규제연구 제13권 제2호 2004년 12월

위치정보 규제와 개인정보 보호

이 영 대* · 최 경 규**

(접수일 : 4/22, 게재확정일 : 5/27)

위치기반서비스의 구현에서 핵심적인 역할을 하는 것은 위치정보이다. 이러한 위치정보의 대상이 '사람'일 경우에 그 개인의 위치정보는 개인정보 보호 및 프라이버시(사생활) 보호의 문제와 직결된다. 개인정보 보호와 프라이버시 보호를 구별하는 것은 개인위치정보가 성명, 주민등록번호, 주소, 전화번호 등과는 달리 직접적으로 사생활 침해를 발생시킬 수 있기 때문이다. 따라서 개인위치정보는 여타의 개인정보에 비해 보다 강력한 보호가 필요하다는 것을 의미한다. 가까운 장래에 우리나라에서 위치기반서비스가 활발하게 이루어 질 것을 감안할 때, 법제도적으로 서비스의 신뢰를 높이고, 서비스 제공자와 고객이 모두 만족할 수 있는 규율을 만드는 것이 필요하다. 위치정보보호법은 정보계약, 위치정보의 규제와 프라이버시, 민감 개인정보에 대한 보호강화를 포함하여야 한다.

핵심용어 : 개인정보 보호, 위치기반서비스, 위치정보, 정보계약, 프라이버시 보호

*법무법인 수호 변호사, 서울시 서초구 서초동 1533-13 영암빌딩 2층 이영대 법률사무소 (pydl@unitel.co.kr)

**국회예산정책처 산업사업평가 팀장, 서울시 영등포구 여의도동 27-1 한국투자증권빌딩 19층 국회예산정책처(gchoi@nabo.go.kr)

Ⅰ. 서 론

IT기술의 급속한 발전으로 인한 정보화 사회의 도래와 함께 인터넷은 우리 생활 전반에 깊숙이 자리잡아 가고 있다. 텔레매틱스telematics로 알려진 정보, 커뮤니케이션 그리고 차량 내지 이동전화 장치에서 오락물의 제공 등은 위치기반서비스가 가능해짐에 따라 엄청난 성장과 관심을 받고 있다. 또한, 위치기반시스템을 통하여, 지능형 교통 시스템(Intelligent Transportation System, 'ITS')은 교통관리기관이 개인이 어디로 여행하는지, 그들이 어느 경로로, 얼마만큼 여행할 것인지를 알 수 있게 할 수 있다. 위치에 민감한 콘텐츠location-sensitive content, 광고와 개인화 서비스는 현재 전개되고 있다.

모바일 커머스와 관련한 특정 법적 이슈들은 대체로 다음의 단계 중 하나에 해당한다.[1)]

ⅰ) (필수요소의) 설정Setup: Prerequisites

ⅱ) (모바일기기를 통한) 접속Access

ⅲ) (정보제공자와 소비자간에 전달되는) 콘텐츠Contents

ⅳ) (모바일 전자거래) 계약Contracting

ⅴ) (네트워크상의 정보의) 이전Transit

ⅵ) (지불) 이행Fulfillment: Payment

이 중 접속 단계에서의 가장 큰 이슈는 프라이버시(사적자유)이다. 프라이버시는 '기밀성'의 이슈와 유사하나, '혼자 있을 권리'를 포함한다. 그러나 현재의 셀 기반cell based은 휴대폰을 켜는 순간 사용자 위치의 인식을 가능케 한다. 그 결과로, 사용자의 인지와

1) 이영대 · 최경규, 「모바일 비즈니스 법제 기초 연구」, 『기업의 모바일 비즈니스 활성화 방안 연구』, 전자거래진흥원, 2003.

의지와는 무관하게 사용자의 움직임은 추적당할 수 있다. 이 위치인식은 상업적 운영자에게는 큰 기회를 부여하는데, 타깃 마케팅이 그중 하나이다. 그러나 이 현상은 소비자의 혼자 있을 권리를 위협한다.

우리나라는 2000년말부터 이동통신사를 중심으로 교통정보, 친구찾기 서비스 등을 제공하여, 2003년 7월말 기준으로 376만 명의 가입자로부터 월 60억원의 매출을 올리고 있다. OVUM에 의하면 세계 위치정보서비스(location-based service: LBS) 시장은 매년 200~300% 성장하여 2003년 10억 7천만 달러의 규모에 이르렀고 2005년에는 61억9천5백만 달러로 급성장할 것으로 전망한다. 국내시장 또한 2003년의 5천9백만 달러에서 2005년 2억9천5백만 달러로 급격히 증가할 것으로 전망되고 있다.[2)]

이 밖에 LBS는 긴급 구난구조 서비스, 물류/운송 관제 서비스, 문화 관광분야 등에서 광범위하게 사용될 수 있다. 그러나 LBS는 그 서비스의 효용과 함께 개인정보 및 프라이버시의 침해가능성이라는 역기능이 상존하고 있다. 즉 위치정보는 다양한 방법으로 수집 가능하나, 응용 서비스의 보급과정에서 오·남용될 경우 개인의 사생활과 재산권이 침해될 우려가 있다. 위치정보의 이용에 대한 공유성, 보안성 및 사후 관리 측면에서 프라이버시 보호 방안 마련이 지속적으로 요구되어 왔다.

이러한 요구에 부응해 위치정보보호 관련법인 '정보통신망이용촉진및정보보호등에관한법률중개정법률안'이 국회에 의해 발의돼 2003년 12월 29일 국회 본회의 의결을 통과하였다. 또한 정보통신부는 2004년 4월에 현행 '정보통신망이용촉진및정보보호등에관한법률' 내에 포함된 개인정보 보호 관련 조항 하위 개별법 등을 분리해 '민간부문개인정보보호에관한법률(가칭)'로 입법화하고 본격적으로 작업에 나섰다.[3)] 한편, 정보통신부에 의해 2003년 발의된 '위치정보이용및보호등에관한법률(안)'은 차세대 이동통신산업 육성 및 긴급 구난구조시 활용도라는 명분에도 불구하고 사생활 침해에 대한 우려 탓에 뜨거운 논란을 야기하였고, 2004 정기국회에 재상정될 예정이다.

미국의 경우, 이동통신산업협회(Cellular Telecommunications Industry Association, CTIA)는 위치정보 프라이버시 원칙을 연방통신법에서 실행하기 위한 규칙제정을 연방

---

2) 김도경, 「위치정보보호법의 제정에 따른 LBS산업의 규제정책 방향」, 『정보통신정책』, 제15권 19호, 2003.

3) 전자신문 사이트, http://www.etnews.co.kr/news

통신위원회(Federal Communications Commission: FCC)에 요청하였다.[4)]

유럽의 위치정보규제 관련법은 EU가 개인정보 처리와 원활한 이동을 보장하기 위해 프라이버시가 존중되어야 함을 강조하고 프라이버시 보호가 미흡한 다른 국가로의 개인정보 이전을 금지하고 있는 것이다. 그리고 이용자 사전 동의와 위치정보 이용 후 저장 금지 등을 명시하고 있는 '이동통신환경하의 개인정보 보호와 처리에 관한 규정'을 제정하였다.

본고는 위치정보 규제에 관한 비교법적 규제연구를 통하여 위치정보 규제를 개인정보 보호와 정보계약의 관점에서 통합적으로 이해하고 우리나라에 대한 함의를 도출하고자 한다.

Ⅱ. 개인정보 보호 관련 법제 검토

1. 개 요

정보화 사회가 심화되어 정보가 제3의 자원이 되면 당연히 개인정보까지도 수집·정리·보관 및 전파의 대상이 된다. 그러한 과정에서 개인이 공개되기를 꺼리는 자기만의 사적 영역의 정보도 부득이 공개되거나 타인에 의해 수집·관리되는 경우가 있게 마련이다. 실제로 현재 정부나 기업에 의하여 정보를 절취당하거나 개인기록이 악용되는 사례는 점점 늘어가고 있으며 불법도청이 정치사회 문제화한 경우도 허다하다.

이러한 배경하에서 대다수 국가들은 사생활 및 개인정보를 헌법 또는 법률의 차원에서 보호하기에 이르렀는바, 개인정보보호법을 제정한 각국의 입법은, 개인데이터의 보호 대상 분야를 일괄 규제할 것인가 아니면 규제대상마다 별개의 입법을 할 것인가에 따라 차이를 보이고 있다. 독일의 연방 데이터 보호법이 대표적인 유럽의 여러 나라는 공적분야와 민간 분야를 함께 취급하는 옴니버스omnibus방식을 채용하고 있는 데 반하여 privacy act를 대표적 법률로 하는 미국은 공적분야와 민간분야를 별개로 할 뿐 아니라 별개의 영역에 대해 별개의 법률을 제정하는 이른바 세그먼트segment방식을 취하고 있는

4) Michael F. Altschul, *The CTIA location information privacy petition*, 2001.5. p.2.

것이 대표적인 특징이라고 할 수 있다.[5)]

우리나라는 미국의 법제와 유사하게 공적분야와 민간분야를 별개로 하면서 별개의 영역에 대해 별개의 법률을 제정하는 이른바 세그먼트segment방식을 취하면서도 대국가적인 면에서는 '공공기관의개인정보보호에관한법률'이라는 일반법을, 대사인간의 관계에서는 '정보통신망이용촉진및정보보호에관한법률'의 제정으로 개인정보 보호에 관한 일반법을 가지게 되어 양자의 방식을 절충하는 법제를 취하고 있다고 볼 수 있다.

위치기반서비스를 통해 제공되는 위치정보의 경우도 그 서비스의 효용과 함께 개인정보 및 프라이버시의 침해가능성이라는 역기능이 상존하고 있다. 비근한 예로, 2004년 8월 22일 지리산 등산 중 실종된 김모씨의 휴대폰번호에 대한 위치추적이 영장을 요구하는 현행 법규정('개인정보보호에관한법률')으로 인해 절차에 시간이 소모되어 구조 후에 숨진 사건이 있다. 이는 긴급 조난구조시 소방방제청 등에서 개인의 위치정보를 알 수 있는 '위치정보의이용및보호에관한법률안'(이하 '위치정보법')이 통과됐다면 목숨을 구할 수도 있었던 위치정보의 긍정적인 기능의 단면을 보여준다. 반면, 삼성그룹계열사의 삼성SDI 전현직 직원 9명이 불법복제된 휴대폰으로 회사 측에 의해 위치추적을 당했다며, 삼성의 간부 7인을 통신비밀보호법 및 정보통신이용촉진및정보보호등에관한법률 위반혐의로 고소한 사건은 개인위치정보 및 개인정보 침해의 문제로서 사회문제화되었다.

이에 대해 이동통신업체들과 솔루션업체들은 '위치정보법'이 지나친 정보보호로 관련 산업의 성장을 억제해서는 안 된다는 입장이고, 참여연대, 진보네트워크 등 시민단체들은 '위치정보법'이 위치정보이용에 따른 개인정보 오남용의 여지가 커 '프라이버시 영향평가'를 실시해 인권침해 요소를 제거해야 한다는 입장으로 대립하고 있다.

위치정보의 이용에 대한 공유성, 보안성 및 사후 관리 측면에서 프라이버시 보호의 방안은 마련되어야 한다. 미국과 유럽의 경험에 비추어 볼 때 위치정보 법제의 기본은 위치정보의 보호로 요약될 수 있다. 이를 여하히 보호하느냐에 따라 이에 관한 산업 발전의 수준과 정도가 결정되기 때문이다. 이는 위치정보가 소비자에게 매우 민감하고 중요한 정보라는 점에서 더욱 중요성이 강조되고 있다. 위치기반서비스에 관한 법률에서 개인정보 보호를 위해 필요한 규정들을 마련하는 것이 필수적이다.

---

5) 박용상, 「정보보호법제」, 『정보사회와 사회윤리』, 아산사회복지사업재단, 1996, p.194.

2. 개인정보규제의 근거

(1) 헌법적 근거

개인정보를 보호하는 헌법적 근거는 헌법 제17조 및 제10조를 직접적 근거로 하는 '프라이버시의 권리' 내지 '일반적 인격권'에 있다. 개인정보 보호 법제를 이해하는 데 있어서는 국가와 국민간의 관계와 사인간의 관계를 나누어 이해하여야 한다. 국민의 국가에 대한 관계에서는 알권리 내지 정보공개청구권이 국민에게 일반적으로 보장되는 기본권이므로 국가 등 공공기관이 보유하는 정보는 개인정보의 성격을 가지고 있더라도 공개함이 원칙이고(공공기관의 정보공개에 관한 법률) 정당한 사유가 있는 때 예외가 인정되는 것임에 반하여, 사인간의 관계에서 정보공개의 법리는 적용되지 않기 때문에 정보를 구하는 측이 알권리를 근거로 타 개인이 보유·관리하는 정보를 요구할 수 없음은 물론이고 특히 그 정보의 내용이 타인의 개인적 프라이버시에 관한 것이면 그 정보주체의 '프라이버시권' 내지 '자기정보관리통제권' 사이의 이해조정을 필요로 하게 되는 것이다.[6)]

(2) 형법상 근거

형법은 제35장 '비밀침해의 죄'에서 사생활의 비밀이라는 개인적 법익을 보호하는 죄를 규정하고 있다. 제316조 제2항에서는 '봉함 기타 비밀장치한 사람의 편지, 문서, 도화 또는 전자기록 등 특수매체기록을 기술적 수단을 이용하여 그 내용을 알아낸 자도 제1항의 형과 같다'라고 규정하여 3년 이하의 징역이나 금고 또는 500만원 이하의 벌금에 처할 수 있도록 하고 있으며 제347조의2에서 '컴퓨터 등 사용사기'라는 신종범죄를 처벌하도록 규정되어 있다. 즉 컴퓨터 등 정보처리장치에 허위의 정보 또는 부정한 명령을 입력하여 정보처리를 하게 함으로써 재산상의 이익을 취득하거나 제3자로 하여금 취득하게 한 자는 10년 이하의 징역 또는 2000만원 이하의 벌금에 처한다고 되어 있다.

이는 모두 개인정보 보호를 최종적으로 담보한다고도 볼 수 있는 처벌조항인데, 개인정보에 관한 개별법은 각각 그 벌칙조항에 개인정보 보호에 저해되는 행위를 한 자를

6) 박용상, 전게서, p.121.

처벌하는 특별조항을 둠으로써 실제적으로는 각 특별법이 우선적으로 적용되는 경우가 대부분이다.

(3) 불법행위법의 적용

위치정보는 프라이버시 침해를 이유로 하는 불법원인법의 적용 범위가 된다. 프라이버시의 본질은 '간섭받지 않을 권리right to solitude'이다. 종래 i) 상업적 이용, ii) 왜곡, iii) 사적 영역, iv) 사생활의 비밀이 프라이버시의 주된 영역이었다. 이를 내용별로 분류하면 다음과 같다.

- 정보 프라이버시information privacy : 신용정보와 의료기록과 같이 지극히 개인적인 정보들의 취급과 수집을 다루는 경우
- 신체 프라이버시bodily privacy : 개인의 약의 복용이나 충치 검사들과 같이 신체 질환과 결점에 관한 정보보호
- 영역 프라이버시territorial privacy : 가정과 직장, 기타 공공장소에서의 침해의 제한
- 통신 프라이버시privacy of communication : 우편과 전화, e-mail과 다른 형태의 통신의 프라이버시와 안전

이러한 열거에서 강조되어야 할 점은 프라이버시에 대한 정의에 나열되어 있지 않다 하더라도 "어떻게 보면, 모든 인권은 프라이버시의 권리의 측면과 같다"라는 명제가 시사하는 바와 같이 경시되어서는 안 된다는 것이다.

3. 현행법제의 구조

우리나라는 공공기관의 개인정보 보호에 관한 법률이 일반법으로 제정되기 이전에 이미 개인정보 보호의 필요성이 시급한 사회문제로 됨에 따라 개별적으로 개인정보를 보호하는 법률을 제정하여 왔다. 지금까지 제정된 개인정보보호법제를 개괄하면 공공기관이 보유하는 개인정보에 관한 보호법으로서는 '공공기관의 개인정보 보호에 관한 법률'을 필두로 '주민등록법' 등이 있으며, 민간보유의 개인정보에 대하여는 금융정보를 보호하는 '금융실명거래및비밀보장에관한법률', 개인신용정보에 관하여는 '신용정보의 보호와이용에관한법률'이 있다. 특히 2001.7.1. 전문 개정되어 시행되는 '정보통신망이

용촉진및정보보호에관한법률'은 금융, 신용정보를 막론하고 민간부문에서 정보통신서비스 제공자가 광범위하게 개인정보를 수집할 수 있는 점을 고려하여 개인정보 보호를 강화하는 내용을 담고 있는바, 민간부문의 개인정보 보호에 대한 일반법으로서의 성격을 가지게 되었다.[7]

(1) 공공기관의 일반적 개인정보 보호

1) 공공기관의개인정보보호에관한법률

본 법률은 제1조에 규정되어 있는 바대로, "공공기관의 컴퓨터에 의하여 처리되는 개인정보의 보호를 위하여 그 취급에 관하여 필요한 사항을 정함으로써 공공업무의 적정한 수행을 도모함과 아울러 국민의 권리와 이익을 보호함"을 목적으로 한다.

동법 제4조는 개인정보의 수집에 관하여 "공공기관의 장은 사상, 신조 등 개인의 기본적 인권을 현저하게 침해할 우려가 있는 개인정보를 수집하여서는 아니 된다. 다만, 정보주체의 동의가 있거나 다른 법률에 수집대상 개인정보가 명시되어 있는 경우에는 그러하지 아니하다"라고 규정하고 있다. 이는 인격영역론[8]에서 말하는 개인의 내밀 영역을 알 수 있는 연관성 있는 사항에 관하여는 원칙적으로 개인정보의 수집이 허용되지 않는 것이라는 의미이다.[9]

동법 제10조 제1항은 처리정보의 이용 및 제공에 관하여 "보유기관의 장은 다른 법률에 의하여 보유기관의 내부에서 이용하거나 보유기관 외의 자에게 제공하는 경우를 제외하고는 당해 개인정보화일의 보유목적 외의 목적으로 처리정보를 이용하거나 다른 기관에 제공하여서는 아니 된다"고 규정하고, 제2항에서는 그 예외사유를 규정하고 있다.

정보주체가 자신에 대한 정보의 내용과 유통을 통제할 수 있어야 하는 것은 자기정보

---

7) 김윤명 외 3인, 『사이버스페이스법』, 법률서원, 2001, p.169.

8) 박용상, 전게서, p.177; 인격영역론은 인격이 타인의 무단적인 인지, 특히 공적인 간섭으로부터 해방되어 보호를 받는 일정한 범위가 있다고 하는 점에서 출발하며, 인간생활의 여러 국면은 가장 내밀하고 비밀스러운 것으로부터 가장 공개적인 부분에 이르기까지 상이한 취급을 받게 되는 영역이 세분화된다는 이론으로 내밀 영역, 비밀영역, 사적 영역, 사회적 영역, 공개적 영역으로 그 범주를 나눈다. 이는 개인이 다른 특정 개인에 대하여 알고, 정보를 수집하는 데 대한 한계로서도 역시 기준이 된다고 한다.

9) 박용상, 전게서, p.205.

관리통제권으로부터 귀결되는 요청이다. 이에는 처리정보의 열람청구권과 정정청구권이 있다.

2) 전자정부구현을위한행정업무등의전자화촉진에관한법률

동법 제12조는 개인정보 보호의 원칙으로서 “행정기관이 보유·관리하는 개인정보는 법령이 정하는 경우를 제외하고는 당사자의 의사에 반하여 사용되어서는 아니 된다”라고 규정하고 있다.

(2) 공공기관 보유의 특정 개인정보 보호 : 주민등록법

우리나라에서 행정기관이 개인에 관하여 보유, 처리하는 가장 기본적인 정보인 주민등록에 관한 법으로서의 의의를 갖는다. 그 규제내용으로서, 주민의 등록 또는 그 등록사항의 정정이나 말소는 주민의 신고에 의하여 행함을 원칙으로 한다(제8조). 주민등록표에 기재되는 사항은 개인의 프라이버시에 관계되는 사항이 적지 않고, 법에 따라 이러한 내용을 신고한 개인으로서는 이들이 임의적으로 공개·이용되리라고 생각할 수는 없기에 주민등록법은 주민등록표의 등초본 교부와 주민등록 파일의 전산처리에 의한 이용에 관하여 정보보호를 위한 규제를 가한다.[10]

(3) 민간보유의 일반적 개인정보 보호

1) 정보통신망이용촉진및정보보호등에관한법률

동법 제2조 제6호에서는 개인정보를 “생존하는 개인에 관한 정보로서 당해 정보에 포함되어 있는 성명·주민등록번호 등의 사항에 의하여 당해 개인을 식별할 수 있는 정보(당해 정보만으로는 특정 개인을 식별할 수 없더라도 다른 정보와 용이하게 결합하여 식별할 수 있는 것을 포함한다)를 말한다”라고 규정하고 있으며 제4장에서 ‘개인정보 보호’라는 별도의 장을 두어 개인정보 보호를 강화하고 있다.

‘정보통신망이용촉진및정보보호등에관한법률’은 정보통신망의 이용을 촉진하되 정보통신 서비스제공자가 이용자의 사상, 신념, 병력 등 개인을 식별할 수 있는 정보는 신상정보를 동의 없이 수집, 이용 및 제3자에게 제공하는 것을 금지토록 규정하고 있다. 이

10) 박용상, 전게서, p.210.

것은 개인정보의 보호에 관한 일반적인 규정을 담고 있으면서도, 사회 경제적인 목적 및 공익증진 등을 위해 보다 특별하게 다루어야 할 개인정보의 이용과 보호에 대해서는 별도의 규정을 인정한다.

2) 전기통신사업법

동법 제34조의 4는 정보의 제공에 관하여 "①기간통신사업자는 다른 전기통신사업자로부터 전기통신설비의 제공·상호접속 또는 공동 사용 등이나 요금의 부과·징수 및 전기통신번호안내를 위하여 필요한 기술적 정보 또는 이용자의 인적사항에 관한 정보의 제공을 요청 받은 경우에는 협정을 체결하여 요청 받은 정보를 제공할 수 있다"라고 규정하고 있다.

(4) 민간보유의 특정 개인정보 보호

1) 신용정보의이용및보호에관한법률

소비자 신용정보와 관련하여서는, 통일적 법규제 없이 재무부의 '신용정보교환 및 활동지침'을 비롯한 구舊 신용조사업법 등에 의한 단편적 규제에 불과하던 것을 1995. 1. 5. 공포되어 동년 7. 6.부터 시행된 '신용정보의보호와이용에관한법률'이 이를 규제하게 되었다.[11]

2) 금융실명거래및비밀보장에관한법률

금융기관의 고객에 관한 비밀의 수호의무는 당사자간의 신뢰관계를 본질로 하는 은행계약의 부수적 의무로 생각되고 있으며 정보주체인 고객의 자기정보관리통제권에 그 법적 근거를 갖는다. 개인이 소유하는 재산내역 또는 그 금융기관에 관한 정보는 일반적 인격권의 이른바 비밀영역 내지 사적 영역에 속하는 사항이다. 그리고 이 금융기관의 비밀엄수의무는 제3자에 대한 관계에서는 정보제공거부권을 의미한다.[12]

3) 전자거래기본법

동법은 민간 전자거래에서 파생되는 거래 정보에 포함된 개인정보의 보호를 규제하고 있다. 즉 동법에서는 첫째, 전자거래당사자에게 개인정보수집 목적의 명시의무와 수집 목적 외의 사용금지의무를 부과한다. 둘째, 전자상거래당사자 등은 처리, 반송 또는

11) 박용상, 전게서, p.221에서 재인용.
12) 박용상, 전게서, p.214.

보관되는 정보에 대한 부당한 접근과 이용 또는 정보의 유출 등을 방지할 수 있는 안전대책을 마련해야 하며, 셋째, 개인정보에 대한 본인이 열람을 요구하는 경우 전자거래당사자 등은 지체 없이 응할 의무가 있고 오誤정보에 대한 증빙자료를 제시하여 정정 또는 삭제를 요구하는 경우에는 신속하게 필요한 조치를 취할 의무가 있다.

4) 전자서명법

'전자서명법' 제24조에서는 공인인증기관의 업무와 관련하여 개인정보의 보호를 규정하고 있다. 즉 공인인증기관은 인증업무를 수행함에 있어 필요한 최소한의 개인정보를 수집하도록 하고 있으며 본인의 동의 없이 개인정보를 수집하여서는 아니 된다고 규정하고 있다. 수집된 개인정보를 다른 목적으로 사용하거나 유출할 수 없도록 하고 있으며 가입자는 공인인증기관에 대하여 자신의 개인정보에 대한 열람신청을 할 수 있고 정정이나 삭제를 요구할 수도 있는데 이때 공인인증기관은 지체 없이 필요한 조치를 취하여야 한다.

'전자거래법'과 '전자서명법'은 본인이 자신의 개인정보에 대한 열람이나 정정, 삭제요구를 하는 경우 그 취급을 약간 달리하고 있다. '전자거래법'상 열람신청의 경우 전자거래당사자 등은 이에 응할 의무가 있으나 '전자서명법'의 경우는 지체없이 필요한 조치를 취하여야 한다고 규정하고 있다. 또한 '전자거래법'은 정정, 삭제요구시 본인이 잘못된 정보에 대하여 증빙자료를 제시할 것을 요건으로 하고 있는 데 반해 '전자서명법'에는 그러한 규정이 없다.

5) 통신비밀보호법

'통신비밀보호법'은 국가기관이 도청 등 전자감시에 의해 수사하는 경우 통신망을 통해서 이루어지는 대화 내용과 통신일시 및 로그기록 등 통신사실 확인자료 등을 보호하기 위한 법률로서 수사상 목적 외에는 그 내용 및 자료의 이용을 금지토록 규정하고 있다. 또한 현재 발신 기지국의 위치정보는 통신사실 확인자료로서 수사목적 이외에는 누구도 그 내용을 이용할 수 없도록 규정한다.

6) 약관의규제에관한법률

계약에 의한 개인정보 공개의 경우에도 계약이 현저하게 불공정하거나 부당하게 일방적으로 불리한 경우에는 개인정보 공개가 제한된다. 즉 동법 제11조는 고객의 권익보호를 선언하면서 "고객의 권익에 관하여 정하고 있는 약관의 내용 중 다음 각호의 1

에 해당되는 내용을 정하고 있는 조항은 이를 무효로 한다…… 4. 사업자가 업무상 알게 된 고객의 비밀을 정당한 이유 없이 누설하는 것을 허용하는 조항"이라는 구체적 조문을 두고 있다

Ⅲ. 위치정보 규제의 현황

1. 기본법 제정의 필요성

미국과 유럽 등 선진국에서는 일찍이 개인정보 보호에 대한 중요성이 논의되고, 위치에 기반한 개인의 정보 보호를 위한 법안이 지속적으로 정비되었다. 그러나 현재 우리나라에는 위치정보의 이용과 보호를 규정하고 있는 특별법은 없다. '전기통신사업법'과 '정보통신망이용촉진및정보보호에관한법률'(이하 '정보통신망법'), 그리고 '통신비밀보호법' 등에 의해 segment 방식에 의해 개별적으로 개인정보 보호가 이루어져 왔다. 그러나 설계 시점에서 LBS 환경을 고려하지 않았고, 사용자의 위치에 따른 정보를 고려 대상에 포함하지 않았기 때문에 현재에도 꾸준히 확장되어 가고 있는 LBS의 범위와 콘텐츠 분야를 고려할 때, 개인의 위치정보의 오남용을 효율적으로 막아내기에는 다소 무리가 따르는 것으로 보는 견해가 일반적이다.

'정보통신망법'은 개인정보의 수집 및 보호에 관한 일반원칙을 제시하고 있으며, 위치정보의 활용에서도 이 원칙이 준수되어야 한다. 그러나 위치정보가 단순한 개인정보가 아닌 위치정보업자가 별도로 설치한 장치에 의하여 취득되는 일종의 제작된 정보이다.[13] 또한 위치정보는 노출만으로도 사생활에 대한 직접적인 침해를 유발할 수 있다는 면에서 LBS 제공자의 침해금지를 벌칙규정이 아닌 권고규정으로 소극적으로 규정[14]하고 있는 '정보통신망법'으로는 개인위치정보의 주체가 갖는 인격권적 측면에서의 보호

13) 이상무, 「위치정보 관련 법제도 이슈와 정책 추진방향」, 『한국정보통신학회지』, 제20권 4호.

14) 정보통신망법 제45조 [정보통신망의 안전성 확보 등] ①정보통신서비스제공자는 정보통신서비스의 제공에 사용되는 정보통신망의 안정성 및 정보의 신뢰성을 확보하기 위한 보호조치를 마련하여야 한다. ②정보통신부장관은 제1항의 규정에 의한 보호조치를 구체적 내용을 정한 정보통신서비스의 정보보호에 관한 지침을 정하여 고시하고 정보통신서비스제공자에게 그 준수를 권고할 수 있다.

법익의 침해가능성이 높다.[15]

'통신비밀보호법'은 통신의 '내용'을 보호대상으로 하고 있으나, 개인의 위치정보까지 동법의 대상으로 보기에는 다소 무리가 있으며, 이를 폭넓게 해석하여 개인의 위치정보까지 규제대상으로 포함한다고 해도 개인정보의 적법한 이용에 대한 절차 및 방법이 명확히 규정되어 있지 않아 위치정보를 보호하기 위한 법적 장치로는 미흡하다 할 수 있다.[16]

현행법은 사업자들이 개인정보를 공개하거나 광고 목적으로 사용하는 것만을 금지하고 있을 뿐이며, 타인이 특정 개인에 관한 정보를 소유하고 있다는 사실만으로는 침해유형에 해당하지 않는다. 위치정보는 전파를 기지국에서 수신하면서 자동적으로 수집되는 정보라고 할 수 있으며, 전기통신망을 통한 서비스를 제공받고자 하는 자가 제공하여야 할 최소의 정보라고 볼 수 있기 때문에 수집에 있어서는 당사자의 동의를 요하지 않는 정보라 할 수 있다. 다만 이것이 공개되거나 광고목적으로 사용되기 위해서 사전동의를 필요로 한다.

최근의 상황이 위치기반서비스(LBS)가 IT산업 및 통신 서비스 시장에서 킬러 어플리케이션으로 주목받기 시작하였고, 위치정보가 가지고 있는 특수성을 고려한다면, 개인정보의 보호 수준을 높여야 할 필요성은 분명하다. 따라서 효율적인 위치정보의 활용과 보호를 위하여 위치정보의 정확도, 위험도 정도 등과 같은 위치정보 및 공공구조기관의 요청으로 인한 위치정보의 제공과 같이 공익성이 큰 경우의 LBS의 특수성을 고려한 체계적인 법률의 제정이 필요하다.

이러한 산업과 시장의 분위기에 따라 정부는 최근 개인의 위치정보를 제도적으로 보호하기 위해 '정보통신망이용촉진및정보보호에관한법률'의 개정과 '위치정보이용및보호등에관한법률(안)' 및 '민간부문개인정보보호에관한법률(가칭)'의 제정 추진을 통해 통신 환경하에서의 개인정보를 보호하기 위해 노력을 경주하고 있다.

---

15) 김도경, 전게서
16) 김도경, 전게서

2. 위치정보 규제의 최근 동향

(1) 위치정보이용및보호등에관한법률(안)

정보통신부에 의해 2003년 발의된 '위치정보이용및보호등에관한법률(안)'(이하 '위치정보보호법')은 차세대 이동통신산업 육성 및 긴급 구난구조시 활용도라는 명분에도 불구하고 사생활 침해에 대한 우려 탓에 뜨거운 논란을 야기하였다. 정통부는 이 법안이 이용자의 위치정보 보호 및 사생활 침해의 방지, 위치정보 침해에 따른 손해배상 책임제도 도입 등 주로 개인위치정보 보호의 범위, 정보이용의 법적 근거를 마련하는 데 초점을 두어 위치기반서비스(location-based service: LBS) 활성화의 순기능을 유도하고 개인정보 노출과 사생활 침해 등 개인위치정보 서비스에 따른 부작용을 방지하는 데 목적이 있다고 한다. 주무부처인 정통부와 시민단체간 갈등을 불렀던 위치확인시스템(GPS) 칩을 휴대폰에 의무 내장하는 방안은 무효화하는 대신 휴대폰 생산에서 최종 판매에 이르기까지 사업자와 가입자의 자율적인 선택에 맡기고, 이동전화사업자 등 가입자 위치정보를 직접 수집·관리하는 위치정보사업자의 경우 가입자 위치정보를 활용하기 위한 요건과 절차를 까다롭게 규정했다. 다만 유사시 긴급 구난구조의 목적으로 가입자가 119나 112 등을 통해 스스로 신고할 경우 위치정보사업자가 공공구조기관에 가입자 위치정보를 의무 제공토록 해 최소한의 구난용 범위를 규정했다.[17]

반면, 참여연대 등 시민단체들은 이 법안을 위치정보를 보호하고자 하는 법안이기보다는 위치정보 이용을 촉진하기 위한 법안으로 평가하면서, 현행 법안에 대해서 반대의견을 밝혔다. 특히, 이 법안에서 정의한 위치정보는 특정시점에서 (특정 물건 혹은) 특정인의 위치에 대한 정보로서 가장 민감한 개인정보에 해당하여, 공공 목적 혹은 상업적 목적으로 이동통신 서비스업자가 이동통신 이용자들의 위치정보를 수집하여 이용할 경우, 심각한 프라이버시 침해 문제가 발생할 수 있다고 한다. 또한, 정통부의 법안은 진흥과 규제의 상이한 목표를 제시하고 있어, 법률 제정 목적이 실현될 것인지에 대해서 의구심을 제기하였다. 즉 위치정보 이용을 촉진하는 입법 목적과 위치정보 보호의 입법 목적이 한 법률안에서 양립하기는 대단히 어려우며, 결과적으로 위치정보를 보호

17) 전자신문 사이트, http://www.etnews.co.kr/news

하기 위한 법 조항은 유명무실해질 가능성이 높다고 하며, 서면에 의한 사전 동의 등 정보주체의 권리보호 조항의 강화를 요구하였다.[18]

〈표 1〉 우리나라의 위치정보 법규제 현황

	주요 이슈
정보통신망법	- 통신서비스 가입자의 정보에 대한 보호를 명시 - 개인정보의 이용과 보호에 관한 별도의 규정을 인정하나, 위치정보의 보호에 대한 명확하고 구체적인 개념이 포함되어 있지 않음
전기통신사업법	- 통신서비스와 관련한 개인의 정보를 본인의 동의 없이 제공할 수 없음을 명시 - 현재까지는 위치와 관련한 개인의 정보보호에 가장 근접한 제도적 장치로 보임
통신비밀보호법	- 통신내용에 대한 보호가 주요 내용 - 개념의 확장과 재해석을 통해 위치정보의 보호에 적용시키려는 노력이 있으나, 절차 및 방법이 명확하지 않아 적용에는 무리가 있음.
위치정보보호법(안)	- 개인위치정보 보호의 범위, 정보이용의 법적 근거를 마련하는 데 초점을 두어 위치기반서비스(location-based service: LBS) 활성화의 순기능을 유도 - 개인정보 노출과 사생활 침해 등 개인위치정보 서비스에 따른 부작용을 방지

위치정보보호법은 다음과 같은 문제를 야기할 수 있다. 첫째, 위치정보 수집에 대한 동의의 범위 문제이다. LBS 사업자가 가입자의 동의를 구했다 하더라도, 구체적으로 어떠한 위치정보가 어떠한 목적으로 이용될 것인가가 불분명하기 때문에 구체적인 해결방안이 기술적, 법적으로 제시되어야 하며 이를 반영한 세부적인 법률안이 마련되어야 한다. 둘째, 만 14세 미만 아동의 인권문제이다. 이것은 부모의 동의만으로 아동의 위치를 부모에게 통보할 수 있게 되어 아동의 인권이 전적으로 부모의 통제하에 놓일 수 있다. 셋째, 공공부문에서의 LBS 제공 문제이다. 공공기관의 긴급 구조요청이 있을 시에는 위치정보 주체의 동의 없이도 해당 위치정보를 제공해야 하지만 개인위치정보를 보

18) 참여연대, "위치정보이용및보호등에관한법률안에 대한 참여연대 의견서," http://www.peoplepower21.org; 함께하는 시민행동, "위치추적시스템과 프라이버시 문제," *프라이버시 보호가이드라인 10원칙*, http://www.privacy.or.kr/guideline/guideline-8-e.htm.

호하려는 데 일차적인 목적이 있는 만큼 이에 대한 보다 철저한 제도적인 보안 장치가 뒷받침되어야 한다.[19]

이처럼 위치정보서비스는 다양한 방면으로 활용될 수 있고 그에 따른 인권문제를 야기할 수 있다. 따라서 정책결정자는 사회경제적 논리뿐 아니라 '정보자기결정권'이라는 원칙에 따라 헌법상의 인간의 존엄성 및 행복추구권을 고려하여 신중하게 일을 추진해야 한다.

(2) '민간부문개인정보보호에관한법률(가칭)'

주민등록번호 도용과 프라이버시 침해 등 개인정보가 위협받는 사례가 급증하고 있는 가운데 이를 보호하기 위하여, 정보통신부는 2004년 4월에 현행 '정보통신망법' 내에 포함된 개인정보 보호 관련 조항 및 하위 개별법 등을 분리해 '민간부문개인정보보호에관한법률(가칭)'로 입법화하는 작업에 본격 나섰다. '민간부문개인정보보호에관한법률'의 입법화는 정통부가 2003년 '정보통신망법' 시행령 개정을 통해 개인정보 보호 관련 규제대상을 일정 규모 이상 쇼핑몰사업자까지 확대하는 등 규정을 강화했으나 체계적인 개인정보 보호에는 여전히 한계가 있다고 판단했기 때문이다. 현재 공공부문에 대해서는 '공공기관의개인정보보호에관한법률'을 별도로 두고 있다.

별도 입법화 작업이 현실화될 경우 민간기업이나 타인의 개인정보 수집 및 관리 등에 대한 법규정 마련도 뒤따를 것으로 기대된다. 이에 따라 그동안 명목상으로만 존재했던 개인정보 보호규정이 크게 강화되어 'IT강국'을 내세우면서도 상대적으로 소홀히 취급됐던 개인정보 보호 수준이 한 단계 업그레이드되는 계기가 될 것으로 보인다.

특히 현재 '정보통신망법'에 명시된 기업의 개인정보관리책임자 지정이 의무화될 것인지에 대해서도 관심이 모아지고 있다. 이미 독일 등 유럽에서는 개인정보보호법률의 준수 여부를 감독하는 개인정보보호관(DPO) 임명을 의무화해 시행중이다. 이와 함께 일반기업이 특정 데이터를 수집·관리할 때 미리 개인정보 무단 침해 등을 방지할 수 있는 예방 장치도 마련될 수 있을지 주목된다. 그동안 개인정보 보호 관련 업무는 정통부 외에 산자부, 공정거래위원회, 소비자보호원 등 여러 기관으로 분산돼 있었다. 따라

19) 김도경, 전게서

서 별도 입법은 추진과정에서 정통부와 다른 기관과의 조율이 관건으로 부각되고 있다. 또한 정부혁신지방분권위원회가 공공 및 민간 영역 개인정보 보호 법률의 상위법 개념으로 추진중인 '개인정보보호기본법(가칭)'과도 효율적인 연계가 요구되고 있다.[20]

3. 현행 법제의 한계

현행법의 한계를 논의함에 있어서 위치정보서비스(LBS)는 '정보통신망이용촉진및정보보호등에관한법률' 제2조 제1항 제6호의 "개인정보"의 일종에 해당하는가가 가장 핵심적인 문제이다.

"개인정보"란 앞서 살펴본 바와 같이 "생존하는 개인에 관한 정보로서 성명·주민등록번호 등에 의하여 당해 개인을 알아볼 수 있는 부호·문자·음성·음향 및 영상 등의 정보(당해 정보만으로는 특정 개인을 알아볼 수 없는 경우에도 다른 정보와 용이하게 결합하여 알아볼 수 있는 것을 포함한다)"라고 규정되어 있는바, 위치정보는 당해 정보만으로는 특정 개인을 알아볼 수 없는 경우가 많겠으나 발신자 정보 등과 결합할 경우 발신자 표시 등으로 특정된 개인이 현재 존재하는 곳의 위치와 그 위치를 통한 개인의 행동 등을 추정할 수 있는 정보이므로 위 규정에 부합하는 개인정보의 일종이라고 할 수 있다.

다음 위치정보를 개인의 동의 없이 수집할 수 있는지 여부에 관하여 위에서 본 '정보통신망이용촉진및정보보호등에관한법률'의 각 규정을 보면, "개인정보는 ① 법률에 규정이 있는 경우 ② 요금정산을 위하여 필요한 경우 ③ 정보통신 이용계약의 이행을 위하여 필요한 경우 각 동의 없이 수집될 수 있다"고 되어 있다.

위치정보는 기본적으로 전기통신망을 이용하는 자가 송출하는 전파를 기지국에서 수신하면서 자동적으로 수집되는 정보라고 할 수 있으며, 따라서 전기통신망을 통한 서비스를 제공받고자 하는 자가 제공하여야 할 최소 필요한 정보라고 볼 수 있다. 그렇다면, 위치정보는 위 각 예외조항의 "정보통신의 이용계약의 이행을 위하여 필요한 최소정보"라고 볼 수 있으며, 따라서 수집에 있어서는 당사자의 동의를 요하지 않는 정보라 할

20) 전자신문 사이트, http://www.etnews.co.kr/news

것이다.

나아가 위치정보의 이용 및 제공의 제한에 관하여 살펴보면, 원칙적으로는 위치정보도 개인정보의 일종이므로, 위 법이 규정한 제한을 따라야 한다. 따라서 정보통신서비스의 제공에 따른 요금정산을 위하여 필요한 경우와 통계작성·학술연구 또는 시장조사를 위하여 필요한 경우 특정 개인을 식별할 수 없는 형태로 제공하는 경우에는 당사자의 동의 없이 이용 또는 제공할 수 있을 것이다.

그런데 위 각 법은 다른 법률에 규정이 있는 경우 개인정보를 제공할 수 있다고 하고 있고, 현행 전기통신사업법 제54조의2는 송신인의 전화번호의 고지 등에 관하여 "① 전기통신사업자는 수신인의 요구가 있는 경우에는 정보통신부령이 정하는 바에 의하여 송신인의 전화번호 등을 알려줄 수 있다. 다만, 송신인이 전화번호 등의 송출을 거부하는 의사표시를 하는 경우에는 그러하지 아니하다. ② 전기통신사업자는 제1항 단서의 규정에 불구하고 전기통신에 의한 폭언·협박·희롱 등으로부터 수신인을 보호하기 위하여 정보통신부령이 정하는 바에 의하여 수신인이 요구를 하는 경우와 특수번호 전화서비스 중 정보통신부령이 정하는 경우에는 송신인의 전화번호 등을 수신인에게 알려줄 수 있다" 라고 규정하고 있는바, 그렇다면 위치정보가 "전화번호 등"에 해당되는 정보인지를 판명할 필요가 있다고 본다.

생각건대, 위치정보서비스와 송신인의 발신번호에 관한 정보 서비스는 모두 개인정보의 일종이기는 하지만, 달리 취급되어야 할 필요가 있다. 첫째, 송신인의 발신번호는 수신인이 송신인과의 대화를 통하여 바로 송신인 개인에 대한 식별identify이 가능하므로 미리 그 번호를 알려주더라도 수신인의 대화거부를 제외하고는 다른 문제점이 생기기 어렵고, 둘째, 수신인이 송신 당시 수신을 하지 못하더라도 송신인의 발신번호를 수신인에게 남겨둠으로써 수신인이 송신인의 동일성을 인식할 수 있기는 하지만 원래 송신인이 수신인과의 대화를 원하여 송신한 것이므로 역시 별문제가 없는 것으로 보인다. 하지만, 위치정보는 송신인 개인의 동일성에 대한 식별을 넘어서서 송신인의 현재 상태를 알려주는 중요한 정보가 될 수 있으며, 송신인의 알려주고 싶지 않은 정보를 알려줄 위험이 있다. 예를 들면, 송신인의 사무실에서 전화가 온다면 송신인이 현재 일을 하고 있음을 추측할 수 있고, 위치정보가 계속적으로 변하면 송신인이 현재 이동하고 있음을 추측할 수 있게 된다. 따라서, 위 전기통신사업법에 의하여 송신인의 위치를 "송신인이 거부하지 않는

한" 알려주도록 한다면, 이는 심각한 사생활의 침해를 야기할 수 있다고 보여진다.

따라서 원칙적으로 위치정보는 두 가지의 예외사유에 한하여 당사자의 동의 없이 위 목적에 한정하여 알려줄 수 있다고 하여야 하겠다. 첫째, 예외 사유는 위험한 상황에서의 정보의 제공이다. 예컨대, 급박한 화재현장 또는 범죄현장에서 119 또는 112 신고를 한 사람이 정확한 위치를 알려주지 못하는 경우 소방관서 또는 경찰관서 등에서 위치정보를 이용할 수 있는가 하는 문제가 있다. 이는 비록 법률의 규정이 없다고 하더라도, 정보를 이용당한 자의 명시적 혹은 추정적 승낙, 또는 긴급피난 등의 이유로 정당화될 수 있을 것으로 보인다. 둘째, 범죄자의 추적에 이용될 수 있는지에 관하여는 수사기법의 하나로 범죄자의 현재 위치를 파악하는 데 위치정보가 당사자의 동의 없이 이용될 수 있는지 또한 문제가 된다. 비록 수사기관이 추적중인 범죄자라고 하더라도 확정판결이 있기 전까지는 무죄추정의 원칙이 적용되어 일반인과 같은 신분이라는 점, 범죄자로 추정되는 자의 수사단서를 잡기 위한 전자통신의 녹취, 감청 등에도 법관의 영장을 요하는 등 영장주의가 관철되고 있다는 점을 본다면, 위치정보의 경우에도 법관의 영장을 통하여 이용될 수 있지 않을까 한다.

위치정보는 발신번호와 같이 당사자가 정보의 제공을 동의하였다고 하더라도 앞에서 본 바와 같이 개인의 현재 상황을 암시하는 기능까지 제공하고 있으므로, 특별히 정보제공자가 일반인에게 자신의 정보를 모두 제공하겠다는 특약을 하지 않는 한 정보 수신자를 제한적으로 제공할 필요성이 있지 않은가 한다. 위치정보는 개인의 동일성을 식별하는 정보의 기능도 하면서 동시에 개인의 현재 상황을 알려주는 정보의 역할도 한다고 할 수 있다. 따라서 위치정보는 "정보제공자가 원하는 때에 원하는 사람에게 한하여" 제공될 필요성이 있으며, 그렇게 제한되지 않으면 프라이버시에 대한 심각한 침해가 발생할 수 있을 것으로 보인다. 따라서 현행 법령으로는 정보통신망이용촉진및정보보호등에관한법률에 의한 예외조항을 제외하고는 타인의 이용을 엄격하게 제한하여야 할 것으로 보이며, 달리 특수한 이용-특히 범죄수사 목적의 이용- 등에는 영장주의에 관한 필요한 사항 등을 모두 입법화할 필요가 있다.

Ⅳ. 외국의 위치정보 규제

1. 미국

(1) 위치정보 보호의 헌법적 근거

1) 개관

미국 헌법에는 프라이버시에 대한 권리가 명확히 기술되어 있지는 않다. 미국 대법원은 프라이버시에 대한 권리는 권리장전의 수 개의 규정들에 기반을 둔 제한적인 헌법상의 권리라고 제시했다.

미국은 민간부문에서 프라이버시에 대한 포괄적인 보호법을 가지고 있지 않다. 1974년의 프라이버시에 대한 입법의 대상은 미 정부 기관들에 의해 보유한 기록들을 보호하고 그 기관들로 하여금 기본적인 정당한 정보의 활용을 요구하는 데 국한된 것이었다. 또한 미국에는 프라이버시 침해를 감시하는 기관이 없다. 예산처(The Office of Management and Budget: OMB)에서는 연방 기관들에 대한 제한적인 규제만을 시행하고 있다. 연방거래위원회(FTC)는 소비자들의 신용정보와 거래활동을 감시하고 보호하는 기능을 하고 있으나 불공정 관행 이외의 일반적인 프라이버시의 권리를 보장하는 역할은 수행할 수 없다.

현행 연방 법규의 어떤 조항도 개인적인 정보의 일반적 이용을 금지하고 있지는 않다. 다만 다양한 개별법규가 주정부 차원에서 특별한 범주-재정 기록, 신용 기록, 비디오 대여 기록, 학교 기록, 전화 기록, 자동차 등록 기록, 의료 기록-를 민간이 사용하는 것을 금지하고 있을 뿐이다. 다만 다양한 입법들이 주정부 차원에서 부가되고 있다.

이러한 포괄 입법의 부재는 프라이버시 침해의 빈도를 증가시키고 있다. 전자 감시 수단을 이용한 사례는 1990년을 기준으로 10년간 세 배 이상 증가하였다. 정보기관들은 인터넷 통신들의 감시에 대한 투자에 주력하고 있다.

2) 헌법상 프라이버시 권리right to privacy

프라이버시라는 용어가 최초로 논의되기 시작한 것은 워렌(Samuel D. Warren) 판사와 브랜다이스(Louis D. Brandeis) 판사가 1890년에 발표한 「프라이버시 권리The Right of Privacy」라는 논문에서부터이다. 그들은 프라이버시를 '홀로 있을 권리right to be let alone'라

고 정의를 내리면서 당시 사회환경의 변화에 따라 이와 같은 새로운 유형의 권리를 인식할 필요성을 강조하였다. 그 후 1960년 프로서Prosser는 불법행위 측면에서 '사생활에의 침입intrusion upon seclusion', '사생활의 공표public disclosure of private facts', '상업적 이용appropriation for commercial gain'으로 프라이버시 침해 유형을 분류하였다. 1960년대 말에 이르러서는 정보화 사회가 진전됨에 따라 프라이버시의 개념이 이전의 비밀스러운 사생활을 보호하기 위한 개인적인 이슈에서 벗어나 사회적인 가치로 부상하게 되었다. 특히 컴퓨터의 발전과 관련하여 개인정보에 관한 보호문제가 부각되게 되었고 이것이 점차 중요성을 차지하게 된 결과 오늘날에 와서는 이 부문과 관련된 프라이버시 문제를 별도로 정보 프라이버시Information Privacy 또는 데이터 프라이버시Data Privacy라고 일컫게 되었다. 미국에서는 이러한 이론을 입법화하여 1974년 세계 최초로 프라이버시 법Privacy Act을 제정하였다.

3) 수정헌법 제4조와 통신의 자유

통신의 자유는 미국 헌법에서 영장주의에 의한 보호를 받는다. 즉 수정 헌법 제4조는 부적법한 압수, 수색을 금지하는 조항을 두고 있으며, 통신의 자유를 침해하는 행위, 즉 도청은 이러한 수정헌법상의 보호를 침해하는 것으로 해석하고 있다.[21]

다만 위치정보 제공은 통신의 자유의 중핵을 이루는 통화 내용과는 근본적으로 차이가 있다. 즉 도청을 제한하는 일반 입법의 논리가 위치정보 제공에 그대로 제공될 수는 없다는 것이다. 먼저 도청 장치와 위치확인 장치는 기술적 차이가 있다. 또한 도청 장치에서 얻게 되는 정보의 타입과 양은 단순한 위치확인과는 근본적인 차이가 존재한다.

(2) 연방통신위원회(FCC)에 제출된 '공정한 위치정보 수행방법 확립을 위한 이동통신산업협회(Cellular Telecommunications Industry Association)의 규칙제정청원서'

1) 청원의 배경

모든 위치기반 응용서비스는 많은 소비자 이익을 약속하는 반면, 법적으로 인정되는

21) "The right of the people……against unreasonable searches and seizures shall not be violated……."

프라이버시legitimate privacy는 "사용자의 위치추적을 서비스제공자에게 허락하고, 여행 또는 개인의 상품 판매에 관한 광고를 그들에게 보내는 위치기반 애플리케이션"의 위험성을 내포하게 된다. 이에 대응하여 연방통신위원회(Federal Communications Commission: FCC)뿐만 아니라 연방거래위원회(Federal Trade Committee: FTC)가 새로운 무선기술과 프라이버시, 보안, 그리고 소비자 보호 이슈에 관한 관련 아젠다를 소화하는 규제를 제공하여야 한다. 이에 이동통신산업협회(Cellular Telecommunications Industry Association, CTIA)는 위치정보원칙을 채택하기 위하여 FCC에 연방통신법을 실행하기 위한 규칙제정을 요청하였다.[22]

즉 CTIA는 FCC가 무선통신 고객mobile customers이 ① 수집에 "앞서" 위치정보 수집과 사용 절차를 잘 알려주고, ② 위치기반서비스를 위해 이러한 정보의 사용과 수집에 동의하기 위한 진지한 기회를 주며, ③ 모든 수집된 위치정보의 보안과 무흠결을 확신할 수 있도록 보증할 수 있는 규칙을 공포할 것을 요청하였다. 이 규칙은 이 프라이버시 원칙을 요구하는 모든 위치정보서비스 제공자를 위해 '안전항安全港; safe harbor'을 제공해야 한다. 또한 무선통신 고객의 프라이버시 보장에 대한 기대가 무선통신 장치mobile device의 유형이나 그것이 사용되는 로밍roaming시장에 관계없이 충족될 수 있도록 규칙은 기술 중립적이어야 한다는 것을 명시하고 있다.

2) 무선통신과공공안전법률(Wireless Communications and Public Safety Act: WCPSA)과 고객 소유 네트워크 정보(Customer Proprietary Network Information: CPNI)

1999년의 무선통신과공공안전법률(WCPSA)의 일부로서, 의회는 위치정보가 고객 소유 네트워크 정보(customer proprietary network information: CPNI)에 속하는 것으로서, 1996년 연방통신법하에서 일정한 제한의 대상으로 간주했다. WCPSA 아래에서는 상업용 이동전화 서비스 또는 자동응급통지 시스템의 사용자들은 "명시적 사전 동의 없이" 통화위치정보의 사용 또는 누설 또는 접속 허락에 동의했다고 간주될 수 없다. 따라서 '명시적 동의' 규정에 의하여 통신사업자는 고객의 명확한 서면 요구에 의거하여 그 고객이 지명한 사람에게는 위치정보를 알려주어야disclose 한다. 반대 해석을 하면, 통신사업자는 고객의 동의가 없는 경우 오직 개인 또는 고객 신원과 특성이 삭제된 위치정보

22) Michael F. Altschul, *The CTIA location information privacy petition*, 2001.5, p.2.

를 포함하는 고객 정보만을 사용, 또는 공개할 수도 있다.

이에 대하여 2000년 8월 24일, FCC는 WCPSA의 공공 안전 측면을 보완하기 위한 규정을 제정하면서 CPNI 명세서docket에 위치정보를 포함시킬 것인지에 관하여는 유보적 입장을 견지하였다.[23]

CTIA는 FCC에 대하여 위치정보를 다른 CPNI 이슈와 독립하여 다루어 줄 것을 일관되게 요청하였다. 왜냐하면 위치 프라이버시 문제는 특별히 무선과 긴밀히 연관되어 있으므로 일반적 통신과 구별하여 취급되어야 한다고 여겼기 때문이다. 이것은 공공 이익의 문제이자 위치서비스 제공자들과 그러한 서비스를 이용하는 소비자들의 이익의 문제이기에 가능한 빨리 프라이버시 규칙이 제정되어야 한다고 촉구하였다. CTIA가 제안한 위치 프라이버시 원리는 절차의 공정성과 적법성에 기초한다. 여기서 적법/공정성은 통지notice, 동의consent, 보안과 보전security and integrity, 그리고 기술 중립의 요소들로 구성된다.[24]

(3) 1994년의 '사법절차에 있어서의 통신협력법'(CALEA: Communications Assistance for Legal Enforcement Act)

클린턴 행정부가 추진한 '사법절차에 있어서의 통신협력법(CALEA)'은 기술적인 발달에 대응하는 제안이었다. 당시 FBI 국장이었던 Freeh가 제시한 세 가지 원칙은 일단 법이 지향하는 목표를 분명히 하였다. 첫째, 민간 부문이 사법절차에 협력하는 것은 공공 책임을 분담하는 것이며 이를 위하여 표준 설정을 확립할 필요성을 인정한다. 둘째, 이에 따른 보다 강력한 프라이버시 보호 의제를 구체화한다. 셋째, 사법절차에서의 협력이 새로운 통신서비스와 기술의 혁신을 저해하여서는 안 된다.

---

23) 1996년 5월 17일에, FCC는 고객 소유 네트워크 정보(CPNI) 보호에 관한 통신 법률의 제222조항에서 통신사업자의 의무에 대해서 규칙을 검토하기 시작하였다. FCC는 1998년 2월 26일에 CPNI 명령(order)을 발표했다. 이에 대하여 통신사업자는 CPNI 제한이 수정 헌법 제1조를 위반한다는 이유로 그것에 반대했다. 결국, 연방 법원은 위 명령이 위헌이라고 판단하여 FCC에 패소 판결을 안겨주었다. FCC는 현재까지 이에 관한 후속 조치를 아직 취하고 있지 않다.

24) CTIA가 제안한 위치 프라이버시 원칙은 이 논문의 제5장 1절 '위치정보보호의 원칙'에서 자세히 소개된다.

CALEA의 핵심 내용은 전자 감시electronic surveillance 체제의 확립을 위하여 사법기관(LEA: Law Enforcement Agency)으로 하여금 통신사업자(TSP: Telecommunication Service Provider)에 대하여 일정한 장비 설치를 의무화하는 권한을 부여하는 것이다. 그 대상이 되는 중요 정보 중 하나는 '발신자 식별caller-identification' 정보이다.

다만 프라이버시 보호 원칙은 이러한 정보를 제한적으로 사용할 것을 요구한다. 따라서 합리적으로 이용 가능한 범위 내에서 이용할 수 있도록 제한하고 있다. 그 범위에 관한 구체적 기준은 연방통신위원회(FCC)와 법원의 해석에 달려 있다. 또한 CALEA는 구체적으로 어떤 표준이 적용될지에 관하여는 사업자들에게 그 기준을 제시하도록 유보하였다. 따라서 사업자단체 또는 별도의 표준제정 기관들은 공개적으로 이용가능한 표준을 제정할 수 있도록 규정하였다. 다만 사업자단체에서 정하여진 표준에 관하여 FCC의 승인을 받도록 하여, 만일 공적 기준에 미달하는 경우에는 FCC는 새로운 표준을 제정하도록 요청할 수 있다. 결국 CALEA의 제정으로 공공 목적을 위한 민간의 협력 의무가 규정되었는데, 그 범위를 어디까지로 한정할 것인가 하는 문제가 남게 되었다.

(4) 개인위치정보보호법안(Location Privacy Protection Act of 2001)

2001년 7월 의회 통상위원회에 제출되어 상정중인 '개인위치정보보호법안(Location Privacy Protection Act of 2001)'은 본격적인 위치기반서비스에서의 위치정보의 보호를 규정하고 있다. 위치정보의 수집 및 활용에 관한 개인의 위치정보에 대한 정보주권을 폭넓게 보장할 수 있도록 하기 위하여 이용자의 사전 동의와 위치정보수집자의 사전 고지의무를 규정하고 최소한의 원칙에 따라 동의된 목적 이외의 사용을 금지하였다.

WCPSA에서 규정하고 있는 응급구난의 경우도 고객에 대한 통지와 동의를 필요로 하지 않는 예외에 포함되어 있다. 위치정보가 응급구난의 경우에 효과적으로 활동될 수 있다는 점을 고려한 예외적 내용을 제외하고는 일반적인 개인정보 보호와 다를 것이 없으며, 위치정보를 기존의 법체계에서 보호하고 있는 개인정보의 범주에 포함시켜서 개인정보 보호 원칙을 적용하고 명확한 제도 내에서 위치기반서비스가 이루어지도록 한다는 점에서 그 의의가 있다.[25)]

(5) 위치정보의 개별적 규율

1) 표준 제정 : IS-J-STD-025

1995년, 통신사업자 협회(TIA: Telecommunications Industry Association)는 CALEA에서 요청하는 산업계 표준을 마련하기 시작하였다. 그 내용은 앞서 살펴본 바와 같이 사법기관이 통화자 식별 정보에 접근할 수 있도록 하는 설비의 표준에 관한 것이다. 위 표준의 정식 명칭은 '적법한 전자감시를 위한 임시 표준(Interim Standard: Lawfully Authorized Electronic Surveillance Standard)'이다.

이에 대하여 미 법무부(DOJ)와 FBI는 그 대상에 포함되기를 희망하는 목록punch list을 별도로 작성하여 공표하였다. FCC는 1998년 이해관계인들의 의견을 수렴하여 표준에 관하여 입법예고(NPRM: Notice of Proposed Rulemaking)하였다.

2) FCC Report No. ET(the office of Engineering and Technology) 99-4;
No. WT(Wireless Telecommunications bureau) 99-24

1999년 FCC는 CALEA를 구체화하는 최종 규칙을 공표하였다. 이는 사법절차에 협력하여야 하는 통신사업자의 협력 범위를 결정하는 것이었다. 여기에서는 TIA가 제시한 J-STD-025 표준이 공식적으로 채택되었다. 이로써 공공기관은 자신의 전자 감시의 목적을 민간의 협력을 얻어 달성할 수 있게 되었고, 사업자들로서는 최소의 비용으로 최적의 장비를 통하여 위와 같은 의무를 달성할 수 있게 되었다.

법무부와 FBI의 제안은 9개 중 6개만이 채택되었다. 채택된 내용은 다음과 같다. i)구체적인 목적이 제시된 전화 회의의 내용, ii)전화 회의에 참가한 당사자, iii)구체적인 목적이 제시된 전화의 번호 및 신호 정보, iv)대역내 및 대역외 신호, v)시간 정보, vi)통화 중 사용 번호 등인데, 이 중 접속 후 사용 번호는 후의 판결에 의하여 무효화되었다.

3) 무선통신및공공안전법(WCPSA: Wireless Communications and Public Safety Act of 1999)

미 의회는, 무선통신및공공안전법(WCPSA)에 의하여 위치정보는 고객 소유 네트워크 정보(CPNI: Customer Proprietary Network Information)에 해당되지만, 일반적 사용이 제한되는 예외 규정이 적용된다고 선언하였다. 따라서 명시적 승낙 없이는 통화위치정보

25) 오태원, 「개인위치정보의 법적 문제와 위치기반서비스의 전망」, 『정보통신정책』, 제14권 6호, 2002.4.

의 사용 또는 공개가 금지된다.

4) FCC 99-245(Wireless E911 Rules)

FCC는 1999.9. 위치기준 관련 규정에서 무선 E911 규칙을 제정하였다. 그 주요 내용은 무선망사업자wireless carriers에 대하여 공공안전기관(PSAP: Public Safety Answering Point)의 요청에 따라 자동위치확인(ALI: Automatic Location Identification)이 가능한 무선단말기의 제조를 의무화하도록 규정한 것이다. 이러한 법적 강제는 산업계에 큰 부담을 주는 것이지만, 법제의 진화 과정에서 이른바 아이디어나 인센티브를 제공하는 단계에서 벗어나 실제로 시장 참여자들의 권리, 의무를 규정definition하고 집행enforcement하는 단계로 이행하였음을 보여주고 있다.[26]

5) 1968년 범죄통제법Omnibus Safe Streets and Crime Control Act

미국의 연방 대법원은 선판례에서 도청 장치는 수정헌법 제4조의 압수, 수색의 영역에 드는 것이 아니라고 판시하였다.[27] 이는 실제로 피해자의 물리적 영역을 침해하는 일이 없었다는 해석으로 종래의 '영역침해원칙rule of trespass premise'을 관철한 결과였다. 그러나 Katz v. U.S. 판결에서 이러한 해석이 번복되었다.[28] 이 사건에서는 피고인이 전화를 이용하여 도박 조직을 운영하는 것에 대하여, FBI 요원이 공중전화실 밖에서 전자수신기록장치를 접속하여 도청한 증거를 수정헌법 제4조 위반으로 증거로 사용될 수 없다고 판시하였다. 종래 압수·수색은 대상이 사적 영역에 있었느냐, 공적 영역에 있었느냐를 주로 보고 판단하였었다. 그러나 본 사건에서는 개인의 합리적 기대를 기준으로 물리적 영역 이론을 보다 확장하는 헌법 해석을 하였다.

위 판결의 영향에 의하여 1968년 범죄통제법(Crime Control Act of 1968)에서는 도청에 관한 몇 가지 원칙들을 입법화한다. 이는 요건을 준수한 도청은 합법적, 합헌적임을 뜻한다. 우선 사인私人에 의한 도청은 원칙적으로 전면 금지된다. 도청은 기본적으로 범죄 수사 등 사법적 목적 달성을 위하여 허용된다. 그러나 이러한 입법은 한편으로는 통신의 자유도 일정한 입법 목적을 위하여 합리적으로 제한될 수 있음을 의미한다.

---

26) Michael J. O'Neil, James X. Dempsey, "Threats to Privacy and Other Civil Liberties and Concerns with Government Mandates on Industry," 12 DePaul Bus. L.J. 97, p.6.

27) 문홍주, 『기본적인권연구』, 해암사, 1994, p.372.

28) 389 U.S. 347(1967)

6) 1986년 전자통신프라이버시법(Electronic Communication Privacy Act: ECPA)

1986년 전자통신프라이버시법(ECPA)에서는 도청 장치로부터 보호를 받는 대상을 확장하였다. 즉 전자메일, 휴대전화, 정보, 음성 또는 비디오의 컴퓨터 전달 및 페이징 장치로 보호의 범위를 확장했다. 다만 사법기관에 의한 요청권한은 이러한 새로운 매체에 대하여는 더 이상 허용하지 않았다. 이를 가리켜 입법이 아직 신기술을 추월하는 것을 허용하지 않았다고 평가하기도 한다. 따라서 사법기관은 이러한 새로운 통신사업자에 대하여는 도청을 용이하게 하기 위한 시스템 구축 등을 적극적으로 요구할 법적 권한을 갖지는 못하였다.

또한 전화이용에 관한 일반 기록에 대하여는 도청보다는 훨씬 완화된 기준을 제시하였다. 즉 영장 발부의 사유가 일반 기록을 획득하기 위한 장치를 설치함으로써 범죄 수사에 관련된 정보를 얻을 수 있는 경우 이를 허용하였다. 이는 종래 도청에서 적용된 긴급한 상황에 비하여는 영장발부가 용이한 요건이다.

7) 컴퓨터 범죄방지법(Computer Fraud and Abuse Act of 1986)

이 법은 과거 전통적인 절도 또는 재산권 남용의 법적 접근 방식을 탈피하여 컴퓨터 자료에 관하여 사용허락을 얻지 않은 사용자에 의하여 복제되는 경우도 절도에 포함시킴으로써 정보 프라이버시를 하나의 재산권으로 파악하고 있다.

8) 외국정보감시법(Foreign Intelligence Surveillance Act)

전자감시 체제의 역외 적용을 규율하기 위한 법규도 제정되었다. 이는 개인정보의 흐름이 역내의 제한을 넘어서 전세계적으로 이루어지고 있는 현실을 규율하기 위한 필요성에서 입법되었다.

9) E-911 집행법(E-911 Implementation Act of 2003)

E-911 집행법은 국립통신정보청(NTIA: National Telecommunications and Information Agency)에 연간 1억 달러의 지원을 승인하여 비상시 통신서비스 개선을 시행하도록 한 법이다. 이 법은 또한 이러한 지원금을 관리·감독하고 비상 통신서비스의 조정·협력 방안을 개선하도록 NTIA 내에 E-911 이행법안 조정사무국(E-911 Implementation Coordination Office)을 설치하도록 명시한다. 본 법을 통하여 구체화되는 긴급 구조서비스의 제공 구조는 다음과 같다.

연방통신위원회는 공공 안전 응답 지점(Public Safety Answering Points-PSAPs)에 비

상 911 호출위 위치정보를 제공하도록 한 요구사항들을 채택하게 되었다. 이런 요구사항은 크게 두 단계로 나눠진다. 제1단계는, 1998년 4월 1일에 효력이 생긴 것으로, 무선통신사업자들이 911 호출을 한 핸드폰 번호 및 호출을 받았던 통신 셀cell과 기지국의 물리적 위치를 PSAP로 제공하도록 하였다. 제2단계는 무선통신사업자들이 자동위치정보(Automatic Location Information-ALI)로 알려진 정확한 위도와 경도를 PSAP로 통지할 것을 요구한다.

통신위원회는 무선 E-911 관련 추가적인 행동을 취하였다. 주요 내용을 요약하면 다음과 같다. 첫째, 2001년 10월 2일에, 위원회는 PSAP에 제2단계 E-911 정보를 제공할 무선통신사업자들의 의무사항을 규정한 유효 PSAP 요구사항을 명시하였다. 둘째, 2002년 4월 29일에, 위원회는 무선전화들에 각종 요구사항을 부과하였는데, 이러한 요구사항은 이동전화 서비스에 가입하지 않은 이동전화로 911에 전화를 건 호출자를 다시 호출하고자 하는 것이다. 셋째, 2002년 6월 28일에, 위원회는 모든 디지털 무선서비스 사업자들이 문자 전화 기기를 사용하여 911 호출을 전송할 수 있도록 요구하는 2002년 6월 30일 마감기한을 포기 또는 연장하도록 한 규칙을 발표하였다. 넷째, 2002년 7월 24일에, 위원회는 911 선택식 라우터가 무선사업자와 PSAP 사이의 E911 설치비용을 할당을 위한 결정 단위가 되어야 한다는 무선국Wireless Bureau의 2001년 5월 결정을 승인하였다. 다섯째, 2002년 7월 26일에, 위원회는 두 계층의 비전국적인 CMRS(Commercial Mobile Radio Service) 사업자들을 위해 제2단계 이행의 마감기한의 일시적 연기를 부과하였다.

아울러 위원회는 무선 E911 의무사항과 관련한 시행 수단을 취하였다. 2002년 5월 2일에, 위원회는 각종 기술적 방식에 의한 네트워크 시스템 구축에 대한 법적 근거를 재확인하였다. 또한, 2002년 5월 20일, 위원회는 GSM(Global Standard for Mobile Communications) 네트워크에 관한 E911 의무사항의 AT&T Wireless의 준수 여부를 조사한 후에 NALF(Notice of Apparent Liability for Forfeiture)를 제안하였다.

10) 무선통신 사생활 보호법(Wireless Privacy Protection Act of 2003)

이 법은 크게 ① 무선호출 위치정보에 대한 사용자의 동의, ② 무선 위치 사용 및 정보 폐기에 대한 허가로 나눌 수 있다.

연방통신위원회의 911법은 2003년까지 관할 지역 정보를 제공할 수 있는 업체를 요구하고 있고, 2005년 12월 31일까지 지역에서 완벽하게 무선정보시스템을 이행할 것을

규정하고 있다. 비록 핸드폰 제조업자들이 벌써 청구서를 발행할 목적과 급변하는 핸드폰기기들을 사정할 목적으로 핸드폰 위치추적 정보를 찾고 있지만, 이러한 911의 요청은 좀더 세부적인 위치정보를 요구하고 응급서비스 제조업자들에게 연속적인 정보 공개를 요구하고 있다. 그러한 향상된 핸드폰 위치추적 정보기술은 확실히 부가이익을 주기로 약속했다. 이러한 위치추적 정보의 가능성은 상당한 대중안전을 제공하지만 그 정보는 또한 미숙한 정부의 감시와 오용의 기회를 낳기도 한다.

핸드폰 위치추적으로부터 사생활이 얼마나 보호되는가에 대한 이슈, 사생활 보호가 헌법적 권리인가에 대한 이슈, 그리고 정부가 억제되지 않는 법집행 감시로부터 핸드폰 사용자들을 보호할 수 있는 법적 근거가 존재하는지에 대한 이슈는 핸드폰 위치추적에 의한 사생활과 연관된 권리를 다시 한번 생각하게 한다.

헌법적 보호가 전화기록과 호출기의 사용을 감시하는 것은 전자적 감시와는 다르다는 전통적 견해하에서는 핸드폰 관련 사생활 보호에 관한 헌법적 권리를 명시적으로 도출하기는 쉽지 않다. 위치추적 사생활의 권리를 결정하는 데 있어, 법원은 이러한 전례에 의존하는 것 같으며, 대부분의 사건에서 대법원과 하부법원들은 아직까지는 정부의 편에 서 있었다고 볼 수 있다. 무선통신 사생활 보호법은 이러한 법의 해석의 공백과 흠결을 입법으로 보충하려는 노력이고 모색의 결과이다.

2. 유럽

프라이버시의 권리에 대한 관심은 IT(Information Technology) 산업의 발전과 더불어 증가하기 시작하였다. 감시 가능한 거대한 컴퓨터 시스템들은 수집한 정보들의 관리와 개인적인 정보들을 관리하는 데 있어서 특별한 법규들을 필요로 하였다. 이런 근대적 입법의 발생은 1970년의 독일에서 제정된 정보보호법으로 거슬러 올라간다. 뒤이어 스웨덴의 1973년 법규, 프랑스의 1978년 법규가 제정되었다. 유럽 연합 차원에서는 1981년의 '개인정보 자동처리에 있어서의 보호 협약Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data'과 OECD의 '프라이버시 보호 및 개인정보의 유통 가이드라인Guidelines Governing the Protection of Privacy and Transborder Data'이 중요한 규범으로 등장하였다. 여기에서 개인정보에 대하여 합의된 원칙의 내용은 다음과 같다.

- 정보의 공정하고 적법한 보유
- 정보사용에 있어서 본래의 특정한 목적에 사용될 것
- 적절하고 관련성이 있으며 목적을 넘어 사용되지 않을 것
- 정확하며 시간에 따라 갱신될 것
- 당면 과제를 해결하는 데 유익할 것
- 보안 유지가 될 것
- 목적이 달성된 후에는 정보를 없앨 것

이러한 두 협약은 전세계의 법규들의 시행에 많은 영향을 주었다. 1981년 협약에는 대부분의 유럽 국가들이 인준하였고, OECD 지침은 OECD 국가와 심지어는 비회원국에까지 국제적인 법규로 실질적으로 적용되고 있다.

1) 포괄적 입법Comprehensive Laws

프라이버시와 데이터 보호법의 체계 중 위와 같은 협약은 이른바 포괄적 규정의 형식을 띠고 있다. 즉 개별 사안에서의 보호뿐 아니라 일반적으로 적용될 수 있는 원칙들을 선언하고 프라이버시 권한을 가능한 한 넓게 보호하고자 하는 체제이다. 이러한 포괄적 입법을 채택하는 이유는 다음과 같다.

첫째는 과거의 불합리성을 교정하기 위해서이다. 많은 국가들은 대표적으로 동유럽에서는 이러한 포괄적 입법을 통하여 이전의 독재정권하에서 발생하였던 프라이버시에 대한 위배를 교정하는 것을 목적으로 한다.

둘째는 전자거래를 증진시키기 위함이다. 많은 국가들에서 전자거래를 발전, 증진시키기 위하여 포괄적 입법 형식을 취하고 있다. 이런 국가들은 소비자들이 개인적인 정보가 공개되는 것을 꺼려한다는 사실을 인식하고 있다. 따라서 프라이버시에 관한 법들은 통일된 법규를 형성함으로써 전자거래를 용이하게 하기 위함을 목적으로 하는 법규들의 일부로서 전개되고 있다.

셋째는 프라이버시 법규의 제정도 다른 분야에서의 범유럽 차원의 법규를 제정하는 경향과 궤를 같이 한다. 대부분의 회원국에서의 법제의 논의는 EU 차원의 규범으로 구체화된다.

2) 유럽 연합의 통신 지침 및 개인정보 보호 지침The European Telecommunications Directive / The European Data Protection Directive

유럽 연합은 회원국 국민들의 데이터의 침해에 대한 광범위한 보호를 위하여 두 가지 지침을 마련하였다. 통신 지침과 데이터 보호에 대한 지침은 프라이버시에 관한 일정한 수준의 기반을 마련하여 새로운 권리들에 대한 범위를 확장시켰다. 데이터 보호에 대한 법규는 전 유럽 연합에 걸친 데이터 보호법을 조화시킬 수 있는 국제법의 기준점을 마련하였다. 각 유럽연합의 국가들은 1998년 10월에 서로 보완하는 입법을 시행할 것이 요구되었는데, 이것은 2000년 말경까지에도 아직 완전히 진행되고 있지는 않다. 통신에 대한 지침은 전화, 디지털 TV, 이동 네트워크들, 그리고 다른 원격통신 시스템들을 포괄하는 구체적인 보호를 주요 내용으로 한다.

데이터 보호법에 관한 여러 이론들, 예를 들면, 데이터 발생의 근원에 대한 알 권리, 불분명한 데이터의 교정할 수 있는 권리, 불법 접근에 대한 상환 청구권과 일정 상황하에서 데이터 사용의 승낙을 하지 않을 권리 등의 원리들은 위 지침하에서 더욱 강화되었다. 예를 들면, 개인들은 보내오는 마케팅 물건을 받지 않을 수 있는 권리들을 가진다. 데이터 보호 법규는 민감한 개인적인 데이터와 관련한 건강과 재정 같은 보호들을 강화한다. 이러한 정보의 상업적 사용은 일반적으로 '명시되고 분명한' 데이터 목적이 요구되는 것으로 제한된다.

위 지침들의 또 하나의 초점은 '집행력enforceability'에 맞추어져 있다. 데이터의 주체들은 명문의 법규에 의하여 권리를 보유하고 있으며 자연인이나 공공기관이 정보 주체들의 이익에 반하여 이용될 수 있는 권한을 제한한다. 이를 보장하기 위하여 회원국들은 프라이버시 감독관 또는 관련 기관을 설립하여 이를 집행할 수 있도록 해야 한다.

통신 지침은 광범위한 의무를 통신사업자와 서비스공급자들에게 인터넷과 연계된 활동을 포함한 통신 사용자의 프라이버시를 보호하도록 부과하고 있다. 새로운 법칙들은 프라이버시 법률들의 흠결의 부분을 메워 줄 것이다. 데이터를 선전하는 것은 엄격하게 제한될 것이며 마케팅 활동에 있어서도 향후 그럴 것이다.

V. 위치정보 규제의 지향

1. 지향

전자거래의 신뢰성 및 안전성 확보를 위하여 정보보호가 필수적으로 요구된다. 또한 정보보호에 관한 사항은 향후 거래당사자 특히 사업자의 의무 및 책임문제로 다루어지게 될 것이다. m-비즈니스에서도 전자거래 전반에 있어서와 마찬가지로 정보보호는 전자거래의 신뢰성 및 안전성 확보를 위하여 필수적인 사항이 되고 있다. 그러나 현행 법령은 전자거래당사자들에게 보호조치를 취하도록 규정하고는 있으나, 이러한 의무의 이행기준, 의무불이행시 계약 전체에 대한 효과 및 배상책임의 범위 등에 대하여 아직 충분한 검토가 이루어지지 않고 있다. 따라서 우선은 이러한 법적 논의가 미흡한 이슈들에 대해 재검토하고 전자거래당사자들에게 명확하고 준수 가능한 보호조치의 기준을 설정하여 줄 필요가 있으며, 또한 보호조치와 관련한 제반 문제에 대한 심도 있는 검토가 병행되어야 한다고 본다.[29] 특히 개인위치정보의 효과적인 보호를 위해 개인위치정보 주체의 동의 철회권, 열람 청구권, 손해배상 청구권, 분쟁조정 신청권 등을 보장하는 법적 장치가 마련되어야 하며, 손해배상과 관련 개인정보 보호 주체가 인식하지 못하는 상황에서 통신설비에 의해 위치정보가 수집되는 만큼 입증책임을 해당 위치정보업자가 고의 혹은 과실이 없음을 증명하도록 하고, 분쟁당사자간 대등한 협의를 통해 해결이 어려운 경우 제3의 기구를 통한 해결방안이 마련되어야 한다.

2. 위치정보 보호의 원칙

(1) 공정한 위치정보 실행 방안(Fair Location Information Practices: FLIP)

무선인터넷, 무선 이메일 또는 GPS 서비스와 같은 이동 정보 서비스로부터 유래된 위치정보에 대해 사생활 보호는 핵심 의제이다. 비록 위치정보가 셀룰러폰과 같은 이동통신 서비스 고객을 위해 사용되는 경우, 위치정보 자체에 대한 보호와 업체들이 마케

29) 한국전자거래진흥원, m-커머스 WG 발표 자료, 2000.10.11, p.79.

팅이나 다른 목적을 위해 정보를 사용하기 위한 법적 요건 등이 구비되어야 한다.

다양한 위치기반이동 서비스의 폭넓은 채택과 수용을 촉진하기 위해서, 무선 산업은 위치 관련 사생활 논점에 선도적인 위치를 차지한다. 서비스 이용과 관련된 위치정보는 철저히 보호될 것이고, 회사의 사생활 보호정책 내에서 사용된다는 것을 기업 스스로가 고객에게 보장하는 일련의 과정을 "공정한 위치정보 실행 방안(Fair Location Information Practices: FLIP)"이라 부른다. FLIP을 채택한다는 것은 책임 있는 자율규제를 위한 사업자단체의 현재의 동향을 적극적으로 반영하는 것이다. 실제로, 선도적인 인터넷 CEO 그룹은 최근에 사생활 보호를 근본법칙이라고 환기시키고, 다른 회사들이 견고하고robust, 명백하며visible, 포괄적인comprehensive 사생활 정책을 채택하도록 권고하고 있다.[30] 좀더 무선서비스에 적절한 새로운 조직인 무선광고산업협회(Wireless Advertising Industry Association: WAIA)가 최근 온라인 광고 회사인 AdForce, Motorola, Media Metrix와 무선장비 시장을 증대하기 위한 L-Commerce 관련 선도 업체들에 의해서 형성되었다.[31] 그와 같은 서비스 시장을 위한 사생활 정책의 탄생은 협회 목록의 최우선상에 있다.

고객들에게 어떤 정보를 가지고 이용할 것인지를 알려주고, 참여할 수 있는 선택권을 부여하고, 그들의 개인정보가 보호될 것이라는 점을 철저하게 보장하여야 고객들이 개인정보를 기꺼이 제공하려고 한다.[32] 초창기 L-Commerce 산업에 대한 회의는 고객에게 사생활 위치정보 보호에 대한 약속을 통하여 비로소 해소될 수 있다. 이것이 FLIP의 핵심이다.

(2) 사전 동의 요건

미국의 '무선통신에관한공공안전법(WCPSA: Wireless Communications and Public Safety Act of 1999)'에서 위치정보를 사용하는 데 있어서 고객의 동의는 주요한 사항이

30) Friedman, Sherman, "Top Internet CEOs Urge Better Privacy Policy," Newsbytes, Special to the *E-Commerce Times*, May 11, 2000.
http://www.ecommercetimes.com/news.articles2000/000511-nb2.shtml

31) http://www.adforce.com/waia/

32) Getting to Grips with Privacy Laws, IT-Analysis, April 7, 2000.
http://www.it-director.com/00-05-10-3.html

다.[33] 의회는 이동통신 서비스로부터 유래된 위치정보를 고객 소유 네트워크 정보(Customer Proprietary Network Information: CPNI)로 선언했다.[34] 연방통신법 222(c)(1)에서는 "고객의 동의나 법령에 의한 예외 적용을 제외하고는 서비스의 제공에 따라 고객 소유 네트워크 정보를 얻을 수 있는 통신사업자는 단지 당해 통신서비스나 부수적 필수 서비스에 있어서만 개인식별이 가능한 고객 소유 네트워크 정보를 접근 가능하며, 사용할 수 있다"고 규정하고 있다. 다시 말해서, CPNI는 전화의 목적을 위해서는 사용할 수 있으나 고객의 동의 없이 다른 서비스의 마케팅을 위해 사용하지 않는다. CPNI는 단지 부정 수단을 방지하기 위한 과금 등의 예외의 경우에만 고객 인증 없이 사용할 수 있다.[35]

이와는 달리 연방통신위원회(FCC)는 '위치 CPNI'에 관하여는 현재 분명한 입장을 나타내지 않고 있다. USWest v. FCC 판결에서 FCC의 최근 '위치 CPNI'에 관한 규정은 1999년 제10 순회 항소 법원에 의해서 실효되었다.[36] 실효된 위치 CPNI 규정은 사업자가 고객들에게 CPNI 공개에 관하여 사전 동의를 하지 않을 권한이 있다는 명백한 주의를 의무화하고, 이에 대한 명시적 동의를 요하는 강력한 옵트인opt-in 접근 방법을 요구하였다.[37] 법원은 마케팅을 위한 고객의 CPNI를 사용하기 전에 고객에게 사전 통지를 하고 또한 적극적이고도 명시적 승인만을 얻도록 사업자에게 요구하는 FCC의 규칙은 미연방 수정헌법 제1조의 표현의 자유 조항에 위배된다고 판시하였다.[38] USWest 법원은 의회가 CPNI 목록에 '위치정보'를 추가하였으므로 다른 CPNI 정보에 준하여 처리되어야 함에도 불구하고 특별히 '위치 CPNI'에 관하여 엄격한 절차를 채택한 것의 유효성을 문제 삼은 것이다. 현재의 팽창하는 위치 관련 산업에서의 경쟁과 혁신은 위치정보에 대한 합리적 접근을 보장하는 하나의 압력으로 작용하고 있다. 따라서 필요한 동의 형식은 문서나, 구두, 전자적 형태, 나아가 묵시적, 암묵적 동의를 포함하는 다소 약한

33) 47 U.S.C. 222(f)
34) 47 U.S.C. 222(h)(1)
35) 47 U.S.C. 222(d)
36) *USWest v. FCC*, 182 F.3d 1224(10th Cir. 1999), *pet. For cert.* Filed(Feb. 28, 2000).
37) Second Report and Order and Further Notice of Proposed Rulemaking, Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, CC Docket 96-115, Par. 87(Rel. Feb. 26, 1998)
38) USWest v. FCC, 182 F. 3d 1224(10th Cir 1999), petition for cert. Filed(Feb. 28, 2000)

형태의 동의로도 충분할 것처럼 전망할 수 있다.

이것은 어떤 통신사업자가 새로운 서비스를 활성화하기 위해 주로 사용하는 '수축 포장 계약shrinkwrap contract'의 법리도 원용될 수 있음을 의미한다. 즉 위치정보의 공개를 위해서는 원칙적으로 명시적 동의express authorization라는 요건을 충족해야 하지만, 그것은, 서비스제공자의 청약과 사용자의 서비스 약관에 대한 승낙으로 서비스가 일단 개시되면 동의한 것으로 볼 수 있다는 것이다.[39] 온라인상에서의 클릭 랩clickwrap 계약이나 무선통신에서의 단말기handset상에서의 동의도 "동의하면 send를 누르라"는 방식의 미리 녹음된 메시지에 대한 응답으로 동의를 표시할 수 있다고 할 것이다. 다만 고객이 자신의 위치가 누설될 수 있는 위치기반서비스에 대하여는 동의 여부에 관하여 엄격한 기준이 적용되어 어떠한 의문점도 없어야 한다.[40]

(3) 위치 프라이버시 원리(Location Privacy Principles)

CTIA가 제안한 위치 프라이버시 원리는 절차의 공정성과 적법성에 기초한다. 여기서 적법/공정성은 통지notice, 동의consent, 보안과 보전security and integrity, 그리고 기술 중립의 요소들로 구성된다. 위치정보 프라이버시 원리를 채택하고 이 정책 규정 실현을 위해 서비스제공자들에게 유연성을 허락하는 것은 새롭고 유익한 위치서비스와 응용기술들이 개발되는 동안 위치정보가 보호된다는 것을 소비자에게 보증하는 이중의 이익이 있다는 것을 산업계와 정책 입안자가 공감하였다.

1) 통지notice

첫 번째로 맨 먼저, 위치서비스 제공자는 특정 위치정보 수집을 반드시 "고객에게 알려야"하고 어떤 위치정보의 공개나 사용 "전에" 이를 수행하여야 한다use practices. 서비스제공자가 고객에게 그들의 위치정보 수행방법을 알려주는 데에는 몇 가지의 방법이 선택될 수 있다. 가장 손쉬운 방법으로 통지notification는 서비스의 개시에 앞서 서비스 제공 계약의 내용으로 포함될 수 있다. 제공자는 또한 웹사이트에서, 전자메일에서, 또

39) ProCD, Inc. v. Zeidenberg, 86 F.3d 1447(7th Cir.), rev'g 908 F. Supp. 640(W.D. Wis. 1996)

40) Memorandum Opinion for John C. Keeney, Acting Assistant Attorney General, Criminal Division, from Richard L. Shiffrin, Office of the Deputy Assistant Attorney General 6(Sept. 10, 1999)

는 가입자에게 보내어지는 편지로써 위치정보정책을 설명할 수 있다. 소비자는 또한 사업자의 모든 정책과 실행 방법의 설명을 위한 무료 전화번호나 인터넷 사이트 주소를 청구서에서 통보 받을 수 있다.

2) 동의consent

CTIA 프라이버시 원리의 특징은 연방통신법하의 특정의 예외를 제외하고는 어떤 수집 활동에도 앞서 '명시적 동의'가 필요하다는 것이다. 이는 "명시적 인증express authorization)"이라고도 표현되는데 이는 위치서비스에 관한 동의가 거래에 참여하고 싶다는 고객의 요구를 분명히 입증하는 한 이 원리의 아래에서 문서, 구두, 전자 또는 다른 형태로 이루어질 수 있다는 것을 의미한다. CTIA는 서비스제공자가, 웹사이트 가입에서의 서명된 서비스 계약서 또는 전화기나 PDA에서 사용자 송신하는 "클릭 랩clickwrap" 계약서에 이르기까지 동의 조건을 충족할 수 있는 다양한 방법이 있을 수 있다고 제안하였다. 반복컨대, 여기서 중요한 요소는 동의가 명백하게manifest 또한 위치정보의 사용에 앞서 명시적으로express 이루어진다는 것이다.

3) 보안과 보전Security & Integrity

위치서비스 제공자는 수집된 모든 위치정보를 안전하게 관리하여야 한다. 위치서비스 제공자에 의해 사용되는 시스템은 허가되지 않은 접속과 제3자에로의 누설과 공개로부터 위치정보를 보호해야 한다.

4) 기술 중립 원리Technology Neutral Principles

회사의 프라이버시 정책과 소비자의 프라이버시에 대한 기대 모두 특정 위치 기술에 좌우되어서는 안 된다. 위치기반서비스는 기술 중립적이어야 한다. 즉 서비스가 전화기이든 네트워크를 기반으로 하든 사용되는 프라이버시 표준은 같아야 한다는 뜻이다. 오늘날, 세계의 표준단체들은 무선 터미널과 장치의 지리적 위치를 결정하고 전송하는 능력을 정의하고 표준화하는 과정에 있다. 예를 들면, 위치정보처리 상호운용 포럼은 셀 아이디Cell-ID와 Timing Advance, E-OTD(GSM), AFLT(IS-95)와 MS기반의 Assisted GPS를 기반으로 하는 위치 결정 방법과 그 지원구조를 위한 표준을 조성하고 있다. 이 표준화 노력은 때로 프라이버시에 관계되는 점들을 나타내는 특징들을 포함한다. CTIA는 그런 기술 독립적 프라이버시 솔루션을 지원하는 원칙을 천명하였다.

2. 입법 유형에 관한 결단

위치정보 보호 및 활용에 관한 입법에는 몇 개의 주요 모델들이 존재한다. 각 유형들은 순기능과 역기능을 동시에 가지고 있다. 전항의 위치정보 보호 원칙에 입각하여 입법을 구체화하기 위하여 적합한 입법 유형을 선택하는 의제에 관한 공감과 합의를 이끌어 내는 것이 필요하다.

(1) 포괄적 입법(Comprehensive laws) v. 개별적 입법(Sector laws)

공공 분야와 민간 분야에 의한 개인정보에 관한 수집과 사용 그리고 보급에 관한 것을 총체적으로 규율하는 데이터 보호법의 모델이 있다. 이는 유럽 연합에 의해 채택된 유형이다. 이러한 입법례는 법집행을 위한 공공기관을 따로 설립할 것을 요한다. 이는 종종 커미셔너, 옴부즈만 또는 레지스트라Registrar라고도 불리는데, 법집행을 감시하고 위반 사항을 색출, 조사한다.

미국을 비롯한 몇몇의 나라에서는 일반적인 데이터 보호 법규를 채택하지 않고 특별법만을 제정한다. 예를 들자면 비디오 대여 기록이나 재정적인 프라이버시들이 그러하다. 이러한 경우에, 시행은 개별 사안의 특수한 메커니즘을 통하여 성취될 수 있다. 이러한 접근의 결정적인 단점은 이런 특별법의 시행은 각각의 새로운 기술에 맞는 뒤떨어지지 않는 새로운 법규들을 계속적으로 제정하여야 한다는 것이다. 또한 감시 기관의 결여도 문제가 된다.

(2) 상향 규제(Bottom-Up) v. 하향 규제(Top-Down)

프라이버시 보호에 관해서 미국은 행정감시기구를 설치하지 아니하고 업계의 자율규제self-regulation를 허용하거나 정보 주체인 개인에게 사후적 구제 수단을 부여함으로써 프라이버시를 보호하려는 방식을 취하고 있다. 이러한 방식은 원칙적으로는 사업자들에게 개인정보 보호의 1차적 책임을 부여하고, 특별한 목적이 있는 경우에만 예외적으로 정부의 규제가 개입된다는 의미에서 '상향식Bottom-UP' 규제라 할 수 있다. 이러한 자율규제는 단지 약한 보호라는 것과 강제성의 부족으로 실효성이 없는 경우도 많다. 또한 사업자들이 자신의 영리적 목적 추구와 이해관계에 따라서 규제의 기본인 투명성

transparency을 확보하는 것이 어렵다는 단점이 있다. 또한 인터넷 업체들의 소규모성, 영세성 때문에 규제의 집행에 필요한 자원과 비용을 충당하기 어렵다는 지적도 있다.

반면에 유럽 국가들은 포괄적인 입법을 통하여 행정기관에 의한 감시나 독립적인 기구를 설치하여 개인정보의 취급을 통제하며 이를 위반하는 경우 강력한 집행 수단을 동원하는 방식을 택하고 있다. 이러한 방식은 정부 규제가 프라이버시 보호의 원천이며 민간부문에서의 당사자 사이의 약정의 정당성 판단의 원천이 된다는 점에서 '하향식 Top-Down' 규제라 불린다. 생각건대, 사업자들이 가지는 정보수집자로서의 지위와 정보보호자로서의 지위는 본질적으로 상충되는 것이므로 그들이 자신들의 이익에 도움을 가져올 경우에만 개인정보를 보호하기 위해 나설 것이라는 점은 예상할 수 있으므로, 업계의 자율적 규제에 비하여 정부가 적극 개입하여 행정감시기구를 설치하는 방식이 바람직하다는 것이 이러한 정부통제의 방법의 이론적 근거이다. 다만 이는 관료적 비효율성이라는 문제를 낳는다.

(3) 위치정보 보호(Opt-in) v. 위치정보 이용(Opt-out)

1) 정지조건부 동의 v. 해제조건부 부동의

동의에 관하여 보면, '정지조건인 동의opt-in'와 '해제조건인 부동의opt-out'의 방법으로 정보수집자의 조건을 받아들이거나 거절할 수 있다. 정지조건인 동의는 위 계약의 정지조건이 된다는 것으로서 정보수집자는 동의가 있기 전까지는 개인정보를 원래 제공된 목적 이외에는 사용할 수 없다. 해제조건인 부동의가 위 계약의 해제조건이 된다는 것으로서 개인이 특정 기간 이내에 이의를 제기하지 않는 한 개인정보를 사용할 수 있다.

2) 개인식별 정보(Personally Identifiable Information: PII) v. 개인식별 불능 정보(non-PII)

미국의 소비자 사생활 보호법은 개인식별 정보에 관하여는 opt-in 방식의 동의를 필요로 하지만, 개인식별 불능 정보에 관하여는 opt-out 방식의 동의도 무방하다고 규정하고 있다. 따라서 어떤 개인정보가 개인식별 정보에 포함되는지 여부는 법규의 적용 범위를 정하는 중요한 기준이 된다.[41]

41) 연방통신위원회는 PII의 범위를 다음과 같이 정하고 있다.
이름, 주소, 이메일 주소, 전화번호-사회보장번호, 크레딧 카드 번호, 생일, 출생지, 출생증명번호, 온라

인 및 오프라인상에서의 접촉점, 기타 사업자가 수집, 결합하여 특별히 식별할 수 있게 된 정보

Ⅵ. 결 론

현대 법제에서 가장 바람직한 정보 프라이버시 보호 방안은 계약에 의한 보호 방식이다. 즉 개인과 정보 이용자 사이에 개인정보의 수집, 공개 및 이용에 관한 계약을 체결하는 것이다. 정보 계약의 구성요소는 통지notice 및 동의consent이다.[42] 통지는 개인이 충분한 정보를 가지고 개인정보 이용에 관한 동의informed consent 여부를 결정할 수 있도록 하는 데 목적이 있다. '정지조건인 동의opt-in'는 개인의 명시적인 동의를 요구하며 정보 수집자는 명시적인 의사표시가 있기 전까지는 개인정보를 원래 제공된 목적 이외에는 사용할 수 없음을 의미한다. 그러므로 계약에 의한 정보 보호의 방식을 취하되 옵트인 방식을 기본적으로 적용한다.

이에 따라 위치기반서비스 제공자는 정보주체로부터 사전 동의를 받지 아니하고는 위치정보를 수집할 수 없다. 다만, 위치기반서비스 이용계약의 이행을 위하여 필요한 경우, 위치기반서비스 제공에 따른 요금정산을 위하여 필요한 경우, 특별한 규정이 있는 경우 등은 동의를 요하지 아니한다. 정보주체는 위치정보의 수집, 이용 또는 제공에 관하여 그 범위를 제한하거나 내용의 일부에 관하여 동의를 유보할 권리가 있다.

위치정보 주체가 보유하는 권리는 다음과 같이 요약된다. 만일 자신의 위치정보가 타인에 의하여 보관, 처리, 사용되는 경우에는 이에 대한 내용과 절차를 통지 받을 권리를 보유한다. 특히 위치정보가 어디에 사용되는지에 관한 목적이 구체적으로 명시되어야 한다. 또한 위치정보 처리 사업자는 위치정보 사용에 관한 개인의 동의를 서면 등의 명시적 증거로 확보할 의무를 진다. 또한 그 활용에 관한 제한이 있는 경우 이에 종속된다.

정부는 수사상 또는 사회질서, 국가 안보 등의 필요에 의하여 필요한 경우 통신사업자 등에게 위치정보 포착을 위한 장치의 부착을 명령할 수 있다. 위치정보가 국가의 안전보장을 위하여 요구되는 경우 법정 절차를 거쳐 사용될 수 있다. 이는 일반적 통신 비밀과는 구별되는 별도의 절차를 요한다. 정보주체의 생명, 신체 또는 재산에 대한 위해를 방지하기 위한 경우 당해 정보주체의 동의 없이도 위치정보를 수집할 수 있다.

---

42) Michael Altschul, "The CTIA Location Information Privacy Petition," Cellular Telecommunications Industry Association, May 2001, p.3.

위치기반서비스 제공자는 검사 또는 수사관서의 장, 정보수사기관의 장으로부터 수사 또는 형의 집행, 국가안전보장에 대한 위해를 방지하기 위한 정보수집의 필요에 의하여 정보주체의 위치정보의 제공을 요청 받은 때에는 이에 응할 수 있다.

정부는 주요 기반시설을 마련할 역할을 담당한다. 정부는 전통적인 범죄 수사 및 대외 정보수집 책임 사이의 조화와 균형을 가져야 한다. 수사기관은 사법부의 승인에 의한 감청, 압수 수색 및 정보의 제출을 강제할 수 있는 소환 영장을 발부할 수 있는 권한을 포함하여 분명히 범죄수사 및 정보수집을 위한 강력한 권한을 가지고 있다. 이러한 권한들을 보유하고서도 정부는 기반시설 준비 책임을 맡은 상태에서 추구하는 많은 정보를 얻기 위하여 기업들의 자발적인 협력에 의존할 것이 요청된다.[43] 수사기관과 이러한 종류의 관계 속에서 협력할 것을 요청 받은 기업들은 단지 그들이 법인 책임과 개인 책임을 따로 평가하기를 바라기 때문에 정부의 초점이 자발적인 정보수집으로부터 범죄수사 쪽으로 이동하는 때가 언제인지 명확하게 이해하기를 바라게 된다. 그러나 수사기관은 그러한 경우 수사의 대상에게 경고를 줄 위험이 있기 때문에 보장을 해 줄 수가 없다.

잠재적인 갈등을 최소화하는 한 가지 방법은 수사기관이 보호 임무의 역할로서 수집하는 정보를 엄격히 제한하는 것인데, 사실 수사기관은 기반시설 구성요소와는 단지 접촉하는 수준의 계획을 가지고 있을 뿐이다. 그러므로, 수사기관이 주요 기반시설에 대한 공격을 수사하는 데 있어서 지도적인 위치에 있어야만 하는 반면에, 시민의 자유권의 보호와 효율성의 요구는 모두 기반시설 장착 임무, 그리고 기업들과의 가교 역할은 다른 정부 기관에 위임되는 것이 필요하다. 이러한 역할의 혼선은 진전된 협조적인 정보 공유의 방법으로 해결될 수 있다.

그러한 위험은 법률집행을 위하여 통신사업자와 위치기반서비스업자의 협조와 지원을 규정함으로써 해소될 수 있다. 이를 위해서는 별도로 수립된 기준 확정 과정의 이행이 필수적이다. 필요한 기업의 기술적인 규준 체계는 법원이 명령한 감청, 위치확인 등을 계속적으로 수행할 수 있게 하는 법집행의 요구를 이행하기 위하여 디지털 변환 장비를 개발하는 데 적용된다. 기업에 모든 부가적인 능력을 포함시킬 것을 강제하기 위

43) Magnus Sakberg Oskarsson, *Iceland Telecom: Iceland Telecom*, May 2001, p.10.

하여 분명한 입법적 조치가 입법의 핵심적 내용이 된다. 이를 위하여 정부와 사적 영역 간의 진실로 협력적이고 투명한 동반관계만이 주요 기반시설에 관한 정책의 목적을 달성시킬 수 있다.

그러므로 정부의 규제 및 입법은 다음과 같은 원칙하에 이루어져야 한다.[44] 첫째, 민간부문에 의한 정보의 공유에 정부의 강제와 민간의 자발적 참여가 조화를 이루어야 한다. 산업계의 자발적인 참여가 정부의 접근에 있어 필수적이다. 왜냐하면 민간부문이 이러한 하부조직을 만들었고 운영하므로 민간부문이 이를 가장 잘 이해할 수 있고 그 보안을 향상시키기 위한 노력을 이끌어야만 한다. 둘째, 정부에 의해 부과된 명령에 대한 실행 방법을 마련하여야 한다. 다만 정부는 기업의 예산과 산업 전체의 전망 등을 고려하여 계획을 실현하여 나가야 하며 구체적인 진행은 시스템을 운영하는 사람들에게 맡겨져야 한다. 셋째, 정부는 직접적인 강제보다는 이를 유인, 권장하고 충고하는 정책수단을 우선적으로 시행한다. 또한 정부도 필요한 특별한 지식이나 전문기술을 갖추도록 노력하여야 한다.

44) 이영대 외, 『지리공간정보 유통 촉진을 위한 법 제도 정비 방안』, 정보통신정책연구원, 1999.12, p.142.

참고문헌

김도경, 「위치정보보호법의 제정에 따른 LBS산업의 규제정책 방향」, 『정보통신정책』 제15권 19호, 2003.10.

오태원, 「개인위치정보의 법적 문제와 위치기반서비스의 전망」, 『정보통신정책』 제14권 6호, 2002.4.

염용섭, 「무선인터넷 서비스 현황과 발전 방향」, SK 정보 포럼 발표문, 2001.11.

이영대 · 오승종 · 김은형 · 황주성 · 권헌영, 『지리공간정보 유통 촉진을 한 법 제도 정비 방안』, 정보통신정책연구원, 1999.12.

이영대 · 이병호 · 이창순, 『공공기술이전에 관한 법과 정책 연구 방안』, 2001.12.

이영대 · 최경규, 「모바일 비즈니스 법제 기초 연구」, 『기업의 모바일 비즈니스 활성화 방안 연구』, 전자거래진흥원, 2003.

이영대 · 황철수, 「위성정보의 유통 및 활용 활성화를 위한 법 제도 정비 연구」, 『정부』 2001.2.

정재훈, 「민간부문에서의 정보프라이버시 보호」, 『정보법학』, 1997.9.

한봉조, 「정보화사회의 법률 문제와 정보 보호」, 『정보법학』, 1996.9.

전자신문 사이트, http://www.etnews.co.kr/news

Allen, Richard, “Location-Based Service - Privacy and Security, Issues and Ideas,” *Consult Hyerion*, May 2001.

Altschul, Michael, “The CTIA Location Information Privacy Petition,” Cellular Telecommunications Industry Association, May 2001.

Banisar, David and Davies, Simon of Privacy International, “Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection and Surveillance Laws and Developments,” 18 *J. Marshall J. Computer & Information L.* 1, Fall 1999.

Dresner, Stewart, *Privacy: The Impact of the EU’s Proposed E-com Directive on Mobile Location Services:* Privacy Laws & Business, Symposium on Mobile Location

Service 2001, May 2001.

Friedman, Sherman, "Top Internet CEOs Urge Better Privacy Policy," Newsbytes, Special to the *E-Commerce Times,* May 11, 2000. (http://www.ecommercetimes.com/news.articles2000/000511-nb2.shtml)

Gidari, Albert, *Location Privacy: Fair Location Information Practices for Mobile Commerce: Location Decisions 2000: Application of Location Technology for the International Commercial Environment,* June 13-24, 2000.

GSM(Global System for Mobile Communications), "3GPPS TS 22.071 V4.3.0: 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Location Services(LCS)," Service Description, Stage 1(Release 4), March 2001.

Nieminen, Jukka, *Examining How Terminal Technology is Being Developed to Enable and Enhance Location Service and Applications,* Benefon, May 2001.

Nordstrom, Jonas, *Examining the Latest and Evolving Standards for Advancing Location Based Service,* Ericsson, May 2001.

Nylund, Jared J., "Fire with Fire: How the FBI Set Technical Standards for the Telecommunication Industry Under CALEA," 8 *CommLaw Conspectus* 329, Summer 2000.

O'Neil, Michael J. and Dempsey, James X., "Critical Infrastructure Protection: Threats to Privacy and Other Civil Liberties and Concerns with Government Mandates on Industry," 12 *DePaul Business Law Journal* 97, Fall 1999/Spring 2000.

Oskarsson, Magnus Sakberg, *Iceland Telecom: Iceland Telecom,* May 2001.

Richman, "Gadgets may Compromise Privacy, Seattle Post-Intelligencer," Mar. 9, 2000.

Rosow, Michael A., "Is Big Brother Listening? A Critical Analysis of New Rules Permitting Law Enforcement Agencies To Use Dialed Digit Extraction," 84 *Minnesota Law Review* 1051, April 2000.

Shimomura & Markoff, *Takedown : The Pursuit and Capture of Kevin Mitnick, America's Most Wanted Computer Outlaw-By the Man Who Did It,* Dec. 1996.

Turnill, Mike, *Robust Multi-Access Platforms for Mobile Location Service: Oracle Corporation,* May 2001.

Valentine, Debra A., *Privacy: Protecting the Consumer on the Global Information Infrastructure*, FTC General Counsel, Dec. 1998. (http://www.ftc.gov/speeches/other/dvaboutprivacy.htm).

Weber, Wireless Gadgets, "Web Companies Plan to Map your Moves," *Wall Street Journal*, B1, May 8, 2000.

Wimmer, Kurt, *Mobile Location Privacy and Law Enforcement: The Experience in the United States: Covington & Burling,* May 2001.

Wolfe, D. Forest, "The Government's Right to Read: Maintaining State Access to Digital Data in the Age of Impenetrable Encryption," 49 *Emory Law Journal* 711, Spring 2000.

Wudrak, Jorg, *Location Service with GPRS and UMTS Commercial and Technological Impacts: Siemens,* May 2001.

(Relevant sources)

Electronic Commerce Directive EU (2002)

Electronic Communications Act UK (2000)

Electronic Signatures Framework Directive UK (1999)

Communications Bill "OFCOM" UK (2003)

E-money Directive UK (2002)

Distance Selling Directive UK (2000)

Data Protection Act UK (1998)

Electronic Signatures in Global and National Commerce Act [E-SIGN] USA (2000)

Electronic Commerce Enhancement Act USA (2001)

Paperwork Elimination Act USA (2001)

Utah Digital Signatures Act USA (1996)

California Uniform Electronic Transactions Act USA (2000)

Digital Signature Guidelines ABA Information Security Committee USA (1996)

Uniform Electronic Transactions Act ALI USA (presented 1999)

Model Law on Electronic Commerce UNCITRAL (1996)

Model Law on Electronic Signatures UNCITRAL (2001)

Electronic Transactions Act Australia (2001)

Electronic Transactions Ordinance Hong Kong (2000)

Telecommunications Ordinance, Amendment Hong Kong (2000)

Telecommunications Bill, Amendment Hong Kong (2001)

Personal Data Privacy Ordinance Hong Kong (2001)

Electronic Transactions Act Canada (2001)

Personal Information Protection and Electronic Documents Act Canada (2000)

Electronic Transactions Act Singapore (1998)

Journal of Regulation Studies Vol.13 No.2 December 2004

Regulation on Locational Information and the Protection of Private Information

Young-Dae Lee, Gyoung-Gyu Choi

The core factor in the realization of location-based services (LBS) is locational information. When the subject of the locational information is 'human', the person's locational information directly connects with the issues of the protection of personal information and privacy. The distinction between personal information and privacy is needed since personal locational information may cause intrusion of one's privacy, which differs from information such as one's name, registration number, address and telephone number. Therefore, it implies that stronger protection measures are called for in the case of personal locational information compared to other personal information. Since the LBS will be widespread in the near future, it is necessary to establish rules that satisfy both service providers and customers and that enhance the reliability of the service. Locational information protection laws should include information contracts, regulation on locational information and privacy, and the protection of sensitive private information.

Key words : Location based services, Locational information, Information contract, Personal information protection, Privacy