따라 수집 당시에는 알 수 없는 방식으로 변하게 될 수도 있다. 이러한 개인정보의 조정적인 이용은 소비자들에게 이익을 가져다주는 혁신의 근원처가 될 지도 모른다. 그러나 기업들은 개인 정보의 재사용 이전에, 적절한 수준의 개인사생활 및 보안정책의 공개 및 개별적 선택권을 제공해야만 한다.

특정 목적에 대하여서만 정보를 제공하는 방식에 대한 소비자 프라이버시 권리장전 적용은 기업들로 하여금 유연성을 제공함과 동시에 그들에게 소비자들이 그들이 제공한 상품이나 서비스에 기초한 그들의 정보 정책에 관하여 무엇을 이해할 수 있으며, 기업 자신이 개인정보를 가져오는 역할을 설명하고, 소비자들의 태도 및 이해를 구하며, 소비자들로부터 피드백 할 것인지를 보다 주의 깊게 고려할 것을 요청하고 있다. 제공목적은 개인정보 이용이 소비자의 사생활 보호를 극대화할 수 있는지를 결정하는 것에 기여해야 한다. 기업 대 소비자 관계는 개인정보 처리방침에서 가장 중요한 것이 될 개인정보의 이용에 관한 결정을 이끌어야만 한다. 예컨대, 온라인 소매상들은 소비자들의 주문을 이행하는 배송을 하기 위하여 소비자들의 이름과 집주소를 공개할 필요가 있다. 이러한 공개는 소비자-소매상 관계의 맥락으로부터 분명한 것이다. 소매상들은 그들이 그것을 그들의 개인정보 처리방침 전문에 공개해야함에도 불구하고 중요한 정책에 대한 방침을 제공할 필요가 없다. 기업은 소비자들의 구매와 주문 행위 및 상품의 배달 절차에 대한 광의의 양해에 근거하여 소비자들이 이러한 공개를 동의했을 것이라고 추측할 수 있다.

정보 정책의 몇몇 범주는 많은 목적들에 대하여 일반적이면서 동시에 기업의 운영에 대하여 통합적이다. 앞의 예들은 보다 일반적인 범위의 상품과 서비스 이행으로 귀결된다. 기업들은 소비자들이 그 서비스에 대하여 일반적인 양해가 있기만 하면, 소비자들이 특별히 요청했던 목적들을 성취하기 위한 개인정보를 이용하고 공개하는 것을 동의하였다고 간주한다. 이와 비슷하게, 기업들은 대부분이 이와 같은 디지털 활동 및 개인 상행위에서의 활동의 유사성, 이러한 종류의 판매에 대한 가시성, 그리고 피드백을 제공하는 계약을 하는 당사자를 쉽게 분별할 수 있고, 만약 그들이 그것이 만족스럽지 않을 경우에 회사와 그들의 관계를 끝내는 소비자들의 기회가 있음으로 말미암아, 첫 번째 계약 당사자 관계의 판매에서 허락된 개인정보 사용을 동의했다고 간주하게 될 것이다. 예를 들어, 소비자들이 서비스를 개선하기 위하여 어떤 서비스를 사용하는 방법을 분석하고, 사기를 방지하고, 법률 집행 명령 및 기타의 법적 의무들을 준수하고, 지적 재산권을 보호하는 것은 이제까지 모두, 사업을 경영하고, 기업의 법적 의무를 지키는 것의 기본적인 요소들이 되어 왔다. 기업들은 소비자들이 개인정보를 이러한 목적에 맞는 만큼, 소비자 사생활보호 권리장전에서의 다른 원칙들에 부합하는 것에 대하여서만 수집을 동의했다고 추론할 수 있어야 한다.

또 다른 경우에 있어서, 목적 부합성은 소비자의 통제권을 보장하기 위한 기회들이 기업들이 제공하는 것에 대하여서도 합리적이고 동시에 소비자들에게도 중요한 내용과 관련 있는 결정을 이끌어 내야만 한다. 어떤 목적에 있어서 소비자들에게 중요한 정보나 선택들은 크게 봐서 다른 이들에게는 상관이 없는 것일 수도 있다. 예컨대, 소비자들에게 게임 상태를 저장해주어, 그들이 잠시 쉬었다가도 게임을 재개하는 것을 가능하게 하는, 모바일 기기를 통한 가상 게임 애플리케이션을 생각해 보면, 이런 게임을 제공하는 가상 기업은 제공하는

게임 내용 진행상황을 저장하기 위한 목적을 위한 이러한 “저장(save)” 기능을 제공하기 위하여 각 사용자의 모바일 기기의 고유한 식별자(unique identifier)를 수집한다. 이러한 목적을 위하여, 모바일 기기의 고유한 식별자를 수집하는 것은 이 “저장” 기능과 소비자들이 그것을 사용할 것인지에 대한 결정에 부합되어야만 하고, 특히 회사가 단지 이 목적으로만 식별자를 이용하는 경우에 그러하다. 그럼에도 불구하고, 만약 기업이 소비자들의 고유한 기기 식별자들을 제삼자에게 온라인 광고행위와 같은 목적으로 제공한다면, 기업은 소비자들에게 공지해야만 하고 그들에게 개인정보를 차단하는 것을 가능하게 해야만 한다.

기업의 소비자들에 대한 성숙도는 목적 부합성의 또 하나의 중요한 요소이다. 특히, 사생활 보호 체계는 어른에게 적용되는 보호에 대하여, 이 연령층의 특유의 성격으로 말미암아 아동과 청소년의 사생활 보호 이익에 대한 보호의 정도를 다르게 요청하고 있다. 아동은 사생활 침해에 대하여 특히 더 민감할 수도 있다. 최근에, 아동 온라인 사생활 보호법(the Children's Online Privacy Protection Act, COPPA)[29]과 연방통상위원회(FTC)의 이행 규정들은 아동과 직접적인 관계가 있거나, 혹은 그들이 아동으로부터 개인정보를 수집하고 있다는 것을 아는 온라인 서비스들에게 그들이 그러한 정보를 수집하기 전에 입증 가능한 방식으로 부모의 동의를 취득하도록 요구함으로써, 강력한 보호들을 제시하고 있다. 아동들과 “직접 관계가 있는(directed to)” 온라인 서비스들은 이와 동일한 기준에 부합하여야만 한다. 행정부는 소비자 프라이버시 보호 권리장전에 온라인 서비스들이 개인정보 수집에 대한 필수적인 동의를 취득했다고 할지라도, 아동에 대하여 개별 사용내역들(individual profiles)을 창출하지 않는다는 동의와 같은 보다

29) 인터넷에서 13세 미만 어린이의 개인 정보를 마음대로 수집하지 못하게 제한한 미국 연방통상위원회(FTC) 관할 법률

엄격한 애플리케이션이 아동의 사생활을 보호하기에 적절한 것인지 아닌 지에 대하여 이해관계인들과 함께 해결점을 찾고 있는 중이다.

기업 대 소비자 관계를 규율하는 조항들은 목적 부합성의 또 다른 중요 사항이다. 특히, 광고는 혁신적인 새로운 서비스들을 지원하고, 소비자들에게 광범위한 온라인 서비스 및 애플리케이션의 무상으로 접근하는 것을 가능하게 한다. 개인정보 제공목적에 부합하는 수집・이용・공개 원칙은 어떠한 특정한 광고 기반의 사업 모형들을 담보하지 않는다. 그보다 이 원칙은 다른 개인정보에 기반을 둔 사업 모형들이 또 다른 사생활 보호 위험을 발생시킬 수 있음을 기업들에게 인식할 것을 요청하고 있다. 기업은 그들이 제공하는 개인정보를 위하여 무엇을 교환하고 있는지에 대하여 소비자들에게 분명한 정보를 주어야만 한다. 행정부는 또한 기업들로 하여금 소비자들에게 중요한 사생활 침해를 가져올 수도 있는 고용, 신용, 보험계약 적격 혹은 그와 유사한 문제들에 관하여 의사결정에 쓰여 질 수 있는 개인정보의 수집, 이용, 혹은 공개를 온라인 광고에서 금지하도록 독려하고 있다. 그러한 민감한 이용을 위한 정보 수집은 목적의 부합성에 있어서 수익을 창출하고 그들이 관련 있는 것을 보다 찾기 쉬운 광고를 소비자들에게 제공하려는 분명한 목적과 상충된다. 그러한 정책들은 또한 개인정보 제공목적에 부합하는 수집・이용・공개 원칙이 독려하고 있는 책임 있는 데이터 관리의 개념에 상충하게 될 수도 있다.

예컨대, 계좌를 개설할 때, 사용자의 생물학적 정보를 공개하고, 그들의 사회생활에서의 계약 및 친구, 사업상의 동료들, 그리고 그들의 네트워크상의 동료들을 포함하는 관심사들을 제공하는 온라인 사회 연결망 서비스가 있다고 생각해보면 소비자들이 이 서비스를 이용하는 동안, 그들은 온라인 사회 연결망에서 새로운 글 작성, 사진, 동영상 및 위치 정보를 포함한, 그들의 정체성과 관련한 엄청난 양의 정보를 창출해 내게 될 것이다. 소비자들은 이러한 정보를 그들의 온라

인 사회 연결망의 회원들과 공유하기 위하여 동의의 선택들을 하게 된다. 이러한 정보 공개들은 모두 그것의 사회 연결망 서비스를 제공하는 기업들에게 통합된다. 게다가, 이것은 기업들이 소비자들이 새로운 연결을 형성하는 것을 도와주기 위하여 다른 회원들에 대하여 이러한 최소한의 세부 정보들을 보여주는 것은 합리적인 것이다.

온라인 사회 연결망 서비스 제공자가 이러한 정보를 사용할 것인지 말 것인지, 그리고 무슨 목적인지는 소비자의 경험이라는 문맥상 그다지 분명하지 않다. 소비자들이 창출하는 개인정보는 이 서비스를 개선하고, 온라인 광고를 팔거나, 기업이 제3자에게 제공하는 개별 사용내역을 모으는데 있어서 가치가 있는 것일지도 모른다. 소비자들을 기업들이 그 서비스를 개선시키는 것에 대하여 기대한다. 기업은 항상 현재 보유중인 정보를 서비스를 개선하는데 사용하거나, 개인 정보의 이러한 새로운 사용이 사회 연결망의 상황에서 사용자들이 기대하는 것에 부합하도록 제공 되어진, 새로운 서비스를 창출하는 것에서 조차, 이것을 사용하기 위하여 긍정적인 동의(affirmative consent)를 얻는 노력을 해서는 안 된다.

기업이 개인의 사용내역 정보를 정보 브로커들(information brokers)[30]과 같은 제3자에게 누출시켰다고 가정해 보면, 개인정보 제공목적에 부합하는 수집・이용・공개 원칙은 기업으로 하여금 수령인이 이러한 정보를 구성할 지도 모르는 각각의 이용을 특정 하는 것을 요구하고 있지는 않지만, 최소한, 기업이 개인정보를 보다 더 종합하고 다른 목적으로 이것을 사용할지도 모르는 제3자에게 공개하는 것은 분명하고 확실하게 설명할 것을 요구할 지도 모른다. 개인정보 제공목적에 부합하는 수집・이용・공개 원칙은 또한, 소비자 사생활보호 권리장전에서 다른 원칙들과 결합하여 기업들에게 이러한 노출을 막기 위한 중요한 기회를 소비자들에게 제공할 것을 요청하고 있다.

30) 연구나 기업스파이를 통해 얻은 기업 정보를 판매하는 사람

(4) 개인정보의 적절한 관리

> **개인정보의 적절한 관리(SECURITY)**: 소비자는 개인정보의 안전하고 책임 있는 처리에 대한 권리를 갖는다. 기업들은 개인사생활과 그들의 개인정보정책과 관련 있는 보안 위험들이 가령 손해(loss)와 같은 위험들을 통제하는 합리적인 보호 장치(safeguards)를 유지하고 있는 지를 평가해야만 한다.

개인정보의 보안을 지키기 위한 기술과 절차들은 소비자의 사생활을 보호하는데 필수적인 것이다. 사고에서건 정밀공격에 의해서 비롯된 결과이건, 개인정보를 수반하는 보안 실패는 금전적 손실 및 물리적 해악에 대한 당황스러운 정도의 피해를 유발할 수 있다. 개인정보에 대한 통제를 상실한 기업들은 만약 사업 파트너 혹은 소비자가 안전 위반 이후에 관계를 종료한다면, 금전적 손실뿐만 아니라 명성에 있어서도 손해를 감수해야만 할 것이다. 이러한 결과들은 기업들에게 개인정보 안전보장을 지키기 위한 중요한 장려책이 될 수 있다. 기존 회사들에 있어서 적절한 보안대비책들은 그들의 사업 방침, 기업이 수집하는 개인정보의 종류, 소비자에 대한 침해의 가능성, 그리고 여러 가지 다른 요소들에 따라 달라질 것이다.

보안 원칙은 이러한 필요성들을 인식하고 있다. 보안 원칙들은 기업들이 정보의 보안에 관한 위반이 일어났을 때, 그들이 소비자들 및 법집행 기관들에게 공지해야하는 의무, 그리고 합리적인 보안 정책들을 적용하기 위한 공약들을 포함하는, 어떠한 적용 가능한 정보 보호 규정 하에서도 그들의 의무를 유지하고 부합시키는 개인정보의 규모와 범위를 가장 잘 정하기 위한 기술과 절차들을 선택하는 데 기준을 제시한다.

(5) 개인정보의 접근가능성 및 정확성

개인정보의 접근가능성 및 정확성(ACCESS AND ACCURACY): 소비자들은 개인정보에 대한 접근권을 가지며, 예민한 정보 및 그 정보가 부정확한 경우에 소비자에게 부정적인 결과를 초래할 위험에 대하여 적절하고 이용 가능한 형식으로 개인정보를 정정할 권리를 갖는다. 기업들은 그들이 정확한 개인정보를 보장하기 위한 합리적인 수단을 사용해야만 한다. 기업은 또한 소비자들에게 그들이 그것에 관하여 수집하고 유지하고 있는 개인정보에 대한 합리적인 접근은 제공해야만 할 뿐만 아니라, 부정확한 정보를 정정할 적절한 수단과 기회 혹은 정보의 삭제나 이용의 제한을 요청에 응해야 한다. 개인정보를 처리하는 기업들은 이러한 원칙을 표현과 출판의 자유에 부합하게 해석해야만 한다. 그들이 정확도를 유지하기 위하여 그리고 소비자들에게 접근, 정정 또는 억제력을 제공할 것인지를 결정하기 위해서, 그들이 수집하고 유지하는 개인정보의 규모, 범위 및 민감성을 그리고 그 사용이 소비자들을 금융적으로, 신체적이거나 또는 물리적인 해에 노출시킬 수도 있는 공산을 또한 고려해야할지도 모른다.

점점 늘어가는 다양한 기업들이 그들이 보는 온라인 광고로부터 고용 후보에 이르기까지의 범위에 있어서의 소비자들에게 영향을 미치는 의사결정을 하는데 개인정보를 사용하고 있다. 연방 의료보험 통상 책임법(the Health Insurance Portability and Accountability Act, HIPAA)과 공정 신용보호법(the Fair Credit Reporting Act)과 같은 특정한 연방 사생활 보호법에 의하여 처리되는 분야 외의 것에서, 소비자들은 현재 이 정보에 대한 접근 및 정정 권한을 가지고 있지 않다. 행정부는 혁신, 보안정책의 공개성, 참여 및 협조에 대한 목적을 향상시키기 위한 기계가독형식으로의 인터넷에 대한 데이터 출판에 헌신적이다. 예를 들어, 전력의 전송에 있어서 혁신과 효율성을 촉진시키

기 위하여, 행정부는 소비자들이 적시에 인터넷에 대하여 표준화되고 기계가독적인 형식으로 에너지 사용 정보에 접근하도록 지원한다. 이와 비슷하게, 전자 의료 기록을 통한 개인의료 정보로의 환자들의 접근을 포함한, 개인의료정보기술(Health IT, Health information technology)의 이용의 확대는 행정부의 혁신 전략의 핵심요소이다. 양쪽 모두의 목적에 부합하는, 포괄적인 사생활 보호 및 보안 강화 전략들은 양쪽 모두에 대한 근간을 이룬다.

소비자들에게 이용 가능한 형식으로 그들에 관한 정보에 대한 접근을 제공하는 것은 상업계에서의 계약과 유사하다. 소비자들이 보다 더 선택에 대하여 알 수 있도록 돕기 위하여, 행정부는 기업들에게 개인 정보를 인터넷에 대한 자격이 적절하게 증명된 개인들이 이용할 수 있는 형식으로 만들 것을 독려하고 있다.

개인정보의 접근가능 및 정확성 확보원칙은 부정확한 개인정보의 사용이 어떤 종류의 침해를 야기할 수 있는 가능성을 인정한다. 이러한 침해의 위험은, 기업이 보유하고 있는 개인정보의 규모, 범위 및 민감성과 더불어 무엇이 주어진 상황에서 접근과 정정의 편의가 합리적일 수 있는가를 결정하는데 도움이 된다. 결과적으로, 이 원칙은 소비자를 직접 대하는 기업과 그렇지 않은 기업들 사이를 구별하지 않는다. 그럼에도 불구하고, 모든 경우에 있어서, 기업들이 소비자들에게 그들에 관한 접근을 제공하는 기제들은 추가의 사생활 보호 혹은 보안 위험을 창출해서는 안 된다.

미국 헌법은 사생활보호 이익을 수정헌법 1조의 언론의 자유, 출판의 자유 및 단체결사의 자유에 대한 권리와 나란히 두었다. 그들의 자유로운 언론의 권리를 출판하는 개인 및 집단은 다른 개인들에 대하여 말하는 것과 그들의 언론에서 개인정보를 포함하는 것을 당연하게 여길 것이다. 그러므로 개인정보의 접근가능 및 정확성 확보원칙은 수정헌법 1조의 가치 전체에 기하여 해석되어야만 하며, 특

히 출판의 자유를 행사하는 비영리 언론 및 개인주체들에 대하여 그러하다.

(6) 필요한 정보만을 수집

> **필요한 정보만을 수집(Focused Collection)** : 소비자들은 기업들이 수집하고 유지하는 개인정보에 대하여 합리적으로 제한할 권리를 가진다. 기업들은 그들이 개인정보 제공목적에 부합원칙 하에서 특정되는 목적을 성취할 필요가 있는 한 최대한 많은 개인정보를 수집하려 할 것이다. 기업들은 만약 그들이 그렇게 하지 않을 법적 의무에 놓이지 않는 이상, 그들이 더 이상 그것을 필요로 하지 않게 되는 때 개인정보를 안전하게 공개 혹은 익명화시켜야만 한다.

필요한 정보만을 수집해야하는 원칙은 기업들이 특정한 목적을 완수하기 위하여 수집할 필요가 있는 데이터의 종류에 대하여 고려되는 결정과 연관이 있다. 예를 들어, 앞서 언급했었던 “저장” 기능을 제공하기 위하여 각각의 모바일 기기 장치의 고유한 식별자를 수집하는 가상게임 회사는 그 정보가 모바일 장치 식별자를 사용해야할지 말것인지 혹은 보다 덜 연결된 범위의 식별자로 작업을 해야 할지를 고려해야만 한다. 그럼에도 불구하고 개인정보 제공목적에 부합하는 수집・이용・공개원칙하에서 논의했던 바와 같이, 기업들은 그들이 정보를 수집한 이후에 개인정보를 위한, 공개성 및 개인의 선택이 적절하다고 주어진 새로운 이용처를 찾게 될 것이다.

광범위한 정보 수집은 몇몇의 친숙하고 사회적으로 이로운 인터넷 서비스 및 애플리케이션에 있어서 본질적인 것이다. 검색 엔진들이 그러한 것의 하나의 예이다. 검색 엔진은 월드와이드웹(the World Wide Web)의 내용과 구조에 관하여 세부적인 데이터를 모은다. 소비자들은 검색엔진을 이러한 광범위한 정보를 수집하고 그것을 다양한

최종적인 이용에 이용 가능한 것으로 만드는 것이라고 이해하고 의지한다. 검색엔진은 또한 그들의 서비스를 개선하기 위하여 검색 질문들을 기록한다. 검색 엔진은 그러한 정보를 수집하게 될 것이며, 그것은 개인정보 수집의 목적이 분명하고, 그들이 어떤 이러한 목적을 이루기 위하여 필요한 때 외에는 개인정보를 보유하지 않기만 하다면, 필요한 정보만을 수집해야하는 원칙에 부합한다는 식의 개인정보를 포함한다.

(7) 책임성

책임성(Accountability): 소비자들은 그들의 개인정보가 기업들에 의하여 소비자 프라이버시 권리장전을 충실히 따르기 위한 적절한 방식들로 처리될 권리를 가진다. 기업들은 소비자들에 대하여 이러한 원칙들을 준수하고 권한을 집행해야하는 책임이 있다. 기업들은 또한 이러한 원칙들을 고용인들에게도 준수하도록 해야만 한다. 이러한 결과를 얻기 위하여, 기업들은 이러한 원칙들에 부합하게 개인 정보를 처리하도록 그들의 고용인들을 훈련시켜야만 하고, 이러한 측면에서 그들의 실행이 정기적으로 평가받도록 해야만 한다. 적절한 곳에서, 기업들은 전체에 대하여 회계감사를 받아야만 한다. 개인정보를 제3자에게 공개하는 기업들은 그들이 그렇게 하지 않을 것을 법에 의하여 요청받고 있지 않는 한, 최소한 이러한 원칙들을 준수할 집행력 있는 계약상의 의무 하에 놓여 있는 수령자임을 확실히 해야만 한다.

프라이버시보호는 기업이 소비자 정보 프라이버시 보호를 집행하는 기관들과 마찬가지로 소비자들에게도 책임을 지고 있느냐에 달려 있다. 그러나 책임성의 원리는 기업들이 그들의 사생활 보호 공약에서의 일탈을 방지하고 일어날지도 모르는 어떠한 과실을 제거하고 구제하는 것을 통한 정책들을 아우르는 특별한 책임성을 초과하는 것이다. 기업들이 그들의 사생활 보호 공약들을 입증할 수 있다면, 그들은

소비자들의 신뢰를 유지하고 강화시켜주는 강력한 수단을 갖는 것이다. 기업 자신은 이러한 과정에서 따질 수 없을 만큼의 가치를 증명할 수 있다. 자체 평가가 될 수 있고 전체 감사를 필수적으로 요하지 않는, 적절한 수준의 평가 기술은 보유하고 있는 데이터의 민감성과 더불어, 기업의 사업에 있어서의 규모, 복잡성 및 본질에 따라 다르게 될 것이다. 최근 몇 년간, 최고정보보호책임자들이 유용한 안내 및 내부 평가자로서 나타나고 있다. 최고정보보호책임자들은 상품과 서비스들의 개발을 통하여 기업 내에서 연속적인 안내를 제공할 공산이 크다.

그럼에도 불구하고, 전반적으로 효과를 얻기 위하여, 기업들은 예정된 내부적 기대에 대한 집행을 위한 평가들을 연결해야만 한다. 평가들은 그 자체로 최종적인 것이 아니다. 회계는 회사에 의한 것이든 혹은 독립된 제3자에 의한 것이든 어떠한 상황 하에서 적절한 것이 될 수 있지만, 그것들이 항상 책임성의 원칙을 만족시켜야 할 필요는 없다. 게다가, 책임성은 하나의 기업에서 또 다른 기업으로 정보가 이전되면서 부가될 수도 있다. 소비자 프라이버시보호 권리장전의 관점에서, 중요한 것은 개인정보의 공개 자체가 아니라, 정보의 공개가 그것의 수집 목적에 부합하는 개인정보의 이용 혹은 정보를 통제하는 소비자들의 표현된 욕구를 이끌어 내느냐 아니냐에 있다. 그러므로 만약 기업이 개인정보를 제3자에게 이전하는 경우, 회사는 책임성을 가지며, 이에 따라 계약 혹은 다른 법적 집행 수단들을 통하여서 소비자 프라이버시보호 권리장전에 부합하는 방식으로, 정보를 사용하고 공개하는 것에 대한 수취인의 책임성도 지켜야만 한다.

제 3 절 소비자 사생활보호 권리장전의 이행

광범위한 개인정보의 혁신적인 이용을 통하여 소비자 프라이버시보호 권리장전에서의 일반 원칙들을 시행하는 것은 보다 구체적인 정책

들의 제정하는 과정을 필요로 한다. 행정부는 개별 기업들, 산업 그룹들, 민간 지지자들, 소비자 단체, 범죄 희생자들, 학계, 국제적 동반자들, 주법무부 장관, 연방 민·형사 집행대표기관, 기타의 관련 그룹들이 다양한 이해관계인들과 이러한 일반적인 원칙들을 시행하는 법규명령을 개발하는 과정을 장려하고 있다. 소비자 개인정보 보호에서, 행정부는 인터넷 정책에 영향을 미치는 다른 영역에서와 마찬가지로 다양한 이해관계인들이 인터넷의 성공에 대하여 책임을 지는 많은 제도들의 기저를 이루는 과정에 참여하고 있음을 인식하고 있다. 이 과정은 잘 알려지지 않고, 분권적이며, 사용자 중심인 소통, 혁신, 및 경제적 성장에 대한 플랫폼으로써의 인터넷을 보호하기 위한 행정부의 지속적인 공약을 반영하고 있다.

행정부는 공개적이고 투명한 다양한 이해관계인들과의 합의 절차들을 지원하고 있는데, 그것은 적절하게 잘 구조화 된다면, 그들이 유연성, 속도 및 분권화를 인터넷 정책 발전을 촉진시키는데 필수적인 것으로 만들 수 있기 때문이다. 광범위한 참여자에 대하여 열려 있고 그들 전체 참여를 용이하게 하는 이 절차는 기술 전문가들, 기업들, 민간 지지자들, 민·형사 법집행 대표기관들이 소비자 사생활보호 법률을 집행에 대하여 책임을 가지도록 할 것이며, 학계는 문제점들에 대한 창의적인 해법을 찾는데 함께 할 것이다. 심의 과정에서의 유연성은 이해관계인들이 인터넷 정책 이슈들에 대하여 기술 및 정책 차원들을 탐색하는 것을 가능하게 한다는 점에서 중요하다. 게다가 미국은 앞으로 몇 십 년 동안 광범위하고, 복잡하며, 세계 전체의 소비자 개인정보 보호 문제들에 맞서야 할 필요가 있을 것이다.

다양한 이해관계인들과의 합의절차의 또 다른 중요한 장점은 일반 절차들과 조약을 기반으로 한 기구들에 비하여 보다 시기적절한 해법들을 만들 수 있다는 점이다. 예를 들어, 인터넷 표준 세계에서, 실무그룹들은 종종 특정 문제와 관련된 형식을 가지며 몇 년이라기보다는

몇 개월 내에 해결하는 쪽으로 중요한 절차들을 만든다. 이들 그룹들은 종종 만장일치에 기초하여 역할을 하고 제한된 자원으로서의 개별 주체들이나 집단들의 참여를 수용한다. 이러한 특성들은 이 그룹들과 그들의 해결책들에 합법성을 부여하며, 차례로 신속하고 효율적인 이행을 촉진할 수 있다.

마지막으로, 다양한 이해관계인들과의 합의절차는 문제 해결에 있어서 단일의 집중된 권한에 의지 하지 않는다. 특정 이해관계 기관들은 특정한 종류의 인터넷 정책 과제들을 다루게 된다. 이러한 종류의 특정화는 해결책의 발전의 속도를 증가시킬 뿐만 아니라 이해관계인들의 노력의 중복을 피하는 데도 도움이 된다.

다양한 이해관계인들과의 합의절차에 의존하는 부분이 있기 때문에, 미국의 인터넷 정책은 일반적으로 혁신을 저해하고 소비자의 신뢰를 약화시키는 분열적이고, 권위적이며 예측이 불가능한 규칙들을 피해왔었다. 미국은 또한 정보화 기술 및 서비스에 대한 세계 시장을 분열시킬 수 있거나 혁신을 저해하는, 특정 기술적 요청들을 규정하는 법적 요청들을 삼가 왔다. 대신에, 미국은 일반적으로 인터넷 기술 표준을 만드는 전문 기구들을 따르고 있다. 게다가, 행정부는 개방적이고, 투명한, 인터넷 정책 과정들과 개별 주체 및 기업들에 대한 적절한 이행 의무들을 갖추고 있는 법적 체계 내에서의 협력 촉진을 계속해서 지원하고 있다.

소비자 개인정보 보호 문제는 다양한 이해관계인들과의 합의절차의 필요를 정책 및 일반적인 정책 원리들에 대한 기술적 필요를 발전시키는 전형적인 예로 들고 있다. 미국은 기업이 사생활 보호 정책을 혁신하는 작업을 맡기는 경우에, 기업과 소비자 양쪽 모두가 이익을 보았다는 것을 경험을 통하여 보여 주었다. 인터넷에서의 상업적 활동 초기 시절(1990년대 중반에서 2000년대 초)에, 연방통상위원회(FTC)와 백악관(the White House)은 이렇게 빠른 발전을 보이는 시장에서 사생

활 보호에 관한 정보를 모으는 이해관계인들을 소집하였다. 이러한 노력은 기술 및 비즈니스 형식에서 역동적인 혁신들을 발전시키면서, 중요한 사생활 보호들을 제공했던 유연하고 자발적인 사생활보호 체계를 양산하였다.

입법이 없음에도 불구하고, 행정부는 집행력 있는 법령을 제정하기 위하여 다양한 이해관계인들과의 합의절차을 회합하고 편의를 도모하려 한다. 개방된 포럼에서, 특정 시장 혹은 사업상의 이익을 가지는 이해관계인들은 소비자 사생활보호 권리장전을 이행하는, 법적으로 집행 가능한 법령을 합의하기 위하여 힘 쓸 것이다. 다양한 이해관계인들과의 합의절차는 전통적인 기관의 규칙 제정방식과는 다르다. 연방정부는 이해계인들과 개방적이고, 투명한 과정을 통하여 운용 절차들을 만들기 위하여 노력할 것이다. 그러나 궁극적으로, 이해관계인, 그들 자신들은 이러한 절차와 결과들을 지배하게 될 것이다. 이 절차의 마지막에 연방의 규제는 존재하지 않을 것이며, 법령 또한 그들이 그것을 채택하는 선택을 하지 않는 한 어떠한 기업도 구속할 수 없을 것이다.

이러한 절차에 이해관계인들을 참여시키기 위한 촉진책은 두 가지의 요소를 지니고 있다. 기업들은 소비자들 및 다른 이해관계인들과 이 합의 과정동안 직접적으로 접촉함으로써 소비자 신뢰를 쌓아 나갈 것이다. 이해관계인들이 이러한 합의 과정을 통하여 발전시킨 법규명령의 채택은 보다 깊은 소비자 신뢰를 구축할 지도 모른다. 또한 법규에 의하여 정해진 명령들에 기초한 어떠한 법집행 행위에서, 연방통상위원회는 기업들이 호의적으로 이 법규를 준수하는지를 고려하게 될 것이다.

1. 인터넷 정책 입안의 성공 기반 구축

인터넷은 행정부가 바라는 정책, 여러 이해관계인들에 의한 정책 발전의 몇 가지 성공적인 사례들을 제시하고 있다. 예를 들어, 민간 부문 기준 제정 기구들은 인터넷 관련 기술 표준들을 제정함에 있어서 선두에 위치하고 있다. 인터넷표준화기구(the Internet Engineering Task Force, IETF)[31]와 월드와이드웹컨 소시엄(the World Wide Web Consortium, W3C)[32]와 같은 그룹들은 인터넷 관련 기술 표준들을 제정하기 위하여 개방적인 절차들을 이용하고 있다. 이러한 과정들은 일부 성공적이었는데, 왜냐하면, 이해관계인들이 근본적인 과제들에 대한 만장일치에 기초한 해결책들을 반전시키는 이익을 공유하기 때문이다. 그들이 지원하는 서비스 및 애플리케이션의 범위가 끊임없이 증가하고 있기 때문에 기준들에 대한 결과의 성공은 자명하다.

이와 유사하게, 국제도메인관리기구(the Internet Corporation for Assigned Names and Numbers, ICANN)[33]는 비영리 기구로서, 도메인 네임을 특정 숫자로 된 주소로 만드는 도메인 이름 시스템의 기술적 관리 업무를 맡고 있다. 국제도메인관리기구(ICANN)는 또한 일반최상위도메인기구(generic top level domain registries, gTLD), 도메인 등록기관 및 등록자(registries and registrants), 국가최상위도메인기구(country code top level domain registries, ccTLD), 인터넷주소관리기구(the Regional Internet Registries), 루트서버사업자(root sever operators), 정부 기관들 및 넓은 의미에서의 인터넷 사용자들을 포함하는, 광범위한 인터넷에서의 대

31) 인터넷의 원활한 사용을 위한 인터넷 표준규격을 개발하고 있는 미국 IAB(Internet Architecture Board)의 조사위원회

32) www와 관련된 표준안의 제작과 새로운 표준안 제안 등 급변하는 www의 발전에 따른 신속한 안의 제정과 이를 많은 회사들과 연구기관에서 서로 공유하게 하여 정보화의 세상을 위한 하부구조로서의 www의 기술적, 사회적 확산을 위해 1994년 10월에 창립된 국제적인 웹 표준화 단체

33) 국제 인터넷 주소 관리 기구. 1998년 미국 상무성 주도로 설립된 비영리 민간기구

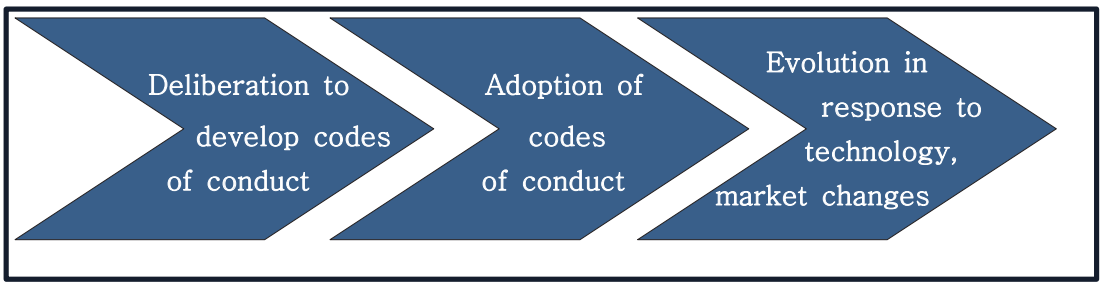
표자들로 구성된 다자 이해관계인 기구이기도 하다. 이러한 구조로써, 국제도메인관리기구는 인터넷의 중요한 역할에 대한 기술적인 관리를 즉 사람들이 컴퓨터가 사용할 수 있는 숫자로 된 주소들을 기억할 수 있는 이름으로 만드는 등 조직화하고 있으며, 그러한 방식은 이해관계인들의 넓은 참여를 더욱 가능하게 한다.

1990년대와 2000년대 초의 사생활 보호 논의를 이끌었던 행정부와 같은, 정책결정을 위하여 모인 정부기관은 미국에서 소비자 개인정보 보호를 향상시키는데 계속해서 중심적인 역할을 맡고 있다. 이 문서에서의 체계는 상무부 인터넷 정책 실무위원회(the Department of Commerce Internet Policy Task Force)의 이해관계인들과 함께 만든 확장 공약의 직접적인 결과이다. 게다가 연방통상위원회(FTC)는 다양한 이해관계인들의 “개인추적장치(Do Not Track)” 체제를 개발하는 노력을 독려해 왔으며, 이것은 소비자들이 온라인 광고행위 상에서 개인정보를 통제하는 것을 보다 더 가능하게 할 것이다.

2. 소비자 개인정보 보호를 위한 다양한 이해관계인의 합의 절차

미국통신정보관리청(the Department of Commerce's National Telecommunications and Information Administration, NTIA)은 소비자 개인정보 문제를 다루는 다양한 이해관계인들의 합의 절차를 소집하는 인터넷 정책의 다른 영역에 대한 역할을 통하여 발전되어 온 권위와 전문지식을 필요로 한다. 미국통신정보관리청(NTIA)은 법규명령(codes of conduct)를 개발하고, 기술과 시장 상황 변화에 따른 소비자들의 사생활을 보호하기 위하여 법규들을 이해관계인들과 조정하는 심의과정에 상무부(the Department of Commerce)의 이해관계인들을 소집하는 일을 이끌어 나가게 될 것이다.

< 소비자 개인정보 보호를 위한 이해관계인 합의 절차의 주요 단계들 >



(1) 심 의

① 쟁점사항 확인(Identifying Issues) : 미국통신정보관리청(NTIA)의 조력자로써, 이해관계 그룹들은 중요한 소비자 개인정보 문제들을 포함하는 시장 및 산업을 확인하게 될 것이며, 강제성 있는 법규 명령에 대한 시기를 맞이하게 될 것이다. 이 과정은 공개되지만, 해당 절차의 초점이 모든 이해관계인들에게 똑같이 맞추어지지는 않을 것이다.

② 심의의 개시 및 진행(Initiating and Facilitating Deliberations) : 통신정보관리청(NTIA)은 집행력 있는 법규명령을 발전시키기 위한 이해관계인들의 참여에 응하기 위한 단계들을 거쳐 가게 될 것이다. 위원회 의장으로서, 통신정보관리청은 국제적 동반자들, 연방통상위원회(FTC), 연방 민·형사 집행대표기관(Federal criminal and civil law enforcement representatives), 주법무부 장관(State Attorneys General)을 포함한 모든 이해관계인들에 대하여 회의는 공개된다. 사업상의 첫 번째 순서로써, 이해관계인들은 운용 과정 및 절차들을 제도화하게 될 것이다. 행정부는 한정된 자원을 가진 그룹들에 의한 참여를 제공하는 공개적이고, 투명한 합의 과정을 약속하고 있다. 그러나 이 심의 과정은 그들의 결과물에 의하여 결정되고 따르는 참여자들의 요구들에 부합해야만 한다.

③ 결론(Conclusion) : 모든 이해관계인들의 합의를 반영하는 법규(code)는 기업들에게 채택을 고려할만한 준비에 들어간다. 그러나 행정부는 합의사항이 법규의 부분에 대하여 알려질 것과 이해관계인들이 가장 어려운 쟁점들을 이 절차 후에 해결하게 될 것을 기대한다. 이 단계에서 통신정보관리청은 이해관계인들 간의 상이한 이해관계에 대한 해결을 돕기 위하여 집중적으로 그들과 함께 작업을 해야 할 필요가 있게 된다. 통신정보관리청의 역할은 그들 자신의 판단을 대리하는 것이라기보다는, 각 당사자들이 그들의 입장이 무엇인지와 합의에 대한 타협에 있어서 선택사항들이 있을 지에 대하여 명확성을 가지도록 돕는 일이 될 것이다. 이해관계인들 일부가 합의를 막는 유연적인 경계선을 그릴 수도 있는 가능성을 최소화하기 위하여, 당사자들은 어떻게 이 그룹들이 순차적임 결론에 도달할 것인지를 좌우하는 규칙 혹은 세부절차들을, 결론에 있어서 완전한 합의가 이루어지지 않은 경우라 할지라도, 이를 합의과정 초기에 논의하고 결정해야만 한다.

(2) 채 택

법규명령이 완성된 때, 이 법규와 관련 있는 기업들은 이것을 채택하기 위한 선택을 해야 할 것이다. 행정부는 이 법규명령을 충실히 지켜나가게 하기 위한 기업들의 공적인 공약이 마치 기업이 오늘날 그들의 사생활 보호 규정들을 따르는 것에 구속되는 것과 같이, 연방통신위원회 법률 Section 5(Section 5 of the FTC Act, 15 U.S.C. §45) 하에서 법적 구속력이 있는 것이 되는 것을 기대하고 있다. 법적구속력(enforceability)은 기업들의 정책과 그들의 공약을 부응시켜 소비자들을 보호하고, 그로 인하여 소비자 신뢰를 강화시키는데 필수적이다.

(3) 평 가

다양한 이해관계인들과의 합의 과정의 핵심 목표는 이해관계인들이 소비자들이 효과적으로 개인정보를 보호하는 것을 보장하기 위하여, 기술, 소비자 기대, 그리고 시장 상황에 있어서 빠른 변화에 대응으로서 사생활 보호를 수정하는 것을 가능하게 하는 것이다. 다양한 이해관계인들에 의한 합의과정은 최근의 법규명령을 유지하기 위하여 몇 가지 방법을 제시하고 있다. 이해관계인들은 기술상 혹은 시장상의 변화에 비추어 보아, 이 법규명령이 소비자 개인정보 보호를 더 이상 효과적으로 제공하지 않을 때를 언제든 결정하게 될 것이다. 통신정보관리청은 이러한 결론을 이끌어 낼 수 있을 뿐만 아니라 재심의(re-convene)를 하기 위하여 시도할 지도 모른다. 그러나 법규명령의 초기 개발에서와 같이, 법규명령의 수정하기 위한 이 과정에 대한 이해관계인 참여는 자발적이 될 것이다. 연방정부는 법규명령을 수정하지 않을 것이다. 그렇게 하기보다는 해관계인 그룹들이 이러한 변화들을 연방정부의 개입을 통하여 만들어 가게 될 것이다. 결국, 다음에서 논의될 입법적인 세이프 하버체계하에서, 의회는 법규명령에 대한 갱신 기간을 규정할 수 있음으로서, 연방통상위원회(FTC)가 정기적으로 집행력의 안전항구의 기초를 이루는 이 법규들을 검토하는 것이 가능해 진다.

제 4 절 소비자 프라이버시 보호 방안

1. 연방통상위원회의 집행 전문성의 구축

(1) 강력한 법집행을 통한 소비자 보호

법적구속력은 기업들이 법규 명령을 채택함으로써 만든 사생활보호 공약들이 의미 있는 것임을 확인한다는 측면에서 중요하다. 회원 기

업들에 대한 자발적 지침들을 개발하고 관리하는, 자율규제 기구들은 여기에서 서술된 이 체계에서 필수적인 것이 아님에도 불구하고, 집행의 초 일선을 규정할 수 있을 것이다. 자율규제 기구들은 초기 단계에서의 규제 준수상의 문제들을 발견하고 구제하는 것을 도울 수 있을 것이다. 결과적으로, 이러한 종류의 집행은 법규 명령 및 법규를 약속한 기업들에 대한 신뢰를 강화시킬 수 있다. 정부 기관들은 법규 명령에서 사생활 보호를 집행하는데 있어서 필수적인 역할을 또한 수행한다. 연방통상위원회는 연방 정부의 소비자 사생활보호 집행을 이끄는 권한을 가지고 있다. 연방통상위원회에 의한 집행 조치들은 기업들이 자발적인 사생활보호 공약들, 말하자면 사생활 정책들이라고 불리 우는 것들을 고착시키는 데 실패한 것을 불공정하거나 기만적인 조치 또는 정책에 대한 연방통신위원회 법률(FTC Act), 그리고 주에서도 이와 유사한 법률하의 금지를 근거로 소송이 가능하도록 제도화하였다. 게다가 연방통상위원회는 이른바 소비자들에 대한 개인 정보를 보호하기 위한 합리적인 보안 수단들을 이용하는 것을 실패한 기업들에 대한 사건들을 가져온다. 이러한 권한을 이용하여, 연방통상위원회는 변화하는 기술과 시장에 대하여 유연하고 진보적인 접근으로 소비자 개인정보를 효과적으로 보호하는 사건들을 다루어 오고 있다. 같은 권한으로 연방통상위원회는 다양한 이해관계인들의 합의를 통하여 발전된 법규 명령을 고착시키기 위하여, 그들의 관할권하에 기업의 공약들을 집행하는 것이 가능하게 될 것이다. 그리하여, 법규명령을 채택한 기업들은 현 법률상 법적으로 구속력이 있는 공약을 체결하게 될 것이다.

(2) 법적 구속력이 있는 법규명령의 개발을 위한 장려책 제공

연방통상위원회는 소비자 개인정보 문제에 관한 법규 명령에 대하여 모든 이해관계인에게 제공하는 중요한 집행 및 전문지식들을 보유

하고 있다. 소비자 개인정보 법률이 있거나 혹은 없거나, 연방통상위원회는 법규명령의 발전과 관련된 조력과 조언을 제공해야만 한다. 법률이 부재인 경우에, 연방통상위원회, 연방 민·형사 법집행 대표기관들, 그리고 주들은 실체 및 절차에 관하여 조언을 제공함으로써 다양한 이해관계인들의 심의과정에 참여해야만 한다. 이해관계인들이 법규를 발전시킬 때, 기업은 보다 많은 확실성을 얻기 위하여, 그리고 그것의 실행이 소비자들의 사생활을 보호한다는 것을 소비자들에게 보장하기 위하여 자발적으로 이 법규를 지키려고 할지도 모른다. 기업들은 다른 선상의 사업들을 포함하는 다양한 법규명령을 채택하는 선택을 할지도 모른다. 소비자 사생활보호 권리장전의 일반적인 기초는 이 법규들이 일관성 있는 것이 되도록 보장하는 것을 도와야 한다. 그런 다음, 하나 또는 그 이상의 법규명령에 해당하여 관련하는 어떠한 조사 및 집행 조치에서도, 연방통상위원회는 기업이 호의적으로 이 법규명령들을 준수하는 것을 고려해 주어야만 한다.

2. 국제 상호운용성의 촉진

인터넷은 미국의 기업들이 경계를 확장하는 것을 돕고 있다. 결과적으로, 국가 간 정보 흐름은 국내 및 국제 경제의 필수적인 요소가 된다. 국내 사생활 보호법의 차이점들은 기업들이 국가 경계를 넘어서서 개인정보를 이전하기를 바라는 변화를 야기 시킨다. 다른 사생활 보호 법률을 준수하는 것은 법적 기준이 관할권 간에 다양할 수도 있고, 기업들이 정기적인 운용을 실행하는 일에서 조차도 다양한 규제 승인들을 받아야 할 필요가 있기 때문에, 분명하고 개별적인 정보 처리 운영의 한 부분으로서 개인 정보를 이전하는 기업들에게는 부담스러운 일이다.

개별 사용자들에게 공급하는 서비스들은 보다 더 심한 규정 준수에 있어서의 도전들을 직면하고 있는데, 그것은 그들이 보다 복잡하고

다양한 정보의 흐름들을 다루고 있기 때문이다. 보다 복잡한 문제들은 클라우드 컴퓨터 시스템(cloud computer system)의 확산이다. 이러한 전 세계적인 퍼진 구조는 비용의 효율, 소비자, 기업 및 정부에게 혁신적인 새로운 서비스들을 전달하는 것을 돕는다. 이것은 또한 소비자 및 기업들이 전 세계적으로 그들이 일반화 하고 이용하는 개인 정보를 그들의 수령자들에게 보내는 것을 가능하게 한다. 소비자 개인정보 체계는 이러한 기술과 비즈니스 모델들을 용이하게 할 뿐만이 아니라 아직까지 드러나지 않은 것들에 대해서도 빠르게 적응시켜야만 한다.

정부가 이러한 도전들에 합당한 다른 조치들을 채택하고 있음에도 불구하고, 그들이 사생활보호제도간의 상호운용성을 창출하기 위하여 노력하는 것에는 디지털 경제의 계속적인 성장이 필수적이다. 행정부는 유연성 있는 다양한 이해관계인들에 의한 합의 절차들이 정보에 대한 기발한 사용과 이전을 행함으로서 상호운용성 있는 사생활보호 제도들을 용이하게 할 것이라고 믿는다. 미국은 그들의 국제적 동반자들과 사생활보호 법률에 있어서 상호인정, 다양한 이해관계인들 간의 합의를 통한 법규 명령들의 제도화, 그리고 상호협력 강화를 통하여, 상호운용성을 증대시키는 노력에 헌신해 왔다. 미국은 또한 사생활보호 문제에 관한 전 지구적인 합의를 가능하게 하는, 이러한 다양한 이해관계인들과의 합의 과정에 국제적 동반자들을 참여시키려고 노력해 왔다.

(1) 상호인정

상업적인 개인정보보호 체계에 대한 상호인정(mutual recognition)은 세계적인 정보 보호를 달성하기 위한 중요한 수단이다. 상호인정에 대한 시작점은 사생활 및 개인정보 보호를 둘러싼 일반적 가치들의 포용이다. 특정 사생활보호 체계 간에 상호인정의 조건이 존재하느냐

아니냐를 결정하는 것에는 두 가지 원칙이 있어야만 한다. 효과적인 집행(effective enforcement)과 기업들이 책임성(accountability)을 인정하는 것을 가능하게 하는 체계들(mechanisms)이다.

기업들이 동일한 법적 의무들 하에 놓여 있을 때, 상호인정은 모든 당사자들이 이 기업들이 의무를 시행토록 하는 것을 의미한다. 따라서 일반적으로 정책들(이라고 알려진, 효과적인 집행은 상호운영성을 확실히 하는 것이 매우 중요하다. 집행 권한 및 체계들은 국가들 간에 다양하며, 미국은 조치들의 다양성이 효과적이 될 수 있다는 것을 인지하고 있다. 미국은 연방통신위원회의 불공정 또는 기만적 조치 및 정책들에 대한 일반적 금지들(general prohibitions)을 사례별로 집행에 주로 의지하고 있다. 이러한 접근은 민간 부문에서 개인 정보를 다루기 위한 진보적인 기준들을 발전시키는 데 도움이 된다.

상호인정이라는 맥락에서, 책임성은 사생활보호(자발적으로 채택을 하였든 혹은 법적 의무의 결과이든) 와 관련하여 법적 구속력이 있는 정책과 절차들에 대한 이행력을 보여주는 기업의 능력을 말한다. 책임 체계는 자체 사정, 평가 및 감사를 포함한다. 행정부는 이해관계인들이 법규명령을 발전시키는 과정에서 전 세계적으로 받아들여지는 책임성이 무엇인지를 함께 정하는 노력을 장려하고 있다.

초국가적인 상호인정의 개시 및 실행의 한 가지 예는 아시아태평양경제협력체(APEC)의 개인정보 국외이전제도(Cross Border Privacy Rules, CBPR)의 자발적 체계이며, 이는 아시아태평양경제협력체(APEC)의 사생활보호 체계에 기초하고 있으며, 아시아태평양경제협력체(APEC) 경제주체들이 인식에 동의하고 있는 사생활보호 원칙들을 포함하고 있다. 이러한 원칙들에 기반을 둔 법규명령은 방대한 아시아태평양경제협력체(APEC) 지역을 통하여 가동되고 있는 기업들의 개인정보 보호 정책 및 실행들을 간소화 시킬 수 있었다. 이행에 있어서, 아시아태평양경제협력체(APEC)의 개인정보 국외이전제도(CBPR) 체제는 아시아

태평양경제협력체(APEC) 사생활보호 체계에 기초하여 요구되는 개인정보 국외이전제도(CBPR) 프로그램 요건들 일체를 준수하는 것을 입증하기 위한 이익이 있는 신청자들을 요구할 것이다. 게다가 이 과정 중에 신청자들이 만드는 공약들은 자발적인 것임에도 불구하고 회원국의 경제체제의 법률 하에서 법적 구속력이 있는 것이 되어야만 한다. 성공적인 개인정보 국외이전제도(CBPR) 인증은 참가기업들이 소비자들에게 책임감 있고, 법률에 부합하며, 전 세계적으로 인정받을 수 있는 기준들을 표시하고 그럼으로써 아시아태평양경제협력체(APEC) 지역 도처에서 개인정보의 이전을 용이하게 하는 참가 기업들에게 자격이 주어지게 될 것이다.

유럽에서, 개인정보 처리와 관련한 개별주체들의 보호 및 그러한 정보의 자유로운 이동에 관하여, 일반적으로 유럽연합 정보보호지침(EU Data Protection Directive)으로 알려져 있는 유럽연합 지침 95/46/EC (European Union Directive 95/46/EC)는 법률의 이행을 돕는 법규명령의 발전을 고무시킨다. 산업특화 법규명령을 제안하는, 행정부 체계와 같이, 이 정보보호지침은 관련 사업에서의 필요에 따라, 일반적인 사생활보호 원칙들의 이행이 세부사항에서 다를 수도 있는 법규명령임을 인식하고 있다. 행정부는 사생활보호에 대한 상호인정에 기초한 법규명령을 만드는 회원국들과 마찬가지로 유럽연합(EU) 수준에서의 기구들과 함께 노력하고 있다.

미국이 유럽연합과 스위스와 함께 발전시켰던 세이프 하버 체계(the Safe Harbor Frameworks)는 대서양연안의 정보 흐름에 중요한 영향력을 끼쳤던, 국제적인 상호운용성의 초창기 예들이다. 기업들이 그들의 국제적 비즈니스 가동을 방해받지 않는 방식으로 정보를 이전할 수 있을 것을 보장하려고 하는 동안에, 미국, 유럽연합, 스위스는 이 체계들을 개인정보 보호의 목적들을 성취시키기 위하여 협상하였다. 이러한 체계들은 기업들로 하여금 이러한 현상들에 대한 연방통신위원

회의 집행을 적용받는 유럽연합 정보보호준칙 하에서의 의무에 부합하는 자체 인증(self-certify)을 가능하게 하였다. 2700개 이상의 기업들이 참여했던 세이프 하버체계는 개인정보를 유럽연합에서 미국으로 이전하게 했을 지도 모른다. 결과적으로 세이프 하버 체계는 개인정보 흐름에 대한 장애를 효과적으로 감소시켜 왔고, 그로 인하여 무역과 경제 성장에 도움을 주었다.

(2) 다양한 이해관계인들과의 합의과정 및 법규명령에 대한 국제적 역할

속도, 유연성 및 잘 짜여진 다양한 이해관계인들 간의 합의에서의 분권화된 문제 해결의 덕은 그것이 혁신을 촉진시키고 소비자들을 보호하는 전 세계적으로 적절한 규칙과 지침으로 세워지게 되면서, 기존의 정부 규제를 넘어서는 어떠한 장점들을 제공하게 되었다. 현존하는 상호인정 체계들과 결합하고, 법규 명령을 발전시킨 다양한 이해관계인들은 기업들의 규칙준수 의무 부담들을 대단히 단순화시키는 것에 대한 약속을 지켰다.

세이프 하버 체계는 대서양 연안의 무역을 용이하게 함에 있어서 가치를 증명한 반면, 그들은 모든 미국의 기업들에 대하여 완벽한 해결책은 아니었다. 연방통상위원회(FTC)에 의하여 규정된 부문들, 말하자면 금융 서비스, 전기통신 일반사업자, 그리고 보험과 같은 것들은 세이프 하버 체계에 의해 포함되지 않는다. 이러한 부분에 있어서 몇몇 기업들은 그들이 대서양 연안국의 정보 이전을 위한 개선된 환경을 보여주기를 원하는 것으로 나타났다.

세이프 하버 체계의 성공을 구축하기 위하여, 행정부는 상무부 및 미국을 통하여, 법적 체제에 대한 상호인정을 지원하고, 정보의 자유로운 흐름을 용이하게 하며, 최근의 사생활보호 문제들을 처리하기 위한 추가적인 기제들을 - 이를테면, 법규명령의 합동 개발과 같은 -

개발하는 계획을 가지고 있다. 행정보는 다양한 이해관계인들의 합의 과정에서 국제적인 이해관계인들이 포함되기를 기대한다. 세이프 하버체계는 언젠가 중요하고 시급한 사생활보호 이슈들에 대하여 대서양연안국들의 합의를 반영하는 법규명령에 의하여 보충될 수 있을 것이다.

(3) 상호협력의 강화

개인정보 보호에서 국제적인 상호운용성을 현실화하기 위하여, 상호인정은 활발한 집행상의 협력이 동반되어야만 할 것이다. 양자 또는 다자간이든 간에, 그러한 협력은 정보 보호 권한들 사이에서 정보 공유를 처리하기 위하여 필요한 것이다.

외국의 상대 파트너들과 함께 협력하는 일에 보다 더 많은 권한을 보장하는 입법에 의하여 권한을 부여받았기 때문에, 연방통상위원회(FTC)는 글로벌 프라이버시 네트워크(the Global Privacy Enforcement Network, “GPEN”)의 창설을 지원하였다. 글로벌 프라이버시 네트워크(“GPEN”)는 사생활 집행 우선권, 모범사례의 공유, 그리고 합동 집행 개시를 위한 지원에 대하여 보다 깊은 발전들을 목적으로 하고 있다. 연방통상위원회(FTC)는 경제협력개발기구(OECD), 아시아태평양경제협력체(APEC), 아시아태평양경제협력체 감독기구 포럼(the Asia-Pacific Privacy Authorities forum, APPA), 그리고 국제 개인정보보호 기구회의(International Conference of Data Protection and Privacy Commissioners, ICDPCICDPC)를 포함하는 다른 여러 국제기구들을 포함하고 있다. 글로벌 프라이버시 네트워크("GPEN"), 경제협력개발기구(OECD), 아시아태평양경제협력체(APEC) 및 기타 기구들에서의 미국의 임무는 국제적으로 사생활보호 조사 및 집행조치에 있어 협력을 증대시키는 것이 되고 있다. 개인에게 미치는 인터넷 기반 서비스들이 전 세계를 관할

권으로 삼고 있는 상황에 놓여 있기 때문에, 홀로 국내적 개인정보보호를 정부들이 집행하는 것은 효과적인 것도 현명한 것도 아니다.

3. 소비자 프라이버시법의 입법

행정부는 의회에게 소비자 프라이버시보호 권리장전을 채택하는 법안을 통과시킬 것을 설득하고 있다. 법안은 특정 연방 개인정보 입법에 해당하지 않는 상업적인 부분에서의 영역들을 통하여 사생활보호 권한들 전체의 기초를 제공함으로써, 디지털 경제에서 신뢰를 촉진시키게 될 것이다. 행정부가 지원하는 유연한 조치는 기업들이 사업상의 정해진 방법으로 기업들에게 소비자 사생활보호 권리장전을 이행하는 것을 가능하게 할 것이다.

(1) 소비자 프라이버시보호 권리장전의 성문화

의회는 행정부가 제안한 소비자 프라이버시보호 권리장전에서 정한 권리들에 대한 위반으로부터 소비자들을 보호하기 위한 조치를 취하여야만 한다. 이러한 권리들은 소비자들에게 확실한 보호를 제공하며, 개인정보에 대하여 빠르게 성장하는 시장을 위한 방법에 대한 규칙들을 정한다. 법제정은 연방통상위원회 및 각 주의 법무부장관에게 이러한 권리들을 직접적으로 집행할 수 있는 권한을 주어야만 한다. 이러한 법제정은 이 문서에서 제공하는 것보다 더 많은 구체성을 가지고 소비자 사생활보호 권리장전 하의 기업의 의무들을 규정해야 할 필요가 있을 것이다. 소비자 사생활보호 권리장전은 행정부가 법적 해석을 하는 것에 있어서, 의회와 함께 공동으로 작업하는 지침이 된다.

행정부는 또한, 보다 큰 법적 확실성을 제공하고 발전과 산업특화 법규명령들(industry-specific codes of conduct)을 채택을 도모하기 위하

여, 연방통상위원회(FTC)에게 법규명령을 검토하고 제정된 규정들의 집행을 삼가기 위하여, 그러한 법규들을 지키려고 노력하는 그리고 지키는 기업들을 보장하는 권한을 주는 입법을 지원하고 있다. 게다가, 소비자 개인정보 입법은 다음과 같은 사항들을 피해야만 한다. ① 이미 사생활보호 원칙들을 법적으로 준수하고 있는 기업들에게 중복적이거나 과도한 부담을 주는 규제 요건들을 추가하는 것, ② 법률의 위반이 수반되는 기술특화 수단들을 처방하는 것, ③ 일반적이지만 이 규정이 작성될 당시에 고려되지 않았던 개인정보의 새로운 이용을 포함할 수 도 있는 소비자 프라이버시보호 권리장전에 부합하는 새로운 사업 유형을 막는 것, ④ 정부가 경계 수색(border searches), 범죄 행위 혹은 기타 법률의 위반에 대한 조사, 혹은 공공의 안전 및 국가 안보의 보호를 지원하기 위하여, 필요한 정보를 얻는 데 따르는 현행하는 법률 혹은 규정으로 정한 권한들을 고치는 것, ⑤ 범죄 행위를 수사하고 기소하며, 공공의 안전을 보장하기 위한 법률 집행 능력을 위반하는 것, ⑥ 정부의 정보화 정책에 적용되거나 순수하게 상업적이거나 소비자 지향적인 것 외의 사생활보호 문제들을 처리하는 현행 법률, 규정 또는 정책 권한들을 변경하는 것이다.

(2) 연방통신위원회 직접 집행 권한의 보장

행정부는 의회에게 소비자 프라이버시보호 권리장전 각 규정을 집행할 권한을 연방통상위원회에게 보장하도록 장려한다. 이 권한은 소비자와 기업 모두에게 보다 큰 확실성을 제공하게 될 것이다. 기업들은 그들의 사생활보호 의무에 대하여 보다 분명한 로드맵(roadmap)을 가지고 시작할 수 있게 될 것이다. 소비자들은 의회가 연방통상위원회에 상업적 시장에서 포괄적인 사생활보호 전체에 대하여 집행할 권한을 주었다는 것을 아는 것으로부터 실익을 갖게 될 것이다. 동시에 연방통상위원회가 소비자 프라이버시보호 권리장전을 집행하는 것을

가능하게 하는 규정은 직접적으로 유연성을 제공하고, 적절한 절차적 보안장치들을 통하여 지배되는 특정 집행조치들을 통하여 연방통상위원회가 문제가 되는 프라이버시보호 이슈들을 처리할 수 있도록 할 것이다. 이러한 법제 하에서 보다 훨씬 더 큰 확실성을 찾는 기업들은 다양한 이해관계인들의 합의 과정 및 앞으로 논의될 시기적절하게 특정 사안에 맞는 법규명령을 발전시키는 피난처 규약을 이용해야만 한다. 행정부는 의회가 주법무부 장관에게도 동일한 권한을 보장하는 것을 권고한다. 그들이 그들의 집행 조치에 있어서 연방통상위원회와 함께 협력하고 있는 동안에, 주들은 추가적인 집행 자원들 및 소비자 개인정보 전문지식에 대한 심의할 수 있는 자원을 제공할 수 있다.

기술 및 사업 사업관행상의 빠른 변화들을 포함하는 도메인들에서, 의회는 그것이 법으로 통과되는 때에 존재하고 있는 기술과 관행에 대하여 맞추기 보다는, 유연성 있는 기준들을 만들어내는 선택을 해 왔다. 예를 들어, 독점금지법 영역에서, 셔먼법(the Sherman Act)[34]은 "무역억제(in restraint of trade)" 에 대한 합의들을 금지하고 있다. 저작권법(the Copyright Act)은 "현재 알려진 또는 최근까지 발전된(now known or later developed)" 기술에 근거하여 "복제(copies)" "장치(devices)" 및 "처리과정(processes)"과 같은 기초 용어들을 정의하고 있다. 그리고 개인정보 보호 영역에서, 연방통상위원회는 "불공정 또는 기만적 조치 또는 실행(unfair or deceptive acts or practices)"에 대한, 연방통신위원회법 섹션 5(the FTC Act Section 5)의 금지 하에 여러 집행 조치들을 도입하였다, 기관 지침들의 결합, 사법적 해석, 그리고 산업적 관행들은 개별주체들과 기업들이 이러한 일반적인 법률을 준수하는 것을 실행할 지의 여부에 대하여 보다 큰 확실성을 가지고 결정하는 것을 가능하게 하는 이러한 용어들에 대한 해석들을 제시한다.

34) 미국 최초의 독점금지법

행정부는 의회가 소비자 개인정보 입법의 기준과 유사한 과정을 따를 것을 원조하고 있다. 기준규정이 연방통상위원회 집행 조치들을 기초로 하여, 기업에 대하여 활동하는 분야의 수준과 소비자들에 대한 일관된 기대사항들, 그리고 보다 큰 확실성 및 공개성을 제공하는 것은 중요한 일이다. 연방통상위원회는 또한 소비자 사생활보호 권리장전의 규정들을 집행할 방법을 공공에 대하여 명확하게 만드는 일을 노력할 수도 있다. 규정들의 요건들을 명백히 하는 기본적 체계는 앞서 논의되었던 것과 마찬가지로 다양한 이해관계인들의 합의과정, 법적 구속력 있는 법규명령에 기초한, 피난처 규약이 되어야만 한다. 그러나 보다 전형적인 일반적인 규제 요건들을 분명하게 하는 유형들도 역시 도움을 주는 역할을 수행할 수 있게 될 것이다.

(3) 세이프 하버 규약을 통한 법적 명확성 제공

행정부는 연방통상위원회가 현행 법률 하에서 가능한 것 보다 법적 구속력 있는 법규명령을 채택한 기업들을 보다 더 기업들에 대한 보장을 제공하는 권한을 부여하는 것을 지원하고 있다. 두 개의 입법 구조가 이러한 목적을 성취하는 것을 돕게 될 것이다. 첫째, 연방통상위원회는 그들이 입법에서 시작했던 것과 마찬가지로, 소비자 프라이버시보호 권리장전에 맞서는 법규명령을 검토하기 위한 명백한 권한을 가져야만 한다. 법제정은 통신위원회(FTC)가 합리적인 시간 안에 (예컨대, 180일) 제출된 법규를 검토할 것과, 연방통상위원회(FTC)가 이 법규에 대한 공공의 의견제출을 고려해야 하며, 다양한 이해관계인들의 합의 과정에서 모든 참가자들의 합의를 반영하는 법규를 승인 또는 거절하는 것에 대한 검토 권한에 제한을 갖고, 기술 및 시장변화를 반영하는 소비자 개인정보를 효과적으로 보호하는 것을 보장하는 승인된 법규를 검토하는 기간을 설정하는 요건을 갖추어야만 한다. 법규를 제정하는 다양한 이해관계인들의 합의 과정으로부터의 기

록은 이 법규가 소비자 프라이버시보호 권리장전을 효과적으로 이행하고 있는지에 대한 평가를 연방통상위원회에게 안내하는데 도움이 될 것이다. 연방통상위원회의 검토의 결과는 기업들이 다양한 이해관계인들의 합의 과정의 최종 결과인 법규명령들을 채택하는 결정에 영향을 주기 쉬울 것이기 때문에, 모든 이해관계인들에 대하여 공개적인 절차를 통하여 연방통상위원회가 검토로 세부사항들을 결정하는 것은 타당하다. 그러나 이들 세부사항들은 법적인 구속력이 있어야만 한다. 따라서 행정부는 의회가 행정절차법(Administrative Procedure Act (5 U.S.C. § 552 이하 참조)) 하에서 법규명령의 검토 및 승인을 위하여 공정하고 공개적인 절차를 제도화하는 규칙을 다루는 권한을 연방통상위원회에게 보장하도록 권고한다.

행정부가 권고하는 두 번째 요소는 연방통상위원회(FTC)에게 연방통상위원회(FTC)가 검토하고 승인했던 법규명령들을 따르는 기업들에게 “세이프 하버(safe harbor)”를 이를테면, 소비자 사생활보호 권리장전 규정의 집행에 대한 관용을 보장하는 권한을 주는 것이다. 법규명령의 채택을 저하하거나, 그들이 채택한 법규에 대한 연방통상위원회(FTC)의 검토에 대하여 노력하지 않는 선택을 하는 기업들은 간단히 법적으로 채택된 소비자 프라이버시보호 권리장전의 일반 의무위반에 처하게 될 것이다.

(4) 소비자 개인정보 보호에서 연방 및 주의 역할의 균형

소비자 프라이버시보호 권리장전을 제정한 연방 법률은 현행 연방 개인정보보호 법률이 적용되지 않는 부분에서의 소비자 프라이버시보호에 대한 국내적 기준을 제공해야만 한다. 국내적으로 표준 소비자 정보보호 규칙들은 기업에 대한 확실성과 소비자들에 대한 일관된 보호를 만들어 낼 필요가 있다. 이러한 규칙들은 목적과 관련한 법률 집행에 유효한, 특정한 정보에 대한 필요를 참작해야만 한다. 게다가

국내 통일령(national uniformity)은 다양한 이해관계인들의 합의과정을 통하여 행정부의 체계가 제시하는 장려책들을 유지하는데 중요하다. 다양한 이해관계인들의 합의 과정에 참여시키기 위한 이해관계인들을 위한 장려책들, 그리고 법규명령을 채택하도록 하는 기업들에 대한 장려책들은 만약 주들(이 보다 엄격한 요건들로 법률을 제정했다면 약화되어 갈 것이다. 그러므로 행정부는 의회가 주 법률을 그들이 제정되고 적용되는 소비자 프라이버시보호 권리장전에 모순되는 범위를 사전에 제압할 것을 권고한다. 행정부는 또한 의회가 연방통상위원회 승인 법규명령을 채택하고 따르는 기업들에 대항하는 저 법률의 집행으로부터 관용을 제공할 것을 권고한다.

행정부의 제안 조치는 주들이 대한 중요한 정책입안 및 집행 역할을 하는 것을 유지시켜준다. 주들은 다양한 이해관계인들과의 합의과정에서 높은 수준으로 건설적인 역할을 수행할 수 있고, 그렇게 해야만 한다. 행정부는 또한 각주의 법무부 장관이 소비자 프라이버시보호 권리장전을 집행하는 권한을 법적으로 승인받는 것을 돕는다. 이러한 점에서 미루어 볼 때, 이러한 체제들은 주에게 주들이 국내적 수준에서 통일령을 유지하는 동안 공감하고 있는 소비자 개인정보 이슈들을 처리하는 수단을 제공하게 될 것이다. 행정부는 또한 소비자 개인정보 보호에 있어서 행정부가 추구하는 광범위한 통일성을 다투지 않을 법률을 주들이 제정할 수 있는 특정한 부문들이 존재 하는지의 여부를 결정하기 위하여 의회, 주, 민간 부문, 그리고 기타 이해관계인들과 함께 작업하게 될 것이다. 예를 들어, 전기 소매 유통과 같이, 주들이 규제하는 부분에 있어서 개인정보에 대하여 소비자 프라이버시보호 권리장전을 적용하는 법률을 제정하는 것을 가능하게 하는 것이 적절한 예가 될 수 있을 것이다.

(5) 현행 연방 개인정보보호 법률에서의 효율적인 보호 유지

소비자 개인정보보호 입법은, 개인정보를 효과적으로 보호하고, 법적 의무들의 중복을 최소화하며, 소비자들에게 그들이 가진 보호가 무엇이며, 누가 그것들을 집행하는 지에 관하여 명백한 감각을 제공하는, 현행 특정 부문 연방 법률들을 유지시켜야만 한다. 그럼에도 불구하고, 현행 연방 법률들이 이러한 지침들에 부합하지 않는 경우에, 행정부는 의회에게 소비자 및 기업들에게 이익을 가져다주기 위하여, 소비자 개인정보보호 입법이 현행의 요건들을 단순화 할 수 있도록 하는 방법을 고려해 줄 것을 장려한다.

일반적으로, 이 특정 부문 연방 개인정보보호 법률들은 그러한 부분들에서 사용된 개인적 정보의 감도 및 만연하는 관행들에 맞추어진 법적 의무들을 창설한다. 예컨대, 의료정보보호법(The Health Insurance Portability and Accountability Act, HIPAA)과 의료정보보호법 프라이버시 규칙법(the HIPAA Privacy and Security Rules)은 의료 제공자, 보험, 의료 정보 센터에 의한, 개인의 의료정보에 대한 수집, 이용 및 공개를 규제하고 있다. 의료정보보호법(HIPAA)은 환자를 다루기 위하여 두 군데의 의료 제공자간에 개인 의료정보의 공개와 같은 의료행위상 필수적이고 일반적으로 받아들여지는 개인 의료정보 실행은 다툼 없이 허락해주고 있다. 교육, 신용 보고, 금융서비스 및 아동 개인정보에 적용되는 연방 개인 사생활보호 법률들은 이처럼 잘 맞춰진 요건들의 예들이다.

1) 이중의 의무부담이 없는 포괄적인 사생활 보호 창설

중복적인 규제 부담이 생성되는 것을 막기 위하여, 행정부는 기업들의 활동이 현행 연방 개인정보보호 법률에 해당하는 범위까지 소비자 개인정보 입법으로부터 기업들을 면제시키도록 돕는다. 그럼에도 불

구하고, 현행 정보보호법률 하에서 맞지 않는 그러한 기업들의 활동들은 행정부가 제안한 입법에 의하여 처리된다. 이러한 대안들은 현행 연방 개인정보보호 법률의 대상이 되는 전체 기업들을 면제시키는 규칙을 가리는 예외를 허락할 수 있다. 예를 들어, 금융현대화법(the Gramm-Leach-Bliley Act, GLB)은 금융기관에게 특정 개인정보보호 및 비공개 개인정보에 대한 보안 예방책들을 취할 것을 요구하고 있다. 만약 금융현대화법(GLB)의 대상이 되는 기업들이 금융현대화법이 포함하고 있지 않은 개인정보를 위하여, 소비자 개인정보보호 법률의 기준으로부터 면제를 받게 된다면, 이 기준 법률의 실효성은 심각하게 저하될 수도 있다.

2) 일관성이 없거나 또는 혼란스러운 요건들을 제정한 법률들의 수정

현행 연방 법률들이 통신부문 내에서 유사한 기술들을 다르게 취급하고 있기 때문에, 행정부는 이것의 법적 범위를 단일화하고 명백히 하며, 연방통상위원회(FTC)에게 통신 서비스제공자들에 대하여 소비자 사생활보호 권리장전을 집행할 책임을 지도록 지원하고 있다.

(6) 보안침해통지에 대한 국내 기준의 설정

보안상의 결함이 있는 특정한 영역에 있어서, 행정부는 기업들이 소비자들에게 어떤 종류의 개인 정보에 대한 권한 없는 공개를 공지해야만 하는 조건을 갖는 국내 기준을 만드는 것을 지원한다. 보안침해통지(Security breach notification, SBN) 법률들은 민감한 개인정보에 대한 보호를 효과적으로 촉진시킨다. 이 법률들은 소비자들에게 누구의 개인정보가 권한 없는 수령자들에게 공개되었는지를 알려줄 어떠한 상황에 놓인 기업들에게 요구된다. 공지는 소비자들이 그들 자신을 신원 도용과 같은 침해들로부터 보호하는 데 도움이 된다. 이것은 또

한 기업들에게 초기에 보다 나은 정보 보안을 설정하기 위한 장려책들을 제공한다. 보안침해통지(SBN) 모형은 또한 소비자를 효과적으로 보호하는 결과기반 요건들(a performance-based requirement, PBN)과 마찬가지로 국제적인 동의를 쌓아가고 있는 중이다.

최근에, 47개의 주, 컬럼비아 특별구, 그리고 몇몇의 미국의 영토국들은 보안침해통지(SBN) 법률들을 가지고 있다. 주들의 다양성은 문제를 헤쳐 나가기 위하여 가장 효과적인 조치들에 대한 의식들을 허용해 왔지만, 국내적 통일성에 대한 요구가 현재 명백하게 존재한다. 소비자들에 대하여 많은 대항력있는 이익 없이, 주 법률들의 조각들을 모아 놓은 법률들은 기업들에게 심각한 부담을 야기한다. 포괄적인 사이버보안 입법체의 한 부분으로서, 행정부는 개인정보의 어떠한 유형에 대하여 권한 없는 공개가 존재하는 경우에, 소비자들에게 공지하는 국내적 기준을 제정할 것을 권고하였다. 이러한 국내적 기준은 오늘날 존재하는 다양한 주의 기준들을 대체하고 이 영역에서 앞으로의 주의 입법을 면하게 할 것이다.

4. 개별주체의 사생활 보호 개선에 대한 연방정부의 역할

소비자 정보보호 외의 영역에서, 행정부는 연방 정부의 공공 및 민간 분야에서의 개인정보 보호의 옹호의 긴 역사를 계속해서 이어나가고 있다. 이 역사는 컴퓨터에 의하여 정보가 처리되는 초기로부터 시작된다. 1973년, 보건교육복지부(the Department of Hearth, Education, and Welfare, HEW) 자동화 개인정보 시스템에 관한 자문위원회(Advisory Committee on Automated Personal Data System) 음반, 컴퓨터, 그리고 시민의 권리(Records, Computers, and Rights of Citizen)이라는 제목의 보고서를 발표하였다. 이 대표적인 보고서는 행정부의 소비자 프라이

버시보호 권리장전의 기초를 제공한, 공정정보규정(FIPPs)에 대하여 초안을 제공하였다.

그 이후로, 연방정부는 개인정보 보호가 국가적 사업으로서 필수적인 것임을 증명하기 위하여 앞장서 왔다. 어떠한 단일 사업 또는 정책의 요구도 이 활동을 독려하지 않은 것이 없었다. 몇몇의 경우에 있어서, 연방 기관들은 그들의 핵심적인 임무들을 향상시키는 혁신적인 계획으로 사생활보호를 통합시킨다. 연방 기관들의 이와 같은 활동들은 의료, 금융서비스, 그리고 교육을 포함하는 광범위한 경제 부문들에 걸치는 범위를 갖는 의무들과 함께 신속한 모범사례, 새로운 서비스를 가능하게 하고, 많은 다른 사생활보호 이슈들을 처리하기 위한 수단들을 제공하며, 개별적 사생활보호 권리들을 집행하는 행정부의 헌신을 보여주는 것이다.

(1) 새로운 서비스의 가능

민간부문에서처럼, 연방 기관들도 누설이 공공에 대하여 서비스된 때, 사생활 정보보호 이슈들을 직면하게 될 수밖에 없다. 특히 사생활보호 이슈들의 집단적 이의제기는 참전용사들(Nations's veterans)에 관한 의료정보 누설과 관련하여 야기된다. 재향군인회(the Department of Veterans Affairs, VA)는 국가에 걸쳐 1400개 이상의 기관에 대하여 8백3천만의 등록된 재향군인의 의료정보를 제공한다. 이러한 규모와 범위의 의료정보를 효과적이고 비용효율이 높게 관리하는 것을 지원하기 위하여, 재향군인회(VA)는 그들의 의료 전달 체계에서 정보 기술을 계속해서 추가해나가고 있다. 재향군인들의 의료정보에 관한 정보를 보호하는 것은 이러한 노력의 성공에 필수적인 것이다.

재향군인회(VA)는 개인의 의료정보를 위한 개인정보보호 및 보안보호(privacy and security protections)를 중요한 장점으로 이끌 수 있는 방법은 의료정보가 전달되는 방법에 있다는 것을 입증하는 계획에 착

수하였다. 재향군인회(VA)는 개인정보 및 보안보호에 “나의 의료정보는 개인 의료기록이다(My HealtheVet Personal Health Record)”를 추가시켰다. 이 시스템은 재향군인들이 그들의 간병인들에게 보다 나은 의료정보를 전달하는 것을 가능하게 돕고, 재향군인들이 그들의 의료정보로 활동적인 동반자가 되도록 힘을 실어주는 다른 인터넷 기반 수단들을 제공하는 정보의 출입구이다. 이 재향군인회 블루 버튼 서비스(Blue Button service)[35]는 재향군인들이 그들의 의료기록 정보를 안전한 방식으로 전자적인 복사를 다운로드할 수 있게 하는 것이다.

행정부는 다른 영역에서 개인정보보호를 어떻게 가능하게 하는가

• **사생활보호의 사이버안전 계획으로 편입 :** 개인정보보호는 생산성과 혁신을 계속해서 증대시키고, 새로운 사업상의 시도들을 지원하는 온라인 환경을 지키기 위한 행정부의 노력들에 있어서 우선사항이다. 미국국립기술표준연구소(the National Institute of Standards and Technology, NIST)에 의하여 주도된, 사이버 공간에서의 신뢰받는 ID를 위한 국가 전략(the National Strategy for Trusted Identities in Cyberspace)은 보다 표준화되고, 안전하며 사생활보호가 강화된 방법들로 개벌주체들의 온라인을 실증하기 위한 발전을 위하여 상업적 부분에서의 파트너십을 요청하고 있다.

• **신용대출시장에서의 투명성 강화** : 행정부는 개인정보보호가 소비자 신용에 관한 용어들로 정해지는 개인정보의 이용에서의 발전들과 보조를 맞추어 가는 것을 보장하고 있다. 연방준비제도이사회(the Federal Reserve Board, FRB)는 연방통상위원회와 함께 소비자의 신용보고서를 기초로 하여, 채권자가 소비자에게 신용을 제공하는 때에, 그것을 다른 소비자들에게 제공하기 보다는 불리한 조건들에 대하여 통지할 것을 요구하는 규칙을 제정하였다. 이 규칙은 또한 그러한 “위험 기반 가격책정(risk-based pricing)”와 같은 통지를 받은 소비자들에게 무료로 신용 보고서를 획득할

35) Blue Button란 미국 재향군인회와 국방부, 메디케어에서 실시된 것으로 재향군인이 지정된 인터넷사이트에 접속해서 인증을 하고 블루 버튼을 누르면 자신의 의료정보, 기록, 청구 사항들을 다운로드할 수 있게 한 것이다.

수 있는 자격을 부여하였는데, 이것은 소비자들이 채권자들이 사용하는 정보가 정확한 것인지 아닌 지를 확인하는 것을 가능하게 한다.

(2) 실효성 있는 집행을 통한 개인정보의 보호

연방통상위원회는 그들의 민사 집행권한을 위원회 규칙을 준수하는 것에 실패하거나 불공정 혹은 중첩적 방식으로 행위하는 상업적 기업들에 대하여 행사하였다. 2009년 이래로, 연방통상위원회는 민감한 개인 및 의료 정보를 보장하기 위한 합리적인 보호를 실행하는 것에 실패했었던, 그리고 기업들이 이러한 인증들을 하지 않거나, 혹은 약화되도록 두거나 혹은 소프트웨어 추적에 대한 이용을 불완전하게 하도록 놓아두는 경우에, 미국과 유럽 또는 미국과 스위스의 세이프 하버 협약(U.S.-EU U.S-Swiss Safe Harbor agreements)에 의해서 준수되었음을 표현해왔던 기업들에 대해서 조치를 취하여 왔었다. 연방통상위원회는 또한 온라인 인증 제공자들, 소셜 미디어 기업들, 그리고 독자성을 주장하는 기업들에 의하여 기만적으로 실행되는 것과 같은 조치들을 조사했다. 게다가 연방통상위원회는 텔레마케팅 규칙(the Telemarketing Sale Rule, TSR), 아동 온라인 사생활보호법 규칙(COPPA Rule) 공정신용보고법(the Fair Credit Reporting Act), 금융현대화법 안전규칙(GLB Safeguards Rule) 하의 사건들을 수사하였다. 행정부는 또한 법으로 정한 프라이버시보호 권리들을 진지하게 집행하고 있다. 법률 집행권한을 가지고 있는 연방기관들은 이러한 프라이버시보호 권리들을 위반하는 이들에 대하여 조치를 취하여 왔다. 예를 들어, 미국법무부(the Department of Justice, DOJ)는 신원도용, 일상생활에 지장을 초래하고 경제적으로 희생자들을 파괴하는 침해를 야기할 수 있는 개인정보에 대한 부적절한 이용과 같은 사건들을 강력하게 수사하였다. 2010년

한해에만, 미국법무부(DOJ)의 연방지방검찰청(United States Attorneys Offices)은 1300건의 신용도용에 관한 사건들을 수사하였고, 주지방검찰청은 최근 회계연도에 거의 700건에 이르는 신원도용 사건을 다루었다. 비밀수사국(United States Secret Service)과 이민세관집행국(U.S Immigration and Customs Enforcement) 등으로 이루어진 연방수사국(the Federal Bureau of Investigation, FBI)과 미국국토안보부(the Department of Homeland Security, DHS)의 지원을 받는, 미국 법무부(DOJ)도 역시 컴퓨터를 개인 정보(또는 기타 정보)를 취득하는 개별주체들을 강력하게 수사하고 있다. 모든 점에서 미루어 볼 때, 이러한 노력들은 개인정보에 대한 비밀유지(confidentiality)를 보호하고 신원도용 그리고 개인정보의 남용과 같은 다른 범죄들을 당한 희생자들을 위해 법률의 제제를 시행하는데 도움이 된다.

(3) 개인정보 보호를 위한 지침

연방 기관들은 또한 민간 부문에서 광범위한 책임성을 가지고 있는 개인정보에 관한 지침을 만들기 위한 자원들에도 노력을 쏟고 있다. 예를 들어, 보건복지부(the Department of Health and Human Services, HHS)는 개인식별정보(personally identifiable information)를 포함하는 보안 침해에 대한 대응을 둘러싼 몇 가지 근본적인 이슈들을 분석하는 지침들을 발표해 왔다. 2009년에, 보건복지부(HHS) 인권사무소(Office for Civil Rights ,OCR)는 의료 정보를 사용할 수 없고, 읽을 가치가 없고, 해독할 수 없는 상태가 되게 하는 기술들과 방법론들을 특정함으로써, 의료정보가 안전한 것으로 여겨지는 그리하여 통지 의무들로 위반으로부터 면제되는 경우에 대한 지침을 발표하였다. 2010년에도 보건복지부 인권사무소(OCR)는 의료정보보호법 사생활보호 규칙(HIPAA Privacy Rule)의 “최소한의 필요(minimum necessary)” 기준 및

의료정보보호법 사생활보호 규칙(HIPAA Privacy Rule) 하의 의료정보의 역동일시(de-identification)에 관한 추가적인 지침을 발표하는 계획을 세웠다.

연방 기관들은 보다 효과적인 현행 사생활보호 수단들의 이용을 어떻게 가능하게 할 것인가에 관한 지침을 제공하고 있다. 2009년에, 8개의 연방 기관들은 금융 기관들이 그들이 소비자들에 대하여 금융현대화법(GLB)에 의하여 요청되는 개인정보 통지를 위하여 이용을 선택할 수 있는 개인정보보호 통지 형식 모형을 발표하였다. 이 형식에 대한 모형의 이용은 이 형식 모형이 요청되지 않음에도 불구하고, 금융현대화법 사생활보호 규칙(GLB Privacy Rule)을 따르는 법적인 세이프 하버를 제공한다. 이 기관들은 광범위한 소비자 연구 및 소비자들이 금융기관이 그들의 개인정보로 무엇을 하며, 쉽게 이해하고 다른 기관들의 정보 공유 관행들과 비교할 수 있도록 하기 위한 형식 모형의 개발에 대한 시험을 지휘하였다.

사생활보호에 관한 기타 주요 행정부 지침

• **사생활 및 정보 보안에 관한 공공의 인식 높이기** : 국토안보부(DHS)는 미국국민에게 사이버상의 안전 강화 및 미국인들이 그들의 온라인상의 안전과 보안을 증대시키는 것을 돕는 실용적 팁을 제공하기 위하여, 소위 멈추라. 생각하라. 연결하라(Stop. Think. Connect.)라고 불리우는 국내적 공공 인식 노력을 이끌어 내고 있다. 게다가 연방통상위원회(FTC)는 소비자 및 기업들이 아동의 온라인상의 개인정보 보호를 실행하고, 의료상의 신원도용을 최소화하며, P2P(peer-to-peer)[36] 파일 공유 애플리케이션을 통한 민감한 정보의 손실을 막을 수 있는 방법들을 설명하는 지침을 발표해 왔다.

• **새로운 기술에 대한 사생활보호 원칙들의 적용** : 행정부는 여기에서 발전된 일반적인 소비자 개인정보 체계가 특정, 위급한 상황에서도 적용된다는 것을 알려주는 동일한 사생활보호 원칙들을 입증하고 있다. “스

마트 그리드(Smart Grid)” - 정보통신 기술들이 전력망의 결함이 보다 효율적이고 보다 깨끗한 에너지 자원을 수용하며, 새로운 직업과 개혁의 원천을 만드는 - 가 그 훌륭한 예이다. 과거 2년 넘게, 미국국립기술표준연구소(NIST)는 이해관계인들에게 유망한 새로운 기술들로부터 야기될 수 있는 사생활보호 이슈들을 이해시키는 노력을 했다. 이 작업은 주정부가 스마트 그리드(the Smart Grid)가 만들어 낼, 포괄적인 공정정보규정(FIPPs)을 세부적인 에너지 사용 정보를 보호하기 위한 시작점으로 만들 것을 권고하는, 행정부의 “21세기 전력망을 위한 정책 체계(Policy Framework for The 21st Century Grid) : 우리의 에너지 미래를 안전하게 하는 것”으로 종결되었다.

(4) 사생활보호의 연방 기관 구조상의 통합

결국, 연방기관들은 사생활보호를 그들의 조직과 운영으로 포함시키고 책임있는 기구들을 개발하는 일에 앞장서고 있다. 이러한 실행과 수단을 향상시키는 책임성의 어떤 부분들은 민간 부문과 전 세계에서 논의되고 있다. 예를 들어, 새로운 정보 체계에서, 그리고 2002 미국 전자정부법(2002 E-Government Act) 하에서 발생하는 잠재적인 사생활보호 이슈들에 대한 잘 만들어진 평가서들을 제공하는, 개인정보영향평가(Privacy Impact Assessments, PIAs)의 이용을 개척하였던 국제수입서비스(the International Revenue Service, IRS)와 국토안보부(DHS)는 어떤 상황들하에서 연방기관들을 필요로 한다. 앞서 설명한 행정부의 노력들을 구축하기 위하여, 행정부는 개인정보영향평가(PIAs)의 이용을 소셜 미디어(social media)에 확대시켜왔다. 연방 정부 내에서 개인정보영향평가(PIAs)의 초기 발전 이래로, 이것은 민간부문 및 유럽연합(EU) 내에서도 폭넓게 사용되어 왔다. 연방기관들은 또한 사생활보

36) 인터넷을 통해 각자의 컴퓨터 안에 있는 음악파일나 문서·동영상 파일뿐만 아니라 DB, CPU 등을 공유할 수 있게 해주는 기술

호 전문가들을 그들의 상위 지도기관으로 계속해서 편입시키고 있다. 여러 연방 기관들은 그들의 기관 내에서 연방 정부 내에서 그리고 일반 국민들과 함께 사생활 보호 이슈에 관하여 보다 광범위한 논의에 종사하는, 상근 전문 최고정보보호 책임자(Chief Privacy Officer)를 두고 있다.

제 4 장 결 론

개인정보의 중요성에 대한 공감대는 전 세계적으로 형성되고 있다. 이에 EU의 일반정보보호규정(안) 제정 및 잊힐 권리의 법제화, 미국 백악관 및 FTC를 중심으로 이루어지고 있는 프라이버시 보호 관련 정책 추진 등 주요 국가들은 개인정보 보호를 위한 정책 및 입법적 노력을 경주하고 있다. 한편 우리나라도 최근「개인정보보호법」제정을 통해 EU의 잊힐 권리에 대응하는 개인정보의 정정·삭제 요구권[37], 개인정보의 처리 정지 요구권[38] 등이 구체적인 예외 사유에서

37) 개인정보보호법 제36조(개인정보의 정정·삭제) ① 제35조에 따라 자신의 개인정보를 열람한 정보주체는 개인정보처리자에게 그 개인정보의 정정 또는 삭제를 요구할 수 있다. 다만, 다른 법령에서 그 개인정보가 수집 대상으로 명시되어 있는 경우에는 그 삭제를 요구할 수 없다.
② 개인정보처리자는 제1항에 따른 정보주체의 요구를 받았을 때에는 개인정보의 정정 또는 삭제에 관하여 다른 법령에 특별한 절차가 규정되어 있는 경우를 제외하고는 지체 없이 그 개인정보를 조사하여 정보주체의 요구에 따라 정정·삭제 등 필요한 조치를 한 후 그 결과를 정보주체에게 알려야 한다.
③ 개인정보처리자가 제2항에 따라 개인정보를 삭제할 때에는 복구 또는 재생되지 아니하도록 조치하여야 한다.
④ 개인정보처리자는 정보주체의 요구가 제1항 단서에 해당될 때에는 지체 없이 그 내용을 정보주체에게 알려야 한다.
⑤ 개인정보처리자는 제2항에 따른 조사를 할 때 필요하면 해당 정보주체에게 정정·삭제 요구사항의 확인에 필요한 증거자료를 제출하게 할 수 있다.
⑥ 제1항·제2항 및 제4항에 따른 정정 또는 삭제 요구, 통지 방법 및 절차 등에 필요한 사항은 대통령령으로 정한다.

38) 개인정보보호법 제37조(개인정보의 처리정지 등) ① 정보주체는 개인정보처리자에 대하여 자신의 개인정보 처리의 정지를 요구할 수 있다. 이 경우 공공기관에 대하여는 제32조에 따라 등록 대상이 되는 개인정보파일 중 자신의 개인정보에 대한 처리의 정지를 요구할 수 있다.
② 개인정보처리자는 제1항에 따른 요구를 받았을 때에는 지체 없이 정보주체의 요구에 따라 개인정보 처리의 전부를 정지하거나 일부를 정지하여야 한다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 정보주체의 처리정지 요구를 거절할 수 있다.
1. 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우
2. 다른 사람의 생명·신체를 해할 우려가 있거나 다른 사람의 재산과 그 밖의 이익을 부당하게 침해할 우려가 있는 경우

정도의 차이는 있지만 법제화되어 있다.

그러나 개인정보는 개인정보의 이용과 보호라는 양립할 수 없는 두 이념적 가치를 균형·조화롭게 입법적으로 제도화 하는 것은 쉽지 않은 난제들을 전제로 하고 있다. 이런 점에서 유럽네트워크정보보호원(ENISA)도 EU의 '잊힐 권리'의 법제화에 대하여 현실적인 실현 가능성에 의문을 가지고 기술적·법적 조치의 중요성을 강조하고 있다. 미국 백악관 및 FTC 위원회에서 발표한

소비자프라이버시 권리장전, 프라이버시 정책 프레임워크를 살펴보아도 법적 규제외에 자율 규제, 기술적 조치의 중요성도 같이 언급되고 있다.

< FTC의 프라이버시 정책 프레임 워크 및 실행 권고 >[39]

<범 위>

최종 범위 : 프레임워크는 연간 5,000명 미만의 소비자에 관한 비민감정보를 수집하고 데이터를 제3자와 공유하지 않는 기업이 아닌 경우에 한하여, 특정 소비자, 컴퓨터 또는 다른 기기에 합리적으로 연결될 수 있는 소비자 데이터를 수집하거나 사용하는 모든 영리 기관에 적용된다.

3. 공공기관이 개인정보를 처리하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우

4. 개인정보를 처리하지 아니하면 정보주체와 약정한 서비스를 제공하지 못하는 등 계약의 이행이 곤란한 경우로서 정보주체가 그 계약의 해지 의사를 명확하게 밝히지 아니한 경우

③ 개인정보처리자는 제2항 단서에 따라 처리정지 요구를 거절하였을 때에는 정보주체에게 지체 없이 그사유를 알려야 한다.

④ 개인정보처리자는 정보주체의 요구에 따라 처리가 정지된 개인정보에 대하여 지체 없이 해당 개인정보의 파기 등 필요한 조치를 하여야 한다.

⑤ 제1항부터 제3항까지의 규정에 따른 처리정지의 요구, 처리정지의 거절, 통지 등의 방법 및 절차에 필요한 사항은 대통령령으로 정한다.

<디자인에 의한 프라이버시>
기본 원칙 : 기업은 조직 전반에 걸쳐 그들의 제품과 서비스 개발부터 모든 단계에서 소비자의 프라이버시 보호를 촉진해야 한다.

A. 실질적인 원칙
최종 원칙: 기업은 데이터 보안, 합리적인 수집 제한, 견고한 보존 및 처분 관행, 그리고 데이터의 정확성 등과 같은 실질적인 프라이버시 보호를 그들의 관행상 포함시켜야 한다.

B. 실질적인 원칙을 구현하기 위한 절차적 보호
최종 원칙: 기업은 그들의 제품과 서비스의 생명 주기 전반에 걸쳐 포괄적인 데이터 관리 절차를 유지하여야 한다.

<소비자 선택의 단순화>
기본 원칙 : 기업은 소비자의 선택을 단순화하여야 한다.

A. 선택을 필요로 하지 않는 관행
최종 원칙 : 회사는 거래의 문맥 또는 소비자와 기업간 관계에 부합하거나, 또는 법률에 의해 요청되거나 특정 권한이 부여된 관행에 관하여 소비자 데이터의 수집 및 사용 전 선택을 제공할 필요가 없다.
선택이 필요 없는 관행의 유형을 제한할 필요성과 유연성의 균형을 도모하기 위하여, 위원회는 최종 프레임워크를 다듬어 소비자의 거래 맥락에 부합하는 관행과 관련된 기업에게는 그러한 관행에 대한 선택을 제공하지 않아도 된다고 하였다.

B. 기업은 그 밖의 관행을 위한 소비자 선택을 제공하여야 한다.
최종 원칙 : 선택을 필요로 하는 관행에 있어, 기업들은 소비자가 자신의 데이터에 관한 결정을 내릴 수 잇도록 한 번에, 하나의 문맥 내에서 선택을 제공하여야 한다. 기업은 (1) 소비자 데이터가 수집된 때 명시된 방법과 실질적으로(materially) 다른 방법으로 소비자 데이터를 이용하기 전 또는 (2) 특정 목적을 위하여 민감정보를 수집하기 전 명시적인 동의를 얻어야 한다.
위원회는 소비자의 온라인 행동 추적에 관한 소비자의 통제를 강화하려는 산업계의 노력, 즉 추적방지 메커니즘의 도입을 언급하고, 이러한 메커니즘의 지속적 개선과 온전한 이행을 장려하였다.

<투명성>
기준 원칙 : 기업은 그들의 데이터 관행상 투명성을 제고하여야 한다.

A. 프라이버시 통지
최종 원칙 : 프라이버시 통지는 보다 명확하고, 간결하며, 보다 이해하기 쉬우며 프라이버시 관행을 비교할 수 있도록 표준화되어야 한다.

B. 접근
최종 원칙 : 기업은 그들이 보유하고 있는 소비자 데이터에 대한 합리적인 접근을 제공하여야 한다; 접근의 범위는 데이터의 민감성과 본질에 비례하는 것이어야 한다.
위원회는 정보 브로커의 관행에 관한 특정 권고를 포함시킴으로써 이 원칙을 지지하였다.

C. 소비자 교육
최종 원칙 : 모든 이해관계자는 상업적 데이터 프라이버시 관행에 관한 소비자 교육에 대한 노력을 증진하여야 한다.

<입법적 권고>
위원회는 현재 의회에 프라이버시 기본 입법을 고려해 줄 것과 데이터 보안 및 데이터 브로커 입법에 관한 개정을 요청하였다. 위원회는 의회, 이해관계자들과 함께 이러한 입법안을 마련할 것이다. 동시에, 위원회는 산업계에 자율규제의 속도를 높여 줄 것을 요청하였다.

<FTC는 5개 핵심 영역에서의 이행을 지원>
위원회는 최종 보고서에서 논의한 바와 같이, 정책 입안자들이 최종 프라이버시 프레임워크를 구성하는 자율 규제 원칙들의 원칙을 이행하기 위한 지원 역할을 담당해 주어야 하는 특정 분야가 있음을 지적하였다. 그 분야는 다음과 같다.

1. 추적방지
산업계는 추적방지 구현에 상당한 진전을 이루었다. 디지털 광고협회(“DAA”)는 아이콘 기반의 툴을 개발하여 브라우저 도구를 이용하고, 월드 와이드 웹 컨소시엄(“W3C”)은 추적방지를 위한 국제 표준을 마련하

는데 실질적인 진보를 이루었다. 그럼에도 불구하고, 작업이 완전히 끝난 것은 아니다. 위원회는 이러한 그룹들과 함께 사용하기 쉽고 효과적인 시스템 마련을 위한 작업을 수행할 예정이다.

2. 모바일

위원회는 모바일 서비스를 제공하는 기업들에게, 짧고 의미 있는 공개 등을 포함한 프라이버시 보호의 개선을 요청하였다. FTC 직원들은 온라인 광고 공개에 관한 기업 가이드라인을 업데이트하는 프로젝트를 발주하고 워크숍을 진행할 예정이다. 위원회는 이 워크샵을 통해 해당 영역에서 산업계의 자율 규제가 촉진될 것으로 기대하고 있다.

3. 데이터 브로커

데이터 브로커의 소비자 정보 수집 및 활용에 대한 소비자의 통제 부족, 비가시성 문제 등을 해결하기 위하여, 위원회는 제112차 국회에 상정된 몇몇의 데이터 보안 법안 내 포함된 것과 유사한 내용, 즉 소비자에게 데이터 브로커가 보유하고 있는 정보에 접근할 수 있도록 규정하는 입법을 지원한다. 투명성을 제고하기 위하여, 위원회는 마케팅 목적을 달성하기 위한 데이터를 컴파일하는 데이터 브로커에게, 데이터 브로커가 (1) 소비자에게 그들이 소비자 데이터를 수집하고 활용하는 방법과 자신의 신원을 확인하도록 하고 (2) 그들이 보유하고 있는 소비자 데이터에 관하여 접근권을 설명하고 선택을 제공하는 웹사이트를 생성할 것을 요청하였다.

4. 대형 플랫폼 제공자

인터넷 서비스 제공자, 운영 체제, 브라우저 및 소셜 미디어 등의 대형 플랫폼의 경우, 소비자의 온라인 활동 추적이 매우 강도 높은 프라이버시 문제를 야기한다. 이러한 유형의 추적과 관련한 프라이버시 및 다른 문제를 탐구하기 위하여, FTC는 공개 워크샵을 개최할 계획이다.

5. 강제 집행력 있는 자율 규제 강령의 촉진

상무부는 산업계의 이해관계자들의 지원을 얻어 특정 부문별 행동 강령 마련을 촉진하기 위한 프로젝트에 착수하였다. FTC는 이러한 프로젝트에 참여할 예정이다. 강력한 프라이버시 강령이 마련될 경우, 위원회는 이러한 강령이 법 집행과 연관성을 맺도록 검토하게 될 것이다. 위원회는 또한 자율 규제 프로그램에 참여하였으나 준수에 실패하거나, 불공정 또

는 기만적인 관행에 연루된 기업에 대한 조치를 취할 수 있도록 FTC 법을 지속적으로 강화해 나갈 방침이다.

'프라이버시 라운드'라는 말에서도 볼 수 있듯이 개인정보보호문제는 글로벌 웹 환경을 기반으로 하기 때문에 단순히 국내 문제로 한정할 수 없을 뿐만 아니라, 향후 국가 간의 합의로 EU처럼 국제 규범화를 통해 국가간 공동 대응을 전제로 한다. 따라서 글로벌 동향에 대한 지속적인 파악을 통해 글로벌 스탠더스에 부합하는 국내 정책 및 입법의 방향을 모색해가야 할 것이다.

39) FTC, "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers", 2012.3.(http://www.ftc.gov/opa/2012/03/privacyframework.shtm)의 주요 내용으로 글로벌 동향의 파악, 국내 입법 및 정책의 방향을 위하여 참고로 소개한다.

참 고 문 헌

Proposal for a 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)

Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data

ENISA, “The right to be forgotten - between expectation and practice”, 2012.11.20.(http://www.enisa.europa.eu)

THE WHITE HOUSE, Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy, 2012.1

FTC, “Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers”, 2012.3.(http://www.ftc.gov/opa/2012/03/privacyframework.shtm)

최경진, “잊혀질 권리 - 개인정보 관점에서”, 정보법학 제16권 제2호, 2012.

한국정보화진흥원, “‘잊혀질 권리’의 법적 쟁점과 개선 방향”, 2012. 11.

지성우, “소위 ‘잊혀질 권리(Right to be forgotten)’에 관한 탐색적 연구”, 정보법학 제15권 제3호, 2011

최경진, “잊혀질 권리의 국내외 동향 및 제도화”, 「잊혀질 권리와 디지털 자유 대토론회 자료집」, 2013.

이민영, “잊혀질 권리 실현을 위한 법제화 방향”, 「잊혀질 권리와 디지털 자유 대토론회 자료집」, 2013.

함인선, “EU 개인정보보호법제에 관한 연구 - ‘2012년 개인정보보호 규칙안’을 중심으로 하여”, 「저스티스」 통권 제133호(2012.12).

민윤영, “인터넷상에서 잊혀질 권리와 「개인정보보호법」에 대한 비교법적 고찰”, 고려법학 제63호, 2011. 12.

문재완, “잊혀질 권리의 입법 현황과 향후 과제”, 한국정보법학회 세미나 자료집(2012.3.13.)

문재완, “프라이버시 보호를 목적으로 하는 인터넷 규제의 의의와 한계”, 언론과 법 제10권 제2호, 2011.