

방송통신정책연구 11-진흥-라-09

모바일 서비스의 개인정보 활용행태 및 보호방안 연구

(A Study on Mobile Data Protection)

박노형

2011. 12

연구기관 : 고려대학교 산학협력단



이 보고서는 2011년도 방송통신위원회 방송통신발전기금 방송통신정책연구사업의 연구결과로서 보고서의 내용은 연구자의 견해이며, 방송통신위원회의 공식입장과 다를 수 있습니다.

제 출 문

방송통신위원회 위원장 귀하

본 보고서를 『모바일 서비스의 개인정보 활용행태 및 보호 방안 연구』의 연구결과보고서로 제출합니다.

2011년 12월

연구기관 : 고려대학교 산학협력단

총괄책임자 : 박 노 형

참여연구원 : 정 명 현

안 민 호

김 규 동

김 호 권

목 차

요약문	i
제1장 서 론	1
1. 연구의 배경과 목적	1
2. 연구의 방법 및 주요 내용	2
3. 주요 용어의 정의	4
제2장 모바일서비스의 개인정보 이용 양태	6
제1절 스마트 미디어와 개인정보 보호	6
1. 스마트 모바일기기 보급 현황과 전망	6
2. 스마트 미디어의 특성	9
제2절 모바일서비스를 통해 수집/이용되는 개인정보의 유형 및 수집방법	14
1. 개인정보의 유형별 분석	15
2. 스마트폰 애플리케이션 및 앱스토어 현황	27
제3장 모바일서비스의 개인정보 이용의 문제점	13
제1절 모바일 환경의 도래에 따른 외국의 동향	34
1. 유럽연합	34
2. 영국	36
3. 미국	37
제2절 모바일서비스 개인정보 이용에 대한 이용자 인식도 조사를 통해 드러난 문제점	40
1. 조사의 목적과 방법	40
2. 설문조사 결과	40
3. 설문조사 분석	71
제3절 사례를 통하여 드러난 문제점	97
1. 모바일서비스상 개인정보 불법수집 사례	97

2. 사례 분석	104
제4절 소 결	109

제4장 현행 법제의 평가 및 개선방안 12

제1절 모바일서비스에 적용되는 현행 법체계 개관	112
1. 개인정보보호법의 주요규정	114
2. 정보통신망법의 주요규정	116
3. 위치정보법의 주요규정	118
제2절 개인정보의 범위와 적용대상의 불명확성	120
1. “개인정보”의 범위	120
2. 개인정보보호법제의 인적·장소적 적용 범위	139
제3절 동의 획득 절차 — 적법하고 정당한 동의의 획득	147
1. 동의 방식의 개선	147
2. 선택적 동의제도의 효율적 확보	156
제4절 개인정보파일 등록 및 개인정보 영향평가 대상의 확장	165
1. 개인정보파일 등록의 의무	166
2. 개인정보 영향평가	167
3. 개인정보파일 등록 및 영향평가를 통한 모바일 개인정보의 보호	169
제5절 모바일서비스에 특화된 개인정보 취급방침의 정비	171
1. 정보통신망법의 문제점	171
2. 개인정보 취급방침에 대한 이용자 접근성 확보	173
제6절 제3자 제공시 동의 방식/범위	178
1. 제3자로부터 개인정보를 제공받는 자의 의무 강화	178
2. 위치기반서비스의 약관 동의 방식의 개선	183

제5장 결 론 184

참고문헌	189
------------	-----

부 록 : 모바일 개인정보보호에 대한 이용자 인식도 조사	195
---------------------------------------	-----

표 목 차

<표 2-1> 국내 스마트폰 가입자 현황 (단위 : 만명, %)	7
<표 2-2> 일반 피쳐폰과 스마트폰의 특성 비교	10
<표 2-3> 운영체제별 애플리케이션 마켓 성장 전망	28
<표 2-4> 국내 안드로이드 마켓 최다 이용 애플리케이션	30
<표 3-1> 안드로이드 마켓 서비스 약관 동의 획득 절차	73
<표 3-2> 정보통신망법 제27조 2에 따른 개인정보 취급방침 필수항목	81
<표 3-3> 카카오톡의 변경 전 개인정보 취급방침	90
<표 3-4> 스마트폰을 이용한 철회의 절차	94
<표 4-1> 분야별 개인정보에 관한 국내법	113
<표 4-2> 법규별 개인정보의 정의	121
<표 4-3> 관련법상 개인정보보호 관련 형벌 규정	128
<표 4-4> 관련법상 개인정보보호 관련 행정벌(과태료) 규정	131
<표 4-5> 동의 획득 과정에서 제시되어야 하는 필수적 항목	148
<표 4-6> 모바일 앱에서의 동의 획득 절차의 비교	149
<표 4-7> 동의 획득 필수적 항목의 개정안	155
<표 4-8> 개인정보 처리 목적과 수집 목적의 요건	158
<표 4-9> 영국 개인정보보호법 개인정보 처리원칙과 국내 개인정보보호법 개인정보 수집원칙의 비교	163
<표 4-10> 개인정보 영향평가 관련주체	168
<표 4-11> 개인정보 취급(처리)방침의 공개 방법	172
<표 4-12> 미국 MMA의 개인정보 취급방침 가이드라인의 예	174

그 립 목 차

<그림 2-1> Global Smartphone Sales Will Grow at +24% CAGR (단위: 백만)	7
<그림 2-2> 국내 휴대폰 및 스마트폰 가입자 전망	8
<그림 2-3> 국내 스마트폰 및 스마트패드(누적) 보급 전망('10~'15년)	9
<그림 2-4> SK텔레콤 음성통화료 및 무선인터넷 사용량 변동 추이	12
<그림 2-5> 카카오톡의 휴대전화 상태 및 ID 읽기 권한 명시 화면	17
<그림 2-6> 카카오톡 이용약관 및 개인정보 취급방침 동의 화면	18
<그림 2-7> 카카오톡 최초 설치 화면	19
<그림 2-8> 스마트폰 위치정보 수집 흐름도	23
<그림 2-9> 안드로이드용 페이스북 앱의 동기화 기능	25
<그림 3-1> 모바일 앱 보유 현황	41
<그림 3-2> 모바일 개인정보에 대한 불안감	42
<그림 3-3> 모바일 환경 고유의 개인정보 보호의 문제	42
<그림 3-4> 모바일 개인정보에서 가장 우려가 되는 사안(복수응답)	43
<그림 3-5> 이용자의 개인정보 통제 인식	45
<그림 3-6> 현재 개인정보자기결정권에 대한 만족도	46
<그림 3-7> 개인정보 자기통제 강화에 대한 찬성도	47
<그림 3-8> 개인정보자기결정권과 편리한 모바일서비스의 이용	48
<그림 3-9> 하거나 말거나 식의 동의절차에 대한 경험	49
<그림 3-10> 선택적 동의 절차에 대한 경험	50
<그림 3-11> 선택적 동의 절차의 도입에 대한 견해	51
<그림 3-12> 개인정보 취급방침에 대한 이용자의 태도	53
<그림 3-13> 개인정보 취급방침을 읽지 않는 이유	53
<그림 3-14> 모바일기기와 일반 컴퓨터의 개인정보 취급방침 접근성 비교	54
<그림 3-15> 개인정보 취급방침에 대한 이용자의 숙지도	55
<그림 3-16> 개인정보 수집목적의 광범위한 설정	56

<그림 3-17> 목적의 범위를 벗어난 개인정보의 수집	57
<그림 3-18> 개인정보 제3자 제공에 대한 불안감	58
<그림 3-19> 제3자 제공에 따른 통지 경험	59
<그림 3-20> 제3자 제공의 개별 통지 의무에 대한 인식	60
<그림 3-21> 무료 모바일서비스 이용에 따른 개인정보 제3자 제공 의사	61
<그림 3-22> 무료 모바일서비스를 위한 개인정보 제공의 허용범위	62
<그림 3-23> 강압적인 동의 절차에 대한 대안	63
<그림 3-24> 동의의 철회 후 이용자 개인정보 파기에 대한 신뢰도	64
<그림 3-25> 동의 절차와 철회 절차의 접근성 비교	65
<그림 3-26> 철회의 경험이 없는 이유	66
<그림 3-27> 철회를 하지 않은 후 문제점 인식에 대한 경험	67
<그림 3-28> 정부의 통일적 지침 마련에 대한 의견	68
<그림 3-29> 개인정보보호 위반시 처벌 수위	69
<그림 3-30> 개인정보 보호를 위한 개선사항	70
<그림 3-31> 2011년 9월 카카오톡 이용약관 변경	75
<그림 3-32> 아이폰에 나타나는 개인정보 취급방침의 예	79
<그림 3-33> 한 화면에 나타나는 개인정보 취급방침	80
<그림 3-34> 모바일게임 개발사 게임빌 개인정보 취급방침	82
<그림 3-35> 안드로이드 마켓에서 모바일 앱의 다운로드 방식	83
<그림 3-36> 개인정보 개념에 대한 이용자의 이해	84
<그림 3-37> 카카오톡 주소록 개인정보 수집에 대한 이용자의 인식	85
<그림 3-38> 카카오톡 친구추천 기능에 대한 불안감	87
<그림 3-39> 카카오톡 친구추천 기능에 대한 이용자의 인식	88
<그림 3-40> SK텔레콤 개인정보 이전 통보 및 철회 절차에 대한 인지	95
<그림 4-1> 영국 ICO 홈페이지의 개인정보처리 동의화면	151
<그림 4-2> 미국 TRUSTe에서 제공하는 모바일 개인정보취급 도안	176

요 약 문

1. 제 목

모바일 서비스의 개인정보 활용행태 및 보호방안 연구

2. 연구 목적 및 필요성

모바일 기술이 발전함에 따라 스마트폰을 비롯한 모바일 서비스 이용은 매해 급증하고 있으며 이러한 추세는 가속화될 전망이다. 모바일 서비스를 이용한 개인정보보호의 문제는 어느 다른 개인정보보호의 문제와 구별된다. 이는 기존의 유선 인터넷 접속방법과는 구별되는 모바일 기술만의 고유한 기술적 특징에 기인한다.

그러나 이러한 모바일 서비스로 인해 침해되는 정보주체의 권리에 대하여 『정보통신망 이용촉진 및 정보보호 등에 관한 법률』과 『개인정보보호법』 등의 현행법은 충분한 보호를 부여하지 못하고 있는 실정이다. 이러한 기술과 제도 사이의 격차를 극복하기 위하여 모바일 환경에서 발생할 수 있는 개인정보의 침해를 사전에 방지하고, 발생한 피해에 대한 정보주체의 권리를 구제할 수 있는 보호방안이 요구된다.

3. 연구의 구성 및 범위

본 연구는 제2장에서 새로운 모바일 환경의 도래로 인하여 발생가능한 개인정보의 문제가 무엇인지 파악한다. 기존의 오프라인이나 온라인에서 정보주체가 직접 자신의 정보를 제공하는 방식과 달리 응용 프로그램의 설치, 구동에 따라 자동적으로 기기 내 저장된 정보를 추출하여 개인정보처리자의 서버로 전송하는 모바일 환경은 개인정보보호에 대한 새로운 문제를 제기하고 있다. 특히 스마트 미디어를 통한 모바일서비스 이용에 있어서 행태 정보의 수집의 문제는 개인의 프라이버시를 침해할 수 있는 위험을 꾸준히 제기하고 있다.

모바일 서비스 이용 과정에서 처리되는 정보의 유형은 매우 다양하다. 모바일 기기의 설계상 자동적으로 수집되는 정보, 통신서비스 가입시 기본적으로 설치되어 있는 프로그램에 따라 서비스 제공자에게 전송되는 정보, 그리고 이용자의 모바일앱 설치와 실행에 따라

모바일서비스 제공자에게 전송되는 정보는 개인정보보호법제상 보호되는 개인정보에 해당하는 경우도 있고 개인정보의 지위에 이르지 않는 경우도 있다. 이에 따라 본 연구는 기기 식별정보, IMEI번호와 USIM번호와 같은 단말기 고유번호 등 모바일 서비스를 통해 처리되는 개별 정보의 유형을 파악하여 모바일 개인정보의 범위를 명확히 하였다.

제3장에서는 모바일서비스 환경의 도래에 따른 새로운 양태의 개인정보 피해를 우려하고 있는 주요국의 동향과 함께, 모바일 기술의 특징에 따라 발생할 수 있는 문제를 이용자의 인식도 조사와 국내외 사례를 통하여 분석하였다.

제4장에서는 현행 법제의 평가 및 개선방안을 다룬다. 모바일서비스에 적용되는 「정보통신망 이용 및 촉진에 관한 법률」, 「개인정보보호법」, 「위치정보보호법」 등의 현행 법체계가 모바일 개인정보의 범위와 적용대상을 명확하게 규율하고 있는지에 평가한다.

4. 연구 내용 및 결과

비록 동일한 유형의 정보라 하더라도, 모바일 기기를 통하여 처리되는 정보는 일반 컴퓨터를 통하여 처리되는 정보와 비교하여 개인정보에 해당하는 경우가 많다. 예컨대, IP 주소나 MAC 주소는 일반 컴퓨터와 모바일 단말기 모두에서 수집이 가능한 기기정보이다. 그러나 컴퓨터와 직접적으로 연결되는 개인정보 데이터베이스는 일반적으로 존재하지 않는 반면, 스마트폰과 태블릿 PC 등 통신사업자의 서비스를 매개로 하는 스마트 미디어는 자신이 보유하고 있는 이용자 개인정보 데이터베이스와 해당 기기정보를 일대일로 매칭하는 방법을 통하여 특정 개인에 대한 식별을 할 수 있다. 또한 개방형 운영체제를 사용하는 스마트 미디어의 특성상 기기로부터 정보를 수집할 수 있는 주체 역시 다변화되었다. 개방성에 따른 서비스 주체의 다양화는 개인정보에 대한 법률관계가 다양해지고 복잡해진다는 것을 의미한다. 과거의 이동통신서비스에서 개인정보의 문제는 이동통신사업자와 이용자 양자간의 문제로 한정되었다. 그러나 스마트 미디어는 구매 후 이용자에 의하여 설치되는 모바일 앱이 증가함에 따라, 앱 개발자와 공급자가 모바일 개인정보보호에 있어서 중요한 문제로 부각되었다.

모바일서비스 환경에서 새롭게 일어날 수 있는 개인정보보호의 문제는 국내에 국한되지 않는다. 유럽연합은 모바일서비스의 개인정보보호를 효율적으로 다룰 수 있는 법 제정의

필요성을 느끼고 2009년부터 모바일 기술에 따른 관련법 개정안을 연구하고 있다. 유럽위원회는 개인정보 접근성을 비롯한 정보주체의 권리가 보장되지 못하는 것에 대하여 우려를 표명한 바 있으며, 제29조작업반(Article 29 Working Party) 역시 유럽연합에서 증가하고 있는 모바일 개인정보에 대한 우려를 반영하여, 1995년 채택된 기존의 개인정보지침을 재해석하고 모바일 개인정보 처리에 대한 책임소재의 파악을 하기 위하여 노력하고 있다. 1998년 개인정보보호법을 제정한 영국은 모바일 기기가 차세대 주요 인터넷 접속장비로서 이용될 것이라는 전제 아래, 이용자들이 자신의 휴대기기를 스스로 프로그래밍하기 어렵다는 사실에 근거하여 사생활 보호에 대한 대책이 모바일 기술의 발전과 동시에 이루어져야 한다는 입장을 취하였다. 유럽연합의 통합적 규율과 달리, 민간자율형 규율을 채택하고 있는 미국은 개인정보보호를 포괄하여 다루는 법이 존재하지 않는다. 그러나 최근 모바일 서비스 환경에 따른 프라이버시 침해 논란이 증가하자 미국 국회는 「온라인 추적 금지법」(Do-Not-Track Online Act of 2011), 「위치사생활 보호법」(The Location Privacy Protection Act) 등과 같은 모바일 개인정보 관련입법을 추진하고 있다.

모바일 개인정보 처리에 대한 이용자 인식도 조사는 개인정보 처리에 대한 동의 절차, 개인정보 취급방침의 접근성, 최근 논란이 되고 있는 모바일 앱 프로그램의 형식적이고 고압적인 개인정보 처리에 대하여 이용자의 전반적인 인식을 파악하기 위하여 실시되었다. 이용자 인식도 조사는 모바일 환경에서 이용자의 개인정보자기결정권이 확보되어 있지 않다는 문제를 드러냈다. 정보통신서비스 제공자에 의하여 형식적으로 제시되는 모바일 동의절차는 이용자로 하여금 동의 절차에 대한 관심을 잃도록 유도하고 있다. 뿐만 아니라, 대다수의 이용자는 자신의 동의로 인하여 정보통신서비스 제공자의 개인정보 처리가 적법한 처리가 된다는 사실을 인식하지 못하고 있었다.

개인정보 취급방침 역시 많은 문제를 드러냈다. 개인정보 취급방침을 읽지 않거나 숙지하지 않는 이용자의 수가 절대적으로 많았고, 이는 자신의 개인정보가 언제 누구에게 어느 범위까지 알려지고 또 이용되도록 할 것인지를 이용자가 인지하고 스스로 결정할 수 있는 가능성을 배제한다는 점에서 심각한 문제이다. 또한 대부분의 이용자가 실제 처리되는 자신의 개인정보에 무엇인지 알지 못하는 반면, 개인정보 제공에 대하여 스스로가 설정한 허용기준은 엄격하여 이용자의 보호의식과 실제 처리되는 개인정보의 현실 사이에 많은 차이가 존재한다.

최근 급속도로 성장하고 있는 기술을 바탕으로 선보이고 있는 개별 정보통신서비스 제공자의 다양한 모바일서비스는 전혀 다른 새로운 개인정보의 처리양태를 보이고 있다. 이용자 인식도 조사는 이용자의 관점에서 새로운 기술의 출현이 개인정보보호의 기준을 스스로 설정함에 있어서 혼란을 가져올 수 있다는 사실을 반영하고 있다. 즉, 이용자는 새로운 모바일서비스를 이용함에 있어서 특정 정보가 자신 혹은 타인의 개인정보인지에 대하여 확신을 가지고 있지 못하였다.

모바일 개인정보보호의 문제는 국내외 사례에서도 드러나고 있다. 증권정보 모바일앱 ‘증권통’ 사건은 모바일앱 제공자가 개인정보 처리에 있어서 어떠한 처리가 위법을 구성하는지에 대하여 확신을 가지고 있지 못하다는 사실을 부각시켰다. 즉, 단말기 고유번호의 자동수집과 같은 기준에 존재하지 않았던 정보 처리 행위에 대하여 개인정보의 범위와 보호대상이 모호하다는 문제가 발견되었다. 카카오톡의 과도한 개인정보 수집에 대하여 방송통신위원회를 대상으로 이루어진 국가인권위원회의 권고는 적법한 동의 절차의 기준이 명확하지 못하다는 문제를 제기하였다. 또한, IT기업의 위치정보 수집에 대하여 내려진 방송통신위원회의 행정처분은 위치기반서비스사업자의 기술적 조치가 어느 정도까지 이루어져야 하는지에 대하여 아직까지 법적기준이 명확하게 마련되어 있지 않다는 문제를 드러냈다. 마지막으로, 본 연구는 모바일 개인정보보호에 대한 적용 법률의 파편화 문제를 지적하였다. 사례에서 나타난 바와 같이, 모바일 기기는 위치정보의 수집이 가능하다는 점에서 「위치정보보호법」, 무선랜을 이용한 네트워크가 가능하다는 점에서 「정보통신망 이용 및 촉진에 관한 법률」, 개인정보를 처리한다는 점에서 「개인정보보호법」이 적용 가능하다. 개인정보보호법 제6조와 같이 관련법의 적용 순위에 차등이 부여되고 있다 하더라도, 이처럼 적용 가능한 법의 파편화는 법적안정성을 저해할 수 있다. 담당기관의 혼재 역시 문제가 된다. 현재 개인정보관련법제에서 권한을 위임하고 있는 담당기관은 방송통신위원회, 행정안전부, 한국인터넷진흥원, 한국정보화진흥원 등 여러 기관으로 혼재되어 있다. 다수의 담당기관이 혼재되어 있다는 사실은 복잡하고 비효율적인 관할의 단점을 드러내고 있으며, 이는 개인정보보호와 관련된 행정을 정보보호위원회(Information Commissioners Office)로 하여금 총괄적으로 다루도록 권한을 위임하고 있는 영국의 개인정보보호법제와 대조된다.

설문조사와 사례를 통해 드러난 모바일 개인정보보호의 문제는 크게 여섯 가지로 구분

된다. 첫째, 새로운 기술에 따른 모바일 개인정보 처리를 규율하기에는 모바일 개인정보의 범위와 그 적용대상이 모호하다. 둘째, 형식적이고 강압적인 동의 획득 절차는 개인정보 처리에 있어서 이용자의 실질적인 통제를 배제하고 있다. 셋째, 개인정보 취급방침의 낮은 실효성과 접근성은 이용자로 하여금 개인정보 처리의 내용을 구체적으로 확인하고 개인정보 자기결정권을 확보함에 있어 걸림돌이 된다. 넷째, 모바일 환경에서 선택적 동의 제도가 정착되지 않음에 따라 개인정보의 과도한 수집이 이루어지고 있다. 다섯째, 개인정보처리가 처리하는 위치정보와 같은 행태정보는 모바일서비스에서 개인정보 제3자 제공의 형태로 빈번히 일어나므로 이에 대한 강화된 보호가 요구된다. 여섯째, 담당기관의 혼재와 적용법의 파편화는 개인정보보호와 그 피해에 대한 책임소재를 불명확하게 만들고 이용자로 하여금 혼란을 가중시킨다.

개인정보보호법의 경우, 위반에 대한 제재 수단으로 형벌을 규정하고 있다는 점에서 형벌이 적용되는 규정들은 형사특별법적 성격을 가진다. 따라서 개인정보라는 구성요건이 불명확하다면 이는 죄형법정주의의 명확성 원칙에 위배될 가능성이 있다. 위치정보의 경우, 모바일기기로부터 수집될 수 있는 위치정보는 일률적으로 개인위치정보 및 개인정보에 해당한다고 단정지을 수 없으며, 향후 사안별로 식별가능성 여부를 검토하여야 할 것이다. 개인정보보호법제의 인적·장소적 적용범위에 대한 평가는 모바일기기가 가지는 이동성에 근거한다. 모바일서비스 제공자나 이용자가 해외에 있는 경우에 국내법의 적용 가능성 여부가 문제되고, 이에 따라 형사사법공조 절차의 활용과 개인정보보호법의 역외적용 가능성 등의 문제가 고려되어야 한다.

적법하고 정당한 동의 획득 절차는 모바일 개인정보 보호의 핵심적 내용이다. 이용자의 동의는 모바일서비스 제공자의 개인정보 처리를 적법하게 만드는 구성요건에 해당하기 때문이다. 이에 따라 모바일서비스마다 상이한 동의 절차를 통일하고 무선랜의 특성을 활용한 사전 동의의 효율적 확보가 이루어져야 할 것이다. 또한 선택적 동의 제도의 효율적인 정착을 위하여 필수항목과 부가항목을 명확히 구분하는 기준이 되는 개인정보 처리 목적에 대한 원칙을 수립하고, 적법하지만 정당하지 못한 방법으로 처리되는 개인정보의 과도한 수집과 이용을 방지하기 위한 개선안을 마련할 필요가 있다.

개인정보보호법에서 규정하고 있는 개인정보파일 등록의 의무와 개인정보 영향평가는 그 대상이 공공기관으로 한정되어 있다는 문제가 있다. 구(舊) 「공공기관의 개인정보보호

에 관한 법률」이 폐지되고 개인정보보호법이 제정된 것은 민간부문과 공공부문을 가리지 않는 통합적 규율을 통하여 개인정보에 대한 보호범위를 넓히기 위함이다. 특히, 개인정보 보호법시행령에서 규정하고 있는 개인정보 영향평가의 대상은 100만 명 이상의 개인정보를 처리하는 공공기관인데, 유명 모바일앱의 경우 이용자의 수가 100만 명을 상회한다는 사실은 개인정보 영향평가 대상이 민간부문으로 확장될 필요성을 제기하고 있다.

모바일서비스에 특화된 개인정보 취급방침의 정비는 이용자의 개인정보가 어떻게 처리되는지, 언제 누구에게 어느 범위까지 처리되는지에 대하여 이용자가 한눈에 알아보고 수시로 확인할 수 있도록 그 접근성이 제고되어야 한다. 이에 따라 구체적이고 세부적인 가이드라인을 채택하여, 개인정보 취급방침의 형식을 통일하고 작은 모바일 화면에서 나타나는 까다롭고 복잡한 공개방식을 간소화할 필요가 있다.

제3자 제공시 동의의 방식과 범위에 대하여 현행법의 규율은 강화되어야 한다. 특히, 개인정보의 제3자 제공이 이루어지는 시점에 정보주체가 그 사실을 인지할 수 있도록 하는 방안이 마련되어야 한다. 영국의 개인정보보호법은 우리 법제와 달리 정보주체가 아닌 다른 자로부터 개인정보를 수집하는 경우, 제공받은 자는 개인정보처리자로서 개인정보 제공에 대한 사항을 정보주체에 반드시 알리도록 규정하고 있다.

모바일서비스의 발전과 확산에 따른 개인정보보호의 문제는 완전히 새로운 문제이기보다는 기존의 문제들이 더욱 부각되는 양상을 보인다. 따라서 모바일 개인정보의 문제는 모바일서비스에 특화된 개별 입법을 통하여 다루어질 것이 아니라 현행 개인정보보호법제를 통하여 일괄적으로 규율되어야 한다. 가장 중요한 문제는 모바일 환경에서 일어날 수 있는 기술적이고 전문적인 개인정보 처리의 문제를 현행법의 내용으로 포섭할 수 있도록 명확한 법적 기준을 마련하는데 있다.

5. 정책적 활용 내용

모바일서비스의 발전과 확산에 따른 개인정보보호의 문제는 완전히 새로운 문제이기보다는 기존의 문제들이 더욱 부각되는 양상을 보인다. 따라서 모바일 개인정보의 문제는 모바일서비스에 특화된 개별 입법을 통하여 다루어질 것이 아니라 현행 개인정보보호법제를 통하여 일괄적으로 규율되어야 한다. 가장 중요한 문제는 모바일 환경에서 일어날 수 있

는 기술적이고 전문적인 개인정보 처리의 문제를 현행법의 내용으로 포섭할 수 있도록 명확한 법적 기준을 마련하는데 있다.

본 연구의 결과에 따라 적법하고 모바일서비스를 이용자가 이용하는 과정에서 적법하고 정당한 사전 동의 절차의 확립과 현재 개별 모바일서비스 제공자마다 다른 개인정보 취급 방침을 정비하는 정책적 효과를 거둘 수 있다. 또한 개인정보파일등록에 대한 의무와 개인정보 영향평가의 시행과 관련된 정책적 개선과 함께 개인정보의 제3자에 대한 제공의 보호를 이끌어낼 수 있다.

6. 기대효과

본 연구는 영국과 미국 등 다른 국가와의 비교연구를 통하여 국내 현행법의 문제점을 파악하고, 현행법이 보호하지 못하는 모바일서비스의 특유의 현실을 반영하여 합리적인 개인정보처리의 기준과 개선방안을 제시하기를 기대한다. 방송통신위원회 등 개인정보보호와 관련된 감독기관이 가이드라인을 채택함에 있어서 참고할 수 있는 자료로서 활용될 뿐만 아니라, 모바일서비스 이용자가 정보주체로서 권리의식을 가지게 도와주고, 적용 가능한 관련 법규의 무지로 인하여 법적 혼란을 겪을 수 있는 모바일서비스 제공자에게도 긍정적인 가이드 역할을 하기를 기대한다.

SUMMARY

Rapid mobile technological development has profoundly change the nature of personal data processing and brought new challenges for the protection of personal data. The mobile technology allows individuals to share information about their behavior and preferences easily and make it publicly and globally available on an unprecedented scale. At the same time, ways of collecting personal data have become increasingly elaborated and less easily detectable.

To address this challenge, this research reviews the current legal framework whether it comprehensibly regulate mobile personal data protection. In Chapter II, this paper examines ways of collecting personal data throughout mobile devices such as smart phone and tablet PC. Main concern is that the notion of personal data is vague in areas of mobile service industry. For instance, IMEI serial number may fall within the scope of data protection laws when the entity processing them has a realistic possibility of linking them to a given individual.

Chapter III explores into current problems occurred in mobile service based on public survey on users' prospective and several legal cases. The former investigates consumers' attitudes and perceptions about privacy issues related to using mobile services on their mobile devices. Key questions addressed include how mobile users feel about their privacy and how specific elements users are most concerned with. The survey result analyzes the needs of legal measures providing transparency of data processing. This Chapter also points out current legal problems derived from several cases; the link between the concept of personal data and current legal norms is unclear.

Chapter IV seeks reform of the current legal system targeting ongoing problems. It first examines the current legal regimes focusing on their scopes and legal definition to argue that the role of each regulation in accountability and enforcement is not consistent with each other. As to consent procedure, this paper suggests lawful and

legitimate principle of data protection to increase transparency for data subjects and prevent excessive personal data collection. Transparency is fundamental condition for enabling users to exercise control over their own data and to ensure effective protection of personal data. Moreover, this paper proposes effective ways of improving the access to privacy policy for users. It is essential that individuals are well and clearly informed by data controller about how and by whom their data are collected and processed for what reasons, for how long and what their rights are if they want to access, rectify or delete their data. Increasing transparency also copes with notification process. Compared to the U.K. Data Protection Act, Korean law holds only public authorities accountable for notification process. This paper emphasizes the need of expanding such process covering all data controllers and also introduces specific obligations for data controller on the transfer personal data to third parties.

CONTENTS

Chapter 1. Introduction

1. The Purpose and Scope of the Study
2. Research Methods
3. Terminology

Chapter 2. Processing of Personal Data in Mobile Services

1. Smart Media and Personal Data Protection
2. Ways of Personal Data Collection and Processing

Chapter 3. New Challenges for Mobile Data Protection

1. Legislation Trend in Other States
2. User Survey Analysis
3. Cases Analysis
4. Intermediate Conclusion

Chapter 4. Approaches to Reform Current Legal System

1. An Overview of Applicable Laws to Mobile Data Protection
2. Scopes and Conditions of Current Legal Regimes
3. Lawful and Legitimate Consent Procedures

4. Notification and Preliminary Assessment
5. Privacy Policy Specialized in Mobile Services
6. Personal Data Transfer to Third Parties

Chapter 5. Conclusion

제1장 서론

1. 연구의 배경과 목적

2011년 말 현재 국내 스마트폰 가입자 수가 천만 명을 넘어섰다. 스마트폰을 비롯한 스마트 모바일기기 사용의 확산은 통신서비스 이용자들에게는 다양한 서비스를 편리하게 이용하는 것을 가능하게 하였으며, 서비스 제공자의 입장에서는 다양한 정보를 이용해 개별 이용자에 대한 맞춤형 서비스를 제공하는 것을 가능하게 하고 있다. 그러나 개인의 다양한 정보를 담고 있는 스마트 모바일기기 사용의 확산은 정보통신기술의 발전에 따른 프라이버시 침해를 가속화시킬 수 있는 위험을 함께 증대시키고 있다.

본 연구의 목적은 기술 발전에 따른 새로운 환경에 대응하여 이로 인해 새롭게 제기되는 문제점을 현행 법체계 내에 포섭시키기 위한 방안을 도출함에 있다. 스마트폰 등 새로이 등장한 스마트 모바일기기는 많은 정보를 담고 있으며, 이러한 정보는 기존의 오프라인이나 온라인 상에서 정보주체가 직접 자신의 정보를 제공하는 방식과 달리 응용 프로그램의 설치, 구동에 따라 자동적으로 기기 내 저장된 정보를 추출하여 정보통신서비스 제공자의 서버로 전송하는 것을 가능하게 한다. 또한 일회성 정보 제공으로 정보 수집 절차가 종료되던 기존의 방식에 비하여 모바일 애플리케이션에서의 정보 수집은 최신 정보의 주기적 혹은 지속적인 업데이트가 이루어질 수 있다. 이와 같은 기술적 변화는 정보 수집에 대한 정보주체의 인지 및 통제 가능성을 약화시킬 수 있으며, 이러한 상황을 예정하지 아니한 현행 법체계에서 정보주체의 자기결정권 보호에 허점이 발생할 것으로 예상된다.

또한 「개인정보보호법」을 비롯해 「정보통신망 이용 및 촉진에 관한 법률」 등 현행 개인정보보호법제는 매우 강력한 처벌 규정을 두고 있으며, 적용대상이 광범위하다.¹⁾ 그러나 모바일 환경에서의 개인정보 침해는 피해자들이 인지하지 못하는 “숨은

1) 개인정보보호법의 발효로 적용대상은 기존에 정보통신망법 적용대상 49만 사업자, 「공

범죄”인 반면에 강력한 처벌에 비례하는 강력한 집행을 위한 제도는 정비되지 않고 있다.

본 연구는 모바일서비스에서 발생하는 문제점을 현행 법체계 내에서 해결할 수 있는 방안을 찾는 데 주안점을 두고 진행하였다. 다만 우리 개인정보보호 법제는 정보주체를 보호하기 위한 법률이며, 신설 개인정보보호법은 산재된 법률의 통일적 규율을 목적으로 하고 있다. 따라서 최종적으로는 새로운 특별법의 제정이나 현행법의 개정보다는 현행 규정의 해석과 시행령, 가이드라인 등을 통해 허점을 보완하고 집행결손을 보완하기 위한 정책적 조치를 해결책으로 제시하고자 하였다.

2. 연구의 방법 및 주요 내용

본 연구는 다음의 3단계로 진행되었다.

1단계	모바일서비스의 개인정보 이용양태 분석
	<ul style="list-style-type: none">• 국내 모바일 애플리케이션 및 중개 마켓 현황 분석• 모바일 애플리케이션에서 수집하는 정보의 유형 및 이용행태 분석

제2장에서는 국내외 스마트 모바일기기의 보급 현황과, 모바일서비스상에서 수집/이용되거나 향후 수집/이용이 가능한 개인정보의 유형, 수집방법을 분석한다. 이를 위해 국내에서 서비스되고 있는 대표적 애플리케이션이나 모바일웹서비스의 이용약관, 개인정보 취급방침을 분석하고 해당 프로그램이 모바일기기의 개인정보에 접근하게 되는 기술적 과정을 살펴보고 그 과정에서 이용자가 권한을 통제할 수 있는 범위가 어디까지인지 살펴본다. 또한 국내에서 가장 많은 애플리케이션 다운로드를 기록하고 있는 대표적 애플리케이션 마켓의 현황과 앱 설치과정 및 앱의 판매 과정을 분석한다.

공기관의 개인정보 보호에 관한 법률」의 적용대상 2만 5천 기관에서 등에서 민간사업자 310만명이 추가된 350만 사업자로 확대되었다.

2단계

모바일서비스 개인정보 이용시 문제점 분석

- 설문조사를 통한 이용자 인식도 조사 결과 드러난 문제점
- 사례를 통해 드러난 문제점
- 외국의 대응입법 동향에서 언급되는 문제점

제3장에서는 모바일서비스 제공시 개인정보보호가 문제되는 경우를 분석한다. 모바일 기기의 확산에 따른 새로운 문제는 우리나라 뿐 아니라 유럽과 미국 등 개인정보보호의 선진국에서도 활발히 제기되고 있는 문제로, 이를 참고하여 모바일서비스 이용자들의 인식도 조사와 국내외 사례를 통해 모바일서비스에서 고유하게 발생하거나 심화되는 개인정보보호의 문제점을 도출한다. 이용자 관점에서 인식되는 문제점은 자체 설문조사를 중심으로 최근 미국에서 실시된 미국 내 소비자들의 모바일서비스 개인정보에 대한 인식도 조사를 통해 밝힌다. 또한 모바일기기를 통한 개인정보 수집 및 제3자 제공이 문제되었던 사례로부터 문제점을 도출한다.

3단계

현행 국내법 체계내 포섭 여부 판단

- 설문조사와 사례를 통해 제기되는 문제점들이 현행법 내에서 규율될 수 있는지 여부에 대한 판단
- 포섭되는 경우 집행결손의 해소 방안 제시
- 포섭되지 않는 경우 대안 제시

제4장에서는 신설 개인정보보호법, 「정보통신망 이용 및 촉진에 관한 법률」(이하 “정보통신망법”이라 함), 「위치정보의 보호 및 이용 등에 관한 법률」(이하 “위치정보법”이라 함) 등 개인정보보호에 관한 현행 국내법규범이 제3장에서 제기된 문제점들을 충분히 포섭할 수 있는지를 분석하는 데 주안점을 둔다. 즉 이와 같은 현행 규범들이 모바일서비스에서 제기되는 개인정보보호 문제에 적용될 수 있는지 분석하고, 앞선 장들의 결과를 바탕으로 현행 국내법의 문제점을 도출한다. 또한 모바일서비스의 하드

웨어적, 미디어적 특성에 따른 법제도의 정비 논의는 비단 우리나라 뿐 아니라 유럽과 미국을 비롯한 선진국들에서도 화두가 되고 있는 바, 선진적 개인정보보호 법제를 가진 이들 국가들에서의 논의를 참고하여 우리 법제의 개선에 줄 수 있는 시사점을 도출한다.

3. 주요 용어의 정의

1) 모바일기기

본 연구에서 다루는 모바일기기 혹은 단말기라 함은 데이터통신과 정보처리 능력을 가진 휴대용 통신기기를 의미한다. 대표적인 모바일기기에는 스마트폰이 있다. 스마트폰이란 “일반 PC와 같이 고기능의 범용 운영체제(OS)를 탑재하여 다양한 모바일앱(Mobile App)을 자유롭게 설치·동작시킬 수 있는 고기능 휴대폰”²⁾, 또는 “휴대폰에 컴퓨터 지원기능을 추가한 지능형 휴대폰”³⁾으로 정의된다.³⁾ 스마트폰은 휴대폰 기능에 충실하면서도 PDA 기능, 인터넷 기능, 리모콘 기능 등이 일부 추가되며, 수기방식의 입력장치와 터치 스크린 등 보다 사용에 편리한 인터페이스를 갖춘다. 또한 무선 인터넷 기능의 지원으로 인터넷 및 컴퓨터에 접속되어 이메일, 웹브라우징, 팩스, banking, 게임 등 단말기로서의 기능도 수행한다. 다양한 기능의 수용을 위하여 표준화된, 또는 전용 운영체제(OS)를 갖추기도 한다. 2010년 한 해 동안 총 45종이 출시되는 등 국내에 출시된 스마트폰은 삼성전자의 옴니아, 갤럭시 시리즈, 애플의 아이폰, 엘지전자의 옵티머스, HTC사의 디자인어 시리즈, RIM사의 블랙베리 시리즈 등 매우 다양하다.

삼성전자의 갤럭시탭과 애플사의 아이패드로 대표되는 태블릿 PC 역시 데이터통신 기능과 휴대성을 갖추고 있어 모바일기기의 또다른 예가 된다. 이들 기기에서도 역시 스마트폰과 동일한 방식으로 모바일 애플리케이션을 이용한다.

더불어 무선데이터 통신이 가능하며 애플리케이션을 설치, 이용할 수 있는 아이팟과 같은 일부 MP3 플레이어나 모바일 운영체제를 바탕으로 하는 내비게이션 등도 본 연구

2) 방송통신위원회, 『2011년 상반기 스마트폰이용실태조사』, p. 1.

3) 정보통신용어사전(한국정보통신기술협회)(<http://word.tta.or.kr/index.jsp>).

의 대상이 되는 모바일기기에 포함된다.

2) 애플리케이션

응용 프로그램(application program)은 운영 프로그램(operating program)에 대비되어 특정 운영체제를 기반으로 작업 수행을 돕기 위해 설계된 프로그램을 의미한다. 어떤 종류의 작업 수행을 돕기 위해 설계된 컴퓨터 프로그램을 의미한다. 줄여서 애플리케이션 또는 앱이라고도 한다. 애플리케이션은 컴퓨터를 작동시키는 운영 체제, 애플리케이션의 실행에 도움을 주고 컴퓨터 시스템의 유지 관리를 지원하는 유틸리티 및 프로그램을 작성하는 언어와 구별된다.⁴⁾

본 연구의 목적상 애플리케이션이라 함은 별도의 설명이 없는 한 모바일 애플리케이션을 지칭한다. 모바일 애플리케이션이란 스마트폰에 최적화된 응용소프트웨어로서 메신저, 게임, e-book, 내비게이션 등 다양한 서비스를 제공하며, 애플리케이션 마켓을 통해 이용자는 자신이 원하는 모바일 앱을 구입하고 스마트폰에 추가하여 이용할 수 있다.⁵⁾

3) 애플리케이션 마켓

애플리케이션 마켓은 “스마트폰 등 휴대전화에 필요한 애플리케이션을 거래하는 사이트”를 의미한다.⁶⁾ 애플리케이션 마켓은 앱스토어, 애플리케이션 마켓 플레이스, 앱마켓 등 다양한 용어로 일컬어진다. 애플사의 앱스토어(App Store)가 대표적인 앱마켓으로, 아이폰 확산의 주된 계기가 되었으며, 구글 안드로이드 운영체제를 사용하는 스마트기기의 점유율 증가로 안드로이드 마켓 역시 주요 앱마켓의 예가 된다. 국내에서는 티스토어와 올레마켓 등 이동통신사에 의해 운영되는 애플리케이션 마켓이 있으며, 그 외 노키아를 비롯해 마이크로소프트(MS) 리서치 인 모션(RIM), 삼성전자 등이 독자적인 모바일 앱마켓 사이트를 구축하고 있다.

4) *supra* note 3.

5) *supra* note 2, p. 1.

6) *supra* note 3.

제2장 모바일서비스의 개인정보 이용 양태

제1절 스마트 미디어와 개인정보 보호

1. 스마트 모바일기기 보급 현황과 전망

전세계적으로 스마트 모바일기기는 절대적 수에 있어서나 전체 모바일기기 중 상대적 비중에 있어서 급격히 증가하는 추세를 보이고 있으며, 이러한 추세는 향후 계속될 것으로 보인다. 2011년 현재 보급된 스마트 미디어는 약 56억 대로, 이는 작년의 약 50억 대에 비하여 11% 정도 증가한 것이다.⁷⁾ 시장조사기관 가트너의 발표에 따르면 2015년 전세계적으로 보급될 모바일기기의 수는 74억대로 세계 인구수를 추월할 것으로 전망되었다.⁸⁾

스마트폰의 경우 같은 기간 연평균 24%의 매출 성장을 기록하며 약 25억대가 판매될 것으로 예측되었다.⁹⁾ 2010년 전세계에서 판매된 스마트폰은 2억3백만대를 넘어섰으며, 2011년에는 3억대 이상, 2015년에는 연간 6억1,900만대가 판매될 것으로 예상된다.¹⁰⁾(그림 2-1 참조) 특히 중국과 중남미, 동유럽이 각각 연평균 29%, 33%, 25%의 매출 성장을 기록하며 이와 같은 증가세를 주도할 것으로 전망되었으며, 북미와 서유럽, 중동, 아프리카의 경우 상대적으로 낮은 성장세를 보이겠지만 여전히 20% 이상을 기록할 것으로 전망되었다.¹¹⁾

7) 아이뉴스, “세계 모바일 기기 56억대... 전년 비 11% up”, 2011. 8. 5.

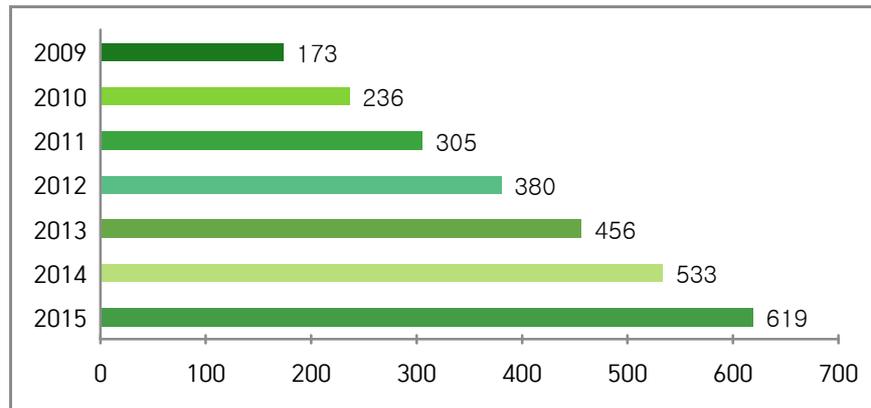
8) *Ibid*

9) Coda Research Consultancy, Worldwide Smartphone Sales Forecast to 2015, (<http://www.codaresearch.co.uk/smartphoneworld/>) .

10) *Ibid*

11) *Ibid*

<그림 2-1> Global Smartphone Sales Will Grow at +24% CAGR (단위: 백만)



출처: Coda Research Agency, 2010

상대적으로 스마트폰의 보급이 늦었던 국내시장의 경우, 방송통신위원회가 2008년 말 무선인터넷 표준 플랫폼인 위피 탑재 의무를 폐지하고 2009년 말 애플의 아이폰이 국내 시장에 출시되면서 스마트폰 보급률이 급격히 높아지게 되었다. 각 이동통신사의 집계 에 따르면 현재 국내 스마트폰 가입자 수는 2011년 3월 기준으로 천만명을 넘어섰으며, 이는 2009년 말의 80만 명, 2010년 6월의 247만명에 비하여 상당히 높은 수치이다. 같은 기간 일반이동전화 가입자 수의 증가는 총 322만여 명에 그쳐 전체 가입자 대비 스마트폰 가입자의 비중은 더욱 급격하게 증가하였다.(<표 2-1> 참조)

방통위는 2011년 말 스마트폰의 가입자 수가 2천만 명을 넘어서고, 전체 이동전화 가

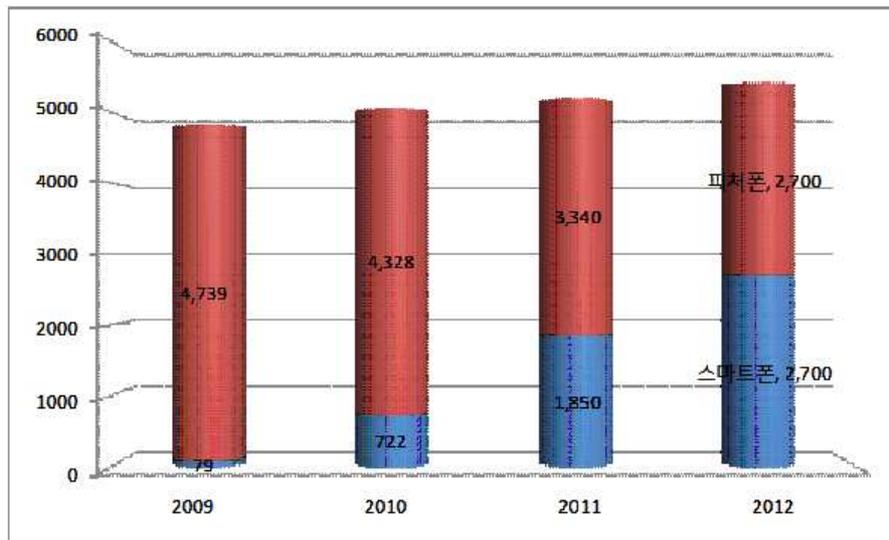
<표 2-1> 국내 스마트폰 가입자 현황 (단위 : 만명, %)

구분	'09.12월	'10.3월	'10.6월	'10.9월	'10.12월	'11.2월
이동전화 가입자(A)	4,794	4,898	4,961	5,021	5,077	5,116
스마트폰 가입자(B)	80	152	247	442	722	926
비중(B/A)	1.7	3.1	5.0	8.8	14.2	18.1

(출처: 방송통신위원회, 스마트폰 관련 통계 현황, 2011)
 입자 대비 비중이 약 37%에 달할 것으로 예상하고 있으며,¹²⁾ 2013년까지 누적 3천만명

이상, 2015년에는 4천만명에 이를 것으로 전망하고 있다.¹³⁾ 이동통신사별 스마트폰 가입자 수는 2010년 10월 기준에서 SKT가 25,498,497명의 가입자를 보유하여 전체의 50.7%를 차지하였고, KT가 15,871,634명(31.5%), LG텔레콤이 8,755,078명(17.8%)으로 그 뒤를 이었다.

<그림 2-2> 국내 휴대폰 및 스마트폰 가입자 전망



출처: SK Marketing & Company

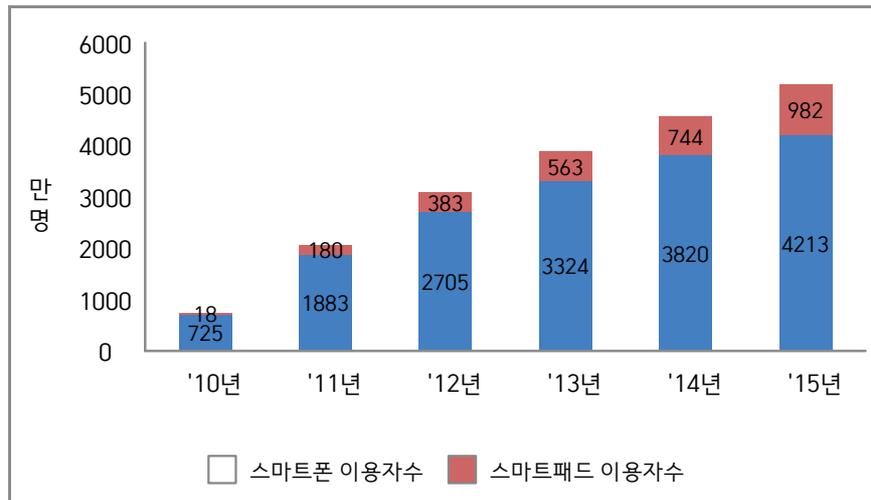
또한 태블릿PC 이용자도 2010년 18만명에서 2015년 982만명으로 증가할 것으로 예상하고 있다.(<그림 2-3> 참조)¹⁴⁾

12) 방송통신위원회 보도자료(2011.3.24), “스마트폰 가입자 1,000만 돌파, 스마트 시대 본격 개막”.

13) 방송통신위원회, “Smart Korea 강국 도약을 위한 스마트 모바일 시큐리티 종합계획”, 2010. 12., p.4.

14) *Ibid*

<그림 2-3> 국내 스마트폰 및 스마트패드(누적) 보급 전망('10~'15년)



출처: 방통위, Smart Korea 강국 도약을 위한 스마트 모바일 시큐리티 종합 계획

이와 함께 스마트폰과 관련한 분쟁 건수도 지속적으로 증가하고 있는 추세이다. 최근 실시된 스마트폰 이용에 대한 만족도 조사에서 스마트폰 앱과 관련한 불만사항 중 주목할만한 것은 “개인정보가 새어 나갈 것 같은 불안감이 있다”는 항목에 답한 비율이 23.0%에 달한다는 점이다.¹⁵⁾ 개인정보 유출이 우려되는 경로로는 모바일 애플리케이션을 통한 유출, 모바일 금융 서비스 이용을 통한 유출, 기기 분실로 인한 유출이 지목되었다.¹⁶⁾

2. 스마트 미디어의 특성

모바일서비스는 기존의 단순 통화 중심의 이동전화 서비스에서 스마트 미디어를 통한 복합적 성격으로 발전하였다. 이는 스마트 미디어 자체의 하드웨어적 성격 변화와, 이용자들의 이용 양태 변화의 두 가지 측면에서 살펴볼 수 있다.

15) 한국정보통신진흥협회, “이용자 관점의 스마트폰 이용실태분석 및 사후규제방안 연구”(2010. 12. 31.), pp.45-47.

16) *Ibid*

가. 스마트 미디어의 하드웨어적 특성

기존의 피쳐폰(feature phone)과 비교하였을 때, 스마트폰은 다음과 같은 특징을 갖는다.

우선 스마트폰은 PC와 유사한 하드웨어 구성을 갖는다. OS와 애플리케이션의 데이터 처리를 위한 CPU와 기억장치, RAM을 가지고 있으며, 기술 발달로 인하여 초소형화된 이러한 부품들로 구성된다.

이러한 하드웨어를 바탕으로 스마트폰은 PC와 같이 안드로이드, iOS, 윈도우즈 모바일, 심비안 등의 범용 운영체제를 사용하여 애플리케이션이라 일컫는 프로그램들을 사용한다. 이로써 휴대폰의 이용 양태는 음성통화에서 데이터 트래픽으로 그 중심이 이동하게 되었다. 또한 범용 OS의 사용은 제3자가 개발하여 제공하는 애플리케이션을 사용하는 것이 가능하도록 하였다. 즉, 피쳐폰에서 사용되었던 카메라나 미디어플레이어 등의 기능은 휴대폰 기기에 부가적으로 장착된 것이었던 데 반해, 스마트폰의 멀티미디어 기능은 자체적인 프로그램의 실행으로 가능하게 되었다는 차이점을 보인다.

노트북 등 필요에 따라 와이파이 등을 통해 통신망에 접속하는 기기와 달리 항상 네트워크에 접속되어 있다는 점도 스마트폰이 갖는 중대한 차이점이다.

<표 2-2> 일반 피쳐폰과 스마트폰의 특성 비교

일반 휴대폰	스마트폰
보이스 중심 서비스 WIPI 기반 호스트만 접속 카메라, MP3 등 멀티미디어 기능 SMS/MMS 위주 제3자 앱 설치 불가	윈도우즈 모바일, 심비안, 안드로이드 등 범용 OS 멀티태스킹/데이터 중심 서비스 Wi-Fi, 블루투스 지원 풀 브라우징 서비스 제3자 앱 설치/사용 가능 서비스 오퍼레이션 인증 필요

(출처 : 스마트폰 활성화 방안과 이동통신사 애플리케이션 스토어 서비스 정책에 관한 연구)

나. 스마트미디어 도입에 따른 모바일기기 이용양태 변화

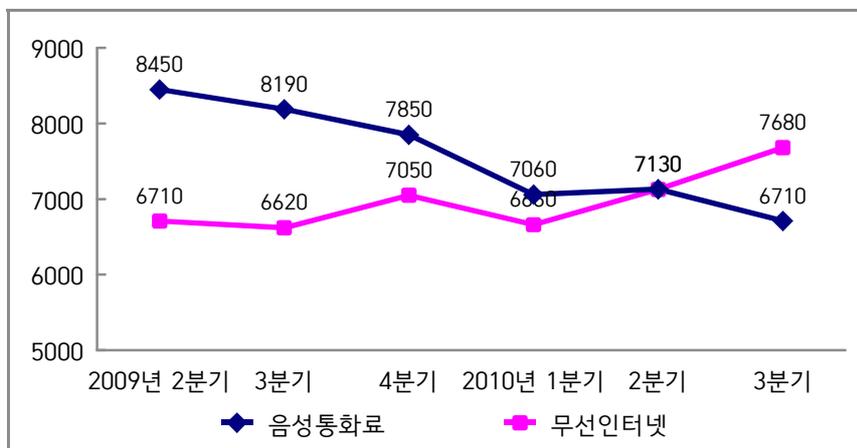
기존의 단말기에 비하여 처리 또는 저장될 수 있는 데이터 양이 비약적으로 증대하였으며, 다양한 응용프로그램(앱)의 설치를 통해 활용할 수 있는 범위가 넓어지면서 모바일기기 이용자들은 물론, 사업자들의 이용양태 또한 크게 변화하였다.

이용자 측면에서 가장 큰 변화는 단순한 통신 기능만을 주로 사용하던 양태에서 일정 관리, 이메일 관리, 문서 관리는 물론 GPS 기능을 이용한 이동거리, 시간 등의 기록 관리에 이르기까지 스마트 모바일기기가 일상생활과 업무에서 차지하는 비중이 크게 높아졌다는 점이다. 초창기 스마트폰이라 할 수 있는 블랙베리가 미국에서 성공을 거두었던 이유는 이메일 송수신 및 작성을 용이하게 함으로써 업무능력을 향상시키는 데 도움이 되었기 때문이며, 이후의 스마트폰은 이보다 더욱 확장된 기능을 갖는다. 따라서 90년대 PC통신에서의 채팅, 2000년대 초 인터넷 환경에서 이메일, 카페, 네이버 지식in 등과 같이 스마트 환경에서의 킬러앱¹⁷⁾이 활발히 이용된다. 모바일 환경에서의 소위 ‘킬러앱(killer-app)’에는 기존에 자리잡은 이메일 서비스 앱을 비롯해 트위터, 페이스북과 같은 SNS 앱, 오브제, T map, 지도서비스 등 위치기반서비스를 제공하는 앱, iCal, 구글 캘린더, 아웃룩 캘린더와 같이 모바일과 유선을 연동시켜 종합적인 일정관리 서비스를 제공하는 앱, 이동 중 문서작업을 가능하게 해주는 Air Sharing, Adobe Reader, 한컴 리더 등의 앱을 들 수 있다. 특히 카카오톡, Skype, 마이피플 등과 같이 데이터통신을 이용한 메신저 또는 음성/영상통화서비스는 이용자들의 요금 부담을 완화하여 통신 기능을 배가시키는 앱으로 카카오톡이 2,500만명, 마이피플이 2,000만명 이상의 가입자를 보유하는 등 많은 이용자를 보유하고 있다. 이러한 앱들은 기존 이동통신사업자들의 수입원이었던 음성통화와 단문메세지 서비스가 줄어들고 있어 앱개발사와 이동통신사업자

17) 킬러앱(killer-app)이란 시대적, 공간적으로 주로 사용되는 응용 프로그램(application program)으로 오랜 기간 시장을 지배하고 있던 경쟁자를 압도하고 시장에 나오자마자 기존의 사회 구조나 산업을 변화시키고 시장을 재편하는 것은 물론 완전히 새로운 카테고리를 형성하는 위력적 기술이나 서비스를 뜻하며, “킬러”라는 단어를 쓴 것은 “기존의 흐름을 완전히 바꾸어 놓으며, 여기에 적응하지 못하면 도태된다”는 것을 나타내기 위함이다.(한국정보통신기술협회 정보통신용어사전 참조, <http://word.tta.or.kr/index.jsp>)

들 사이의 갈등 요인이 되기도 한다. 또한 이와 같은 다양한 애플리케이션의 사용은 네트워크상 데이터의 교신 패턴 자체를 변화시키는 계기가 되었다. 즉 스마트기기의 활성화에 비례하여 데이터 트래픽은 계속하여 증대하고 있는 반면, 음성통화량은 상대적으로 감소하고 있는 경향을 보인다. 최근 국내 통신사업자들이 데이터 무제한 요금제를 폐지하려는 움직임을 잇달아 보이는 것도 이러한 이용양태 변화와 직접적 연관을 갖는다.

<그림 2-4> SK텔레콤 음성통화료 및 무선인터넷 사용량 변동 추이



사업자의 입장에서 스마트 모바일기기의 등장으로 기존 유선상에서 활용되던 것에 비해 개인의 성향을 더욱 정확히 반영한 온라인 행태정보 기반 광고(OBA: Online Behavioral Advertising, 이하 ‘행태기반광고’)가 가능하게 되었다. 개인의 모바일기에 설치된 애플리케이션을 통해 개인을 식별하여 각 개인의 위치에 따라 주변 상점을 홍보하는 서비스나 해당 기기에서의 브라우징 기록, 통화패턴, 애플리케이션 이용패턴 등을 수집, 분석하여 사용자가 관심을 가지는 상품이나 업종, 상표에 대한 광고를 제공하는 등 행태기반광고가 매우 활발히 활용되고 있다. 기존의 TV 또는 라디오와 같은 매체를 통한 마케팅은 이용자의 이용 시간에 따라 그 한계를 지니는 반면, 이용자가 항상

소지하고 있는 스마트폰을 통한 마케팅은 언제 어디서라도 이용자에게 항상 연결될 수 있다는 강점을 지니며,¹⁸⁾ 이용자가 인터넷 또는 해당 사이트에 접속하여 활동을 하는 경우 그 행태만을 분석하여 획득할 수 있는 행태정보에 비하여 항상 네트워크에 연결되어 있고 개인의 위치 등이 모두 접근가능한 모바일기기에서 획득되는 행태정보는 보다 특정되고 세분화된 마케팅 수단으로의 활용이 가능하다는 이점이 있다.¹⁹⁾ 이에 따라 모바일 행태기반광고는 마케팅을 하는 사업자에게는 필수적인 것으로 인식되고 있다. 미국 광고협회의 조사에 따르면 2010년 기준 마케팅 활동을 하는 전체 기업 중 62%가 모바일 마케팅을 활용하였으며, 2011년에는 추가로 26%의 사업자들이 모바일 마케팅을 활용할 의도를 가지고 있음이 확인되는 등 마케팅에서 모바일서비스의 활용은 점차 확대일로에 있다.²⁰⁾

18) 박정현, 스마트폰 시대의 모바일 마케팅, 한국마케팅연구원, 마케팅, 제45권 제1호 2011.1., 34쪽.

19) *Ibid*

20) Association of National Advertisers, *Vast Majority of Marketers will Utilize Mobile Marketing and Increase Spending on Mobile Platforms in 2011*, (2011. 1. 31.) www.ana.net/content/show/id/20953 참조.

제2절 모바일서비스를 통해 수집/이용되는 개인정보의 유형 및 수집방법

1. 개인정보의 유형별 분석

스마트 미디어를 통한 모바일서비스 이용 과정에서 다양한 개인정보가 수집/이용된다. 스마트폰의 경우 최근 애플 아이폰과 구글 안드로이드폰에 대해 문제가 제기되었던 바와 같이 기기 설계상 자동적으로 이용자의 개인정보가 수집되도록 하거나, 혹은 이동통신사업자가 통신서비스 가입시 기본적으로 설치되어 있는 앱 또는 이용 과정에서 이용자가 설치하는 앱의 설치/이용 과정에서 서비스 제공자에게 정보가 전송되도록 설정하는 것이 일반적이다. 스마트 모바일기기에 설치되는 앱의 상당수는 기기고유번호나 전화번호, 이용자의 위치정보, 주소록, 이용기록 등의 개인정보를 서비스제공자에게 전송하도록 설계되어 있다.

일반적으로 이러한 수집에 대해 이용자의 동의 절차를 거치고 있으나, 프로그램의 설치와 구동만으로도 정보의 전송이 가능하다. 이는 특히 동의 없이 개인정보를 수집하거나 동의된 범위를 넘어 개인정보를 수집하는 악성 프로그램을 통한 피해에 대한 우려를 낳는 이유가 된다. 이렇게 애플리케이션의 설치 또는 실행으로 모바일기기로부터 서비스공급자에게 전송되는 정보 중에는 개인정보보호법제상 보호되는 개인정보에 해당하는 경우도 있고 개인정보의 지위에 이르지 않는 경우도 있다. 또한 같은 유형의 정보라도 경우에 따라 개인정보가 되기도 하고 되지 않기도 하여 각 사안별로 개별적인 검토가 필요하다. 특히 각각의 정보만으로는 개인정보에 해당하지 않더라도 수집된 정보들을 결합하거나 웹페이지, 오프라인 등 다른 경로로 수집한 정보와 결합하여, 혹은 따로 이 구축된 데이터베이스와 결합하면 개인정보가 되기도 한다.

페이스북 앱은 우리나라 뿐 아니라 전세계적으로 기기나 OS에 관계없이 가장 많은 이용자를 보유하고 있는 앱으로, 다음의 내용은 페이스북 앱에서 접근할 수 있는 개인정보취급방침의 일부를 발췌한 내용이다.

■ 회원님께서 다른 사람의 프로필을 볼 때, 메시지를 보낼 때, 친구나 페이지를 검색할 때, 광고를 클릭하거나 Facebook 크레딧을 구입할 때 관련 데이터가 전달됩니다.

■ 사진, 동영상 등을 Facebook에 게시하실 때에는 사진이나 동영상을 찍은 시간, 날짜, 장소 등과 같은 추가 정보 전달될 수 있습니다.

■ 회원님께서 Facebook에 접속하기 위해 사용하시는 컴퓨터, 휴대폰 등의 도구로부터 데이터가 전달됩니다. 여기에는 회원님의 IP 주소, 위치, 브라우저 종류, 방문한 페이지 등이 포함될 수 있습니다. 예를 들어 친구가 근처에 있는지 알려드리기 위해 회원님의 GPS 위치를 파악할 수 있습니다.

■ 때에 따라 Facebook은 광고 게시, 온라인 활동 이해, Facebook 기능 개선에 도움을 주는 광고 파트너, 고객, 기타 제 3의 업체로부터 데이터를 받습니다. 예를 들면, 광고의 효과를 측정하고 광고 품질을 개선하기 위해 광고주로부터 회원님이 Facebook 또는 다른 사이트상의 광고에 대해 어떠한 반응을 보였는지 정보를 수집할 수 있습니다.

또한 Facebook은 회원님과 친구에 대해 이미 갖고 있는 정보로부터 데이터를 이용하기도 합니다. 예를 들어 뉴스피드에서 회원님에게 어떠한 친구를 보여주어야 하는지 정하거나 회원님이 게시한 사진에서 태그 추천을 하기 위해 회원님에 대한 데이터를 이용할 수 있습니다. 또한 GPS 정보가 있는 회원님의 현재 거주지 및 기타 위치 정보를 이용할 수 있습니다. 이를 이용해 회원님과 친구들에게 근처에 있는 사람들이나 이벤트에 대해 알리거나, 회원님이 관심있어할 일을 제공하기도 합니다. 또한 회원님과 관련이 있을 수 있는 광고를 보여주기도 합니다.

여기서 제시된 수집항목을 살펴보면 서비스제공자가 특정 정보에 한정되지 않고 이용자의 라이프스타일을 총체적으로 파악할 수 있는 다양한 정보를 모두 수집하고 있음을 확인할 수 있다. 이는 서비스제공자의 개인정보 수집목적은 단순히 해당 서비스의 제공을 위한 것에 한정하지 않고, 광고 등 마케팅 목적이나 사업확장을 위한 자료로 활용하기 위해 최대한 광범위하게 설정해 놓고 개인정보를 수집하고 있음을 보여주는 예이다. 따라서 서비스제공자가 특정 정보를 수집하더라도 경우에 따라서는 개인정보에 해당하거나 해당하지 않을 수도 있어 해당 정보가 개인정보인지의 여부는 그 정보와 결합할 수 있는 데이터베이스의 존재 유무, 수집된 정보를 바탕으로 서비스제공자나 개인정보

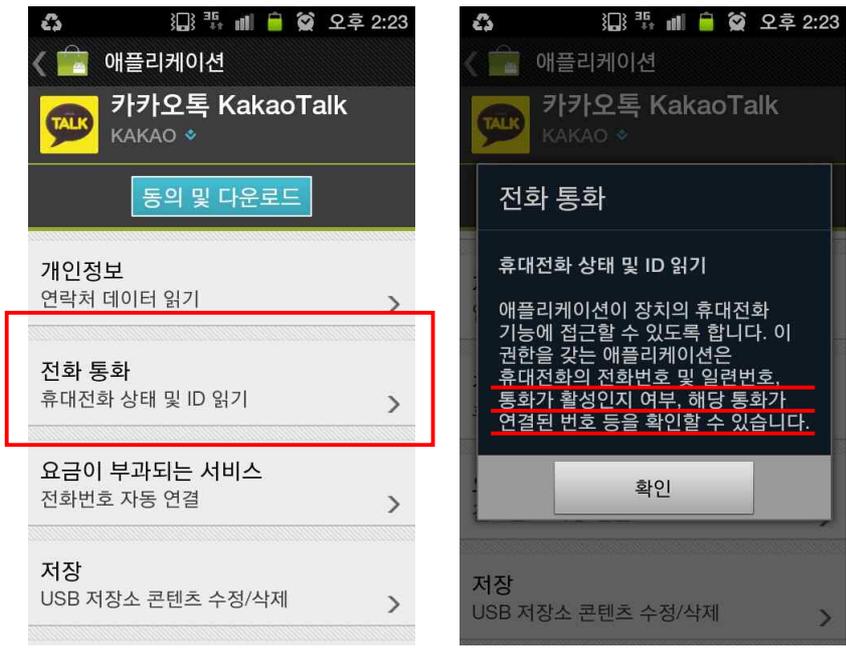
처리자가 새로이 생성한 데이터베이스의 존재 유무 등을 개별 사안에 따라 각각 판단해 결정지어야 한다. 여기서는 우선 애플리케이션의 이용에 따라 빈번히 수집되는 정보들을 유형별로 분류해 살펴기로 한다.

가. 기기 식별정보

스마트폰의 경우, 전화번호는 애플리케이션 마켓의 아이디와 같은 역할을 하기 때문에 접속한 기기의 전화번호는 기본적으로 마켓에 등록, 저장되게 된다. 이러한 정보는 기기를 식별하여 이용자의 앱 구매내역 관리 등에 이용된다. 또한 메신저나 기록이 유지되는 서비스와 같이 이용자를 식별할 필요가 있는 대부분의 애플리케이션의 경우, “휴대전화 ID 읽기” 권한이 활성화되어 있어 기본적으로 전화번호를 비롯해 IMEI(International Mobile Equipment Identity, 단말기 국제 고유 식별번호), IMSI(International Mobile Subscriber Identity, 국제 이용자 고유 식별번호) 등을 수집할 수 있다. 이러한 정보는 온라인 웹사이트에서의 ID와 같이 이용자를 식별하는 기능을 한다.

예를 들어 안드로이드 마켓에서 카카오톡을 다운받아 설치할 경우 이용자들은 <그림 2-5>와 같이 애플리케이션의 접근권한 허가에 대한 동의화면을 접하게 되며, 이 중 전화통화 항목을 클릭하면 오른쪽과 같은 부가적 설명이 주어진다. 이후 다음의 절차를 거치게 된다. 여기서 휴대전화의 전화번호, 일련번호, 통화가 연결된 번호 등을 확인할 수 있는 등 상당히 폭넓은 권한이 부여되는 것을 확인할 수 있다. 다만 이 때 제시되는 동의 화면은 다운로드시 해당 애플리케이션의 접근권한을 확인하고 인정한다는 데 대한 동의일 뿐이며, 정보통신망법에 따른 개인정보 수집에 대한 동의는 애플리케이션 설치, 구동시 별도로 이루어진다.

<그림 2-5> 카카오톡의 휴대전화 상태 및 ID 읽기 권한 명시 화면

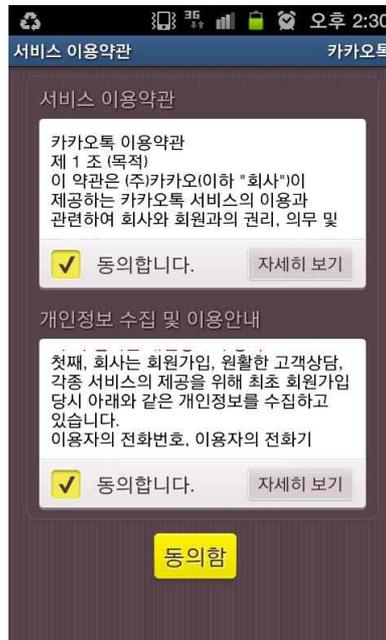


국내 최대 이용자를 보유하고 있는 카카오톡 앱의 경우를 예로 들면, 개인정보의 수집에 대한 동의 절차는 <그림 2-5>에서와 같은 절차에 따라 프로그램을 다운로드한 후, 이를 설치하는 과정에서 <그림 2-6>과 같이 서비스 이용약관과 개인정보 수집 및 이용에 관한 정보를 제공받고 이에 대한 동의 여부를 결정하게 된다. 여기서 이용자에게 제시되는 개인정보수집항목 중 기기정보에 해당하는 것으로는 전화번호, 기기고유번호(디바이스 아이디 또는 IMEI)가 있으며, 이와 같은 정보는 카카오톡 프로그램 실행시 자동으로 수집된다.²¹⁾ 동 개인정보 취급방침에 따르면 기기정보 외에도 14세 미만의 경우 법정대리인의 정보, 이용자 상태 정보, 아이디, 사진, 쿠키, 방문일시, 서비스 이용 기록, 불량이용 기록, 이메일 주소 등의 정보가 자동으로 전달될 수 있다. 또한 자동친구등록 및 친구추천과 같은 기능의 제공을 위해 주소록 내에 저장된 제3자의 전화번호도 역시 수

21) 카카오톡 개인정보 수집 및 이용약관.

집된다.

<그림 2-6> 카카오톡 이용약관 및 개인정보 취급방침 동의화면



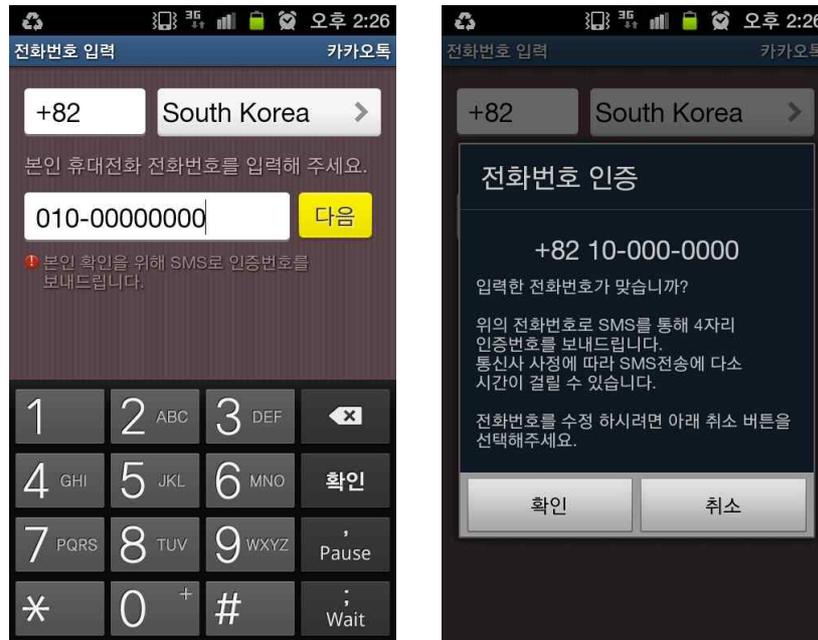
이와 같이 기기별로 부여되어 기기를 식별해낼 수 있는 식별번호로 대표적인 것에는 전화번호, IMEI번호, USIM번호, MAC주소 등이 있으며, 이들 각각은 수집되는 경로나 방법, 개인정보로서의 식별력 정도에 있어 차이를 보인다.

1) 전화번호

전화번호는 이용자를 식별하기 위해 가장 빈번히 수집되는 정보이다. 예를 들어 다음의 <그림 2-7>은 카카오톡 앱의 최초 구동시 접하는 화면으로, 카카오톡은 가입자의 전화번호를 가입자를 식별하기 위한 일차적인 수단으로 사용하고 있다. 이와 같이 전화번호를 이용자의 아이디로 하여 이용자를 인증하는 방식은 T-store 등 국내 애플리케이션

에서 자주 이용된다.

<그림 2-7> 카카오톡 최초 설치 화면



2) IMEI 번호

IMEI란 전 지구적 이동 통신 시스템(GSM) 이동단말기가 서로를 고유하게 식별할 수 있도록 이동단말기에 할당된 식별 번호로, 형식 승인 코드, 최종 조합 코드 및 일련 번호를 포함하여 15자리로 구성되는 기기고유번호이다.²²⁾ 카카오톡이나 증권통과 같이 별도의 로그인 절차를 거치지 않으면서 개별 이용자에게 특화된 서비스를 제공하는 경우 IMEI 정보를 전화번호와 함께 수집하여 ID로 사용하는 경우가 있다. IMEI 번호 자체는 개인과 무관하게 기기에 부여되는 번호이나, 국내에서 개통되는 모바일기기의 경우 이동통신서비스사업자의 가입자 데이터베이스에 개인이 개통한 기기의 IMEI 번호가 저장되므로, 개인을 식별할 수 있는 정보가 될 수 있다.

22) 정보통신용어사전(한국정보통신기술협회)(<http://word.tta.or.kr/index.jsp>)

3) IMSI/USIM 번호

IMSI는 국제 모바일 가입자 식별번호로, 이동통신서비스 가입시 구매하게 되는 USIM(universal subscriber identity module, 범용가입자식별모듈) 카드에 저장되는 정보이다. 이는 MCC(mobile country code, 국가코드) 3자리, MNC(mobile network code, 네트워크코드) 2자리와 전화번호로 구성된다. 대한민국의 국가코드는 450이며, SKT의 MNC는 05, KT는 04, 08, LG U+는 06을 사용한다. 예컨대 의 전화번호를 사용하는 국내 SKT 가입자의 IMSI 번호는가 된다.

USIM 카드는 이용자의 인증을 목적으로 휴대전화 이용자의 개인정보(통신 사업자와 이용자 비밀번호, 로밍 정보, 사용자의 개인 전화번호)를 저장하는 스마트카드로, 단말기 종류나 통신사업자에 관계없이 이용자에 따라 교체할 수 있는 등 IMEI와는 달리 개인에 대한 귀속성이 매우 강하다. 이 또한 모바일앱에서 개인을 식별하기 위하여 빈번히 수집하는 번호이다.

4) MAC 주소

MAC 주소란 “구내 정보 통신망(LAN)의 매체 접근 제어 부분층(MACS)에서 사용하는 국(局) 또는 접속구를 나타내는 주소”²³⁾ 로 각각의 통신장치가 보유하는 고유값이다. 예컨대 일반적으로 노트북의 경우 유선랜을 위한 MAC값과 무선랜을 위한 MAC값을 각각 보유하게 된다. 모바일기기의 경우 MAC값 역시 기기에 부여되는 고유번호라는 점에서 IMEI와 유사하나, IMEI는 국내 이동통신사 가입시 가입자 정보와 함께 데이터베이스 상에 저장되는 반면, MAC값은 항상 기록되는 것은 아니므로 일률적으로 개인정보라 보기에는 무리가 있다. 또한 MAC값의 경우 단말기와 통신설비 사이에 일종의 신원확인을 위해 필수적으로 주고받는 정보로서, 선택적으로 수집되는 IMEI번호와는 차이가 있다.

은행과 같이 온라인으로 금융서비스를 제공하는 경우 전자금융거래법 제7조 제3항과 동 시행령 제7조 제4항에 따라 유무선을 막론하고 전자금융거래의 거래일시, 전자적 장치의 종류 및 전자적 장치를 식별할 수 있는 정보를 수집해야 하며, 이에 따라 MAC 주소를 의무적으로 수집한다. 결제가 빈번히 이루어지는 온라인 게임의 경우에도 MAC 주

23) 정보통신용어사전(한국정보통신기술협회)(<http://word.tta.or.kr/index.jsp>)

소를 수집하는 경우가 많다.²⁴⁾

나. 위치정보

위치정보 수집/이용의 문제는 최근 국내외적으로 가장 빈번히 제기되고 있다. 위치정보를 이용한 서비스, 즉 위치기반서비스(LBS: Location Based Service)²⁵⁾는 새로운 마케팅 수단으로써 사업자들에게 각광받고 있을 뿐 아니라, 이용자의 이용 선호도에 있어서도 위치정보를 활용한 앱은 전체 애플리케이션 중 3위를 차지하는 등 활발히 이용되고 있다.²⁶⁾ 2011년 미국 시장조사기관 Strategy Analytics의 보고서에 따르면 2016년 위치정보를 이용한 마케팅의 경제적 가치는 백억달러 이상이 될 것으로 전망되었으며, 이는 전체 마케팅 액수의 절반 이상을 차지할 정도로 마케팅에서 위치기반서비스의 비중은 높아질 것으로 예측되었다.²⁷⁾ 위치정보를 이용한 서비스로는 크게 소방방재청 긴급구조 서비스 등 공공안전서비스, 교통정보, 대중교통 안내, 길찾기 등 위치추적서비스, 물류관리나 주변 상점 안내 등의 정보제공수집 서비스, SNS에서 흔히 이용되는 상황공유 서비스 등 다양한 형태의 서비스가 있다.²⁸⁾

스마트 모바일기기로부터 위치정보가 수집되는 방법으로 크게 네트워크 기반, 위성신호 기반, 혼합 측위 기반의 측정방식이 사용된다.²⁹⁾ 네트워크 기반 방식은 단말기 주변

24) 머니투데이 2010.7.28. 보도, “SK컴즈, 개인정보수집 시도 ‘해프닝으로 끝나’”.

25) 위치기반서비스의 정의에 대해서는 국내외 다양한 설명이 존재한다. 구 정보통신부에서 내린 정의에 의하면 위치기반서비스란 “이동통신 기지국이나 GPS를 통해 개인이나 차량 등의 위치를 파악하여 긴급구조, 교통정보 등을 서비스하는 신산업분야”라고 한다. 보다 최신기술을 반영한 정의로는 한국전자통신연구원과 모바일전문포털 Wiseinfo에서 내린 정의가 있는데, 이들은 위치기반서비스를 각각 “위치확인 기술을 이용해 이용자의 위치를 파악하고 이와 관련된 애플리케이션을 부가한 서비스”, “각종 무선망을 이용하여 사람, 자동차, 이동객체 등의 위치정보를 파악하여 제공하거나 그 정보에 기반한 응용서비스를 제공하는 기술 및 서비스 일체”라 정의내린 바 있다.

26) 이종관, “스마트폰의 고유 속성에 따른 법적 쟁점과 과제”, 법연 2011. 7., p.19.

27) Strategy Analytics, *Cellphone Privacy Concerns Only a Short Term Barrier to \$10 Billion Location-Based Opportunity*, (2011. 6. 9.)

28) 박정훈, “우리나라 개인정보보호법제상의 추적가능 시스템에 관한 연구”, 토지공법연구 제52집(2011. 2.), pp.297-298 참조.

의 네트워크 거점들을 통해 단말기의 대략적인 위치를 파악하는 방식으로, 이동통신사의 기지국들이나 Wi-Fi 접속 지점들로부터 모바일기기까지의 거리를 신호의 강도에 따라 측정하여 삼각측량에 의해 위치를 파악하는 방식이다. 위성신호 기반 방식은 위성에서 송신하는 신호를 기기 자체에 내장된 GPS 수신기를 통하여 수신함으로써 정확한 위치를 파악하는 것이다. 특히 GPS는 단말기 자체에서 위치를 측정하는 방식으로 확장성이 뛰어나고, 별도의 접속지점 없이 어디서나 위치인식이 가능하다는 장점을 가진다.³⁰⁾ 애플리케이션에 따라서 네트워크 기반의 대략적인 위치와 자세한 GPS 위치를 모두 수집하거나, 양자 중 하나만을 수집하는 경우도 있다. 국내에서 많은 사용자를 보유하고 있는 T map과 같은 내비게이션 앱이나 도로상황 등을 알려주는 교통정보 앱과 같이 위치정보의 이용이 주목적인 경우 대체로 양자를 모두 이용하는 혼합측위 기반 측정방식을 사용한다. 위치정보의 추적 기술에는 이밖에도 적외선, 초음파, RFID(Radio Frequency Identification)을 이용한 것은 물론, 신용카드나 CCTV 등과 다른 데이터의 매칭시스템을 통한 방법 등 다양한 방법이 개발되어 있으나³¹⁾ 모바일서비스를 위한 위치정보와는 관련성이 약하므로 여기서는 논외로 한다.

일반적으로 위치정보의 수집/이용을 주목적으로 하지 않는 서비스의 경우에도 위치정보는 포괄적으로 수집된다. 예컨대, 네이버, 구글, 다음과 같이 종합적인 포털 서비스와 제3자에게 위치기반 마케팅 서비스를 제공하는 서비스의 경우 광범위한 경로를 통해 사용자의 위치정보를 수집하게 된다. 국내에서 널리 이용되는 다음 모바일서비스 이용약관의 예를 보면 GPS는 물론, 와이파이, 블루투스를 이용한 위치를 모두 수집한다.³²⁾

모바일기기의 위치정보를 기반으로 하는 서비스는 크게 위치정보를 수집하여 이용자

29) 방송통신위원회, “LBS 산업육성 및 사회안전망 고도화를 위한 위치정보 이용 활성화 계획(안)”, p.5~6.

30) 박정훈, p.301.

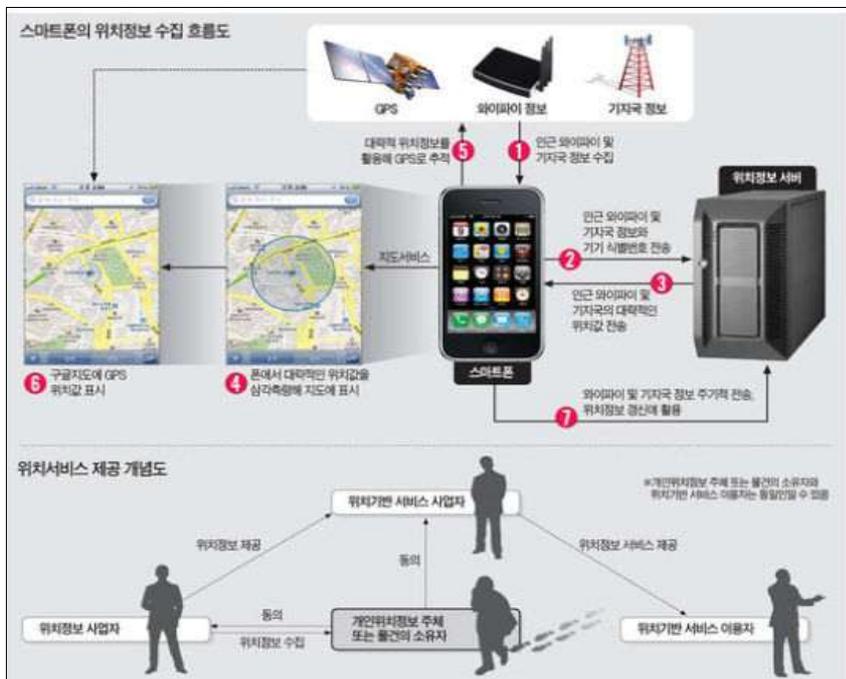
31) 박정훈, “우리나라 개인정보보호법제상의 추적가능 시스템에 관한 연구”, 토지공법연구 제52집(2011. 2.), pp.300-302.

32) 다음 모바일 이용약관, 제13조(위치정보의 수집방법)

“... GPS 수신기, 와이파이, 블루투스(근거리 무선 통신 표준)를 탑재한 사용자가 보유한 단말기로부터, 옥외에서는 GPS 신호를, 옥내에서는 무선 AP들의 MAC주소와 신호강도(RSSI: Received Signal Strength Indication)를 측정 후 얻어낸 GPS와 무선 AP 정보와 구축된 데이터베이스내의 정보를 비교하여 위치 정보를 수집”.

또는 위치기반서비스사업자에게 제공하는 “위치정보사업”과, 이렇게 제공된 위치정보를 이용하여 서비스를 제공하는 “위치기반서비스사업”으로 구성된다.³³⁾ 직접적으로 위치정보를 제공하는 서비스의 예로는 친구찾기, 자동위치찾기, 분실전화기위치조회, 길찾기 등이 있다. 위치기반서비스사업은 주변 상점 추천 기능이나 위치정보를 활용한 태깅 기능 제공 등이 있다.

<그림 2-8> 스마트폰 위치정보 수집 흐름도



위치정보의 경우 모바일기기의 위치정보 이용 기능을 해제하더라도 위치정보사업자들이 기지국을 기반으로 위치를 추적하는 것을 막을 수 있는 기술적 방법이 없다는 점을

33) 위치정보를 이용한 서비스 분류에는 다양한 기준이 이용되나, 여기서는 국내 법제분석을 위한 연구의 취지에 비추어 위치정보법상의 분류를 따르기로 한다. 위치정보법 제2조에서는 다음과 같은 정의를 내린다. 동조에 따라 "위치정보사업"이란 위치정보를 수집하여 위치기반서비스사업자에게 제공하는 것을 사업으로 영위하는 것을 말하며, "위치기반서비스사업"이라 함은 위치정보를 이용한 서비스(위치기반서비스)를 제공하는 것을 사업으로 영위하는 것을 말한다.

유의할 필요가 있다. 또한 마케팅을 위한 위치정보 앱의 경우, 많은 경우 이용자의 로그인 여부와 관계없이 일정 주기에 따라 위치정보를 전송한다는 문제점이 제기되기도 한다.³⁴⁾

다. 주소록 정보

모바일기에 저장된 주소록 정보(연락처 데이터)를 이용한 서비스 제공은 스마트 미디어로의 전환에 따른 가장 중대한 변화 중 하나이다. 주소록 정보에는 애플리케이션 이용자가 자신의 기기에 저장한 제3자의 전화번호, 이메일 주소, 생년월일 등 기념일, 소속기관, 직책 등 다양한 개인신상정보가 포함된다.

주소록 정보를 이용하는 애플리케이션은 매우 다양하다. 1차적으로는 주소록 관리를 주목적으로 하는 애플리케이션은 물론, 페이스북(facebook) 등 소셜 네트워크 서비스(SNS), 카카오톡, 마이피플 등의 메신저 서비스는 주소록 정보를 직접적으로 이용하여 서비스를 제공한다.

카카오톡 개인정보 취급방침은 카카오톡 애플리케이션을 실행하면 친구자동등록이나 친구추천 등의 기본기능의 제공을 위해 전화번호부에 저장된 제3자의 전화번호를 자동으로 수집하게 됨을 명시하고 있다.

페이스북의 경우 모바일앱 버전이 아니더라도 이용자의 이메일 계정의 주소록 정보를 기반으로 서비스를 제공해 왔으나, 모바일앱에서는 이에 추가하여 모바일기기 주소록 정보를 동기화 할 수 있는 기능을 추가하였다. <그림2-9>에서 보듯 이용자에게는 세가지 선택의 여지가 주어진다. “모두 동기화”를 선택할 경우 온라인 페이스북 계정상 자신의 친구로 등록된 제3자의 사진, 생일, 전화번호, 이메일주소 등의 모든 정보가 모바일기기의 주소록으로 옮겨지게 된다. “기존 주소록과 동기화”를 선택하는 경우 모바일기기의 주소록에 등록되어 있는 친구의 정보만이 업데이트 된다.

34) Monica Desai, Greg Louer, Ryan King, Maria Wolvin, *LBS Marketing—Why Federal Government Cares and What You Can Do About It*, Mobile Marketing Association Working Paper, 2011, pp.2-3.

<그림 2-9> 안드로이드용 페이스북 앱의 동기화 기능



라. 일정관리 정보

많은 스마트기기 이용자들은 자신의 기기를 일정을 관리하는 데 활용한다. 국내의 한 조사에 따르면 일정관리 앱은 스마트폰 이용자들이 가장 자주 이용하는 앱 중 4.3%를 차지하여 전체 항목 중 5번째로 빈번히 이용되는 앱으로 나타났으며, 가장 자주 이용하는 상위 3개 앱 중에서도 13%에 해당할 정도로 많이 이용된다.³⁵⁾ 국내에서 가장 많이 이용되는 일정관리 앱으로는 안드로이드 기반 스마트기기에 기본적으로 설치된 구글 캘

35) 한국정보통신진흥협회, 이용자 관점의 스마트폰 이용실태분석 및 사후규제방안 연구 (2010. 12. 31.), pp.45-47.

린더, 아이폰에 내장된 iCal, 그리고 Jorte가 있다. 기존 피쳐폰에서 제공되던 일정관리 기능과 이러한 애플리케이션의 가장 큰 차이점은 동기화 기능에 있다. 즉 구글 캘린더, iCal, Jorte는 모두 이용자의 계정과 모바일기기를 연동하여 온라인과 오프라인의 일정을 동기화시켜 주어 언제, 어디서나 통합적인 일정관리를 가능하게 해준다. 뿐만 아니라 이용자가 일정을 입력할 때 동참자를 입력하면 주소록 정보를 이용하여 동참자의 이메일 또는 휴대폰으로 일정을 알려주는 기능을 가지고 있다. 일정에 장소를 입력할 경우 지도 태깅 기능을 이용하여 정확한 위치를 알려주기도 한다. 기존 피쳐폰에서의 일정관리가 개개인의 휴대폰 내에서만 이루어지는 데 비하여 모바일 앱에서의 일정관리는 입력한 정보가 앱 제공자의 서버로 전송되어 통합적으로 관리되는 것으로, 개인정보의 수집이 이루어지게 된다.

실제로 2009년 일본에서는 구글 캘린더에 게재된 개인정보를 1,500건 이상의 일정을 이용자가 아닌 제3자가 자유롭게 열람할 수 있게 되는 유출되는 사고가 발생한 바 있다. 당시 유출된 정보로는 병원에서 환자의 병명과 진료일정 등을 입력한 것과 법률사무소에서 의뢰인의 성명과 상담 및 재판 일정 등이 담긴 정보가 포함되었다.³⁶⁾

마. 쿠키 등 로그 기록

로그 기록의 경우, 이용자의 인터넷 프로토콜 주소, 접속일시, 검색한 페이지의 주소(URL), 사용한 브라우저와 운영체제, 사용언어, 쿠키 ID 등이 포함된다. 이 중 쿠키의 경우 이용자의 브라우저를 고유하게 식별할 수 있다. 쿠키란 서비스제공자가 이용자를 식별하기 위해 최초 접속시 이용자의 기기에 전송하는 정보를 가리킨다.

서비스 제공자가 이용자의 쿠키를 포함한 로그기록을 수집, 저장하는 것은 일반적으로 해당 이용자에 대한 맞춤형 서비스를 제공하기 위함이다. 예컨대 구글은 개인정보처리방침에서 “사용자 환경 설정을 저장하고, 검색결과와 광고 선택을 개선하고, 검색 방법과 같은 사용자 트렌드를 추적하는 등 서비스 품질을 향상”하기 위해 쿠키 정보를 이용한다는 것을 명시하고 있다.³⁷⁾ 페이스북 이용약관에는 “Facebook에 접속하기 위해

36) 연합뉴스, 2009. 2. 13. 보도, “일본 구글, 개인 캘린더 정보 유출 논란”.

사용하시는 컴퓨터, 휴대폰 등의 도구로부터 ... IP 주소, 위치, 브라우저 종류, 방문한 페이지 등”³⁸⁾의 데이터가 수집된다고 하고 있는데, 이러한 정보는 로그 기록을 통해 수집되는 정보에 해당한다.

2. 스마트폰 애플리케이션 및 앱스토어 현황

가. 앱스토어 현황

애플리케이션은 이용자가 스마트 미디어 또는 온라인 기기를 통해 애플리케이션 오픈마켓에 접속하여 해당 앱을 자신의 스마트기기에 다운받고, 이를 실행하여 설치하게 된다. 대표적인 앱 오픈마켓에는 애플의 앱스토어, 구글의 안드로이드 마켓, 국내 SK텔레콤의 티스토어, KT의 올레마켓, LG U+ OZ 스토어, 삼성 Apps가 있다. 스마트폰 앱의 경우 2010년 기준으로 다운로드 수는 약 15억 개에 불과하였으나, 2015년까지 연평균 61%의 성장률을 기록하며 열 배 이상 성장하여 약 158억개를 기록할 것으로 전망되었다.³⁹⁾ 운영체제별로는 다음 표에서와 같이 현재 1위를 점하고 있는 iOS가 30.5%의 가장 저조한 성장률을 기록하고, 후발주자로 OS 시장 점유율을 높여가고 있는 구글 안드로이드가 연평균 80.7%의 성장률을 기록하면서 애플리케이션 시장의 선두자리를 차지할 것으로 전망되었다.⁴⁰⁾ 또한 그동안 앱 부족에 대한 문제가 지적되었던 블랙베리폰의 경우 이러한 문제가 해소되면서 연간 100% 이상의 높은 성장률을 기록할 것으로 예측된다.⁴¹⁾

37) 구글 개인정보 취급방침.

38) Facebook 개인정보 취급방침(<http://www.facebook.com/#inforeceived>)

39) 한국정보통신진흥협회, *supra* note 25. p.30.

40) *Ibid* p.32.

41) *Ibid*

<표 2-3> 운영체제별 애플리케이션 마켓 성장 전망

운영체제	2010	2011	2012	2013	2014	2015	연평균 성장률
애플 아이폰	969	1,582	2,233	2,844	3,288	3,699	30.5%
안드로이드	204	744	1,529	2,426	3,187	3,923	80.7%
윈도우모바일	87	242	427	730	1,314	1,820	83.7%
블랙베리	69	362	638	1,083	1,668	2,466	104.7%
심비안	127	836	1,449	2,008	2,614	3,194	90.7%
기타	1	29	111	266	495	693	264.3%
합계	1,456	3,795	6,386	9,357	12,566	15,765	61.0%

단위: 백만 개

(출처 : 이용자 관점의 스마트폰 이용실태분석 및 사후규제방안연구 p.31)

이들 앱 마켓에서는 스마트폰 앱 외에도 아이패드, 갤럭시탭과 같은 태블릿이나 아이팟과 같은 MP3 플레이어 등 모든 스마트 미디어에서 다운이 가능하다.

국내 애플리케이션 마켓 중에서는 SK 텔레콤의 T스토어의 성장이 두드러진다. T스토어는 애플의 앱스토어와 구글 안드로이드 마켓이 국내 애플리케이션 유통 시장을 양분하고 있던 2009년 설립되었다. 현재 T스토어는 개시 2년만에 가입자 920만 명, 누적 판매 3억 2천만 건, 등록 콘텐츠 17만 개를 보유하여 무시할 수 없는 규모로 성장하였다.⁴²⁾

나. 애플리케이션 현황

애플 앱스토어의 경우 2008년 7월 개장 당시 18,000여개에 불과하던 애플리케이션 수가 2009년 12월 10만개를 넘어섰으며, 2010년 10월 현재 약 50만개의 등록 앱 수를 기록하고 있다.⁴³⁾ 구글 안드로이드 마켓의 경우 2009년 개장 당시 1,700여개에 불과하던

42) “토종 앱 장터 T스토어 “잘 자랐네””, 아이뉴스24, 2011년 9월 8일자.

앱의 수가 2010년 10월 557,000여개로 증가하였으며, 총 60억건 이상의 다운로드를 기록하였다.⁴⁴⁾ 안드로이드 앱의 경우에는 운영체제가 개방형이어서 T 스토어 등 국내 오픈마켓에서도 다운로드가 가능하다.

어느 설문조사 결과 응답자의 과반수 이상이 13개 이상의 애플리케이션을 이용하는 것으로 확인되었다. 국내의 한 연구에 따르면 스마트폰 이용자들이 이용하는 애플리케이션은 평균 14.7개로 나타났으며, 30개 이상의 앱을 사용하는 이용자도 13.6%나 되는 것으로 집계되었다.⁴⁵⁾

국내 안드로이드 마켓을 기준으로 상위 30개 다운로드 항목에는 스마트폰 보안 프로그램이나 꾸미기 프로그램, SNS, 메신저 프로그램이 대다수를 차지하였다.(표 2-5 참조) 현재 안드로이드 마켓은 국내에서 심의 문제로 게임을 제공하지 않고 있기 때문에 게임 애플리케이션은 기타 국내 오픈 마켓을 통해 공급되고 있으나, 이에 대한 정확한 통계치는 존재하지 않는다.

43) 애플 앱스토어에 관한 통계는 148apps.biz 참조.

44) 안드로이드 마켓 이용에 관한 통계는 www.androlib.com 참조.

45) 한국정보통신진흥협회, “이용자 관점의 스마트폰 이용실태분석 및 사후규제방안 연구”. 2010.12.31., p.44.

<표 2-4> 국내 안드로이드 마켓 최다 이용 애플리케이션

순위	명칭	다운로드 수	기능
1	카카오톡	10,833,708	메신저
2	GO런처EX	5,204,044	휴대폰관리
3	폰꾸미기	906,285	휴대폰관리
4	네이버 앱	802,166	포털
5	Smart App Protect	568,025	보안
6	다음 마이피플	531,992	메신저
7	싸이월드	408,220	SNS
8	WidgetLocker	382,574	휴대폰관리
9	잠금장치	280,029	휴대폰관리
10	Facebook for Android	272,833	SNS
11	네이트온UC	268,160	메신저
12	멜론	197,282	음악
13	Apps Organizer	191,210	휴대폰관리
14	Hi There	186,986	메신저
15	다음	145,262	포털
16	LockBot Pro	131,502	휴대폰관리
17	Rule the Shy	127,692	SNS
18	Who's this?	124,236	휴대폰관리
19	네이트온	120,435	메신저
20	Light SMS	118,105	무료문자
21	Go SMS Pro	116,271	무료문자
22	Advanced Task Killer	113,594	휴대폰관리
23	Photo Wonder	102,898	멀티미디어
24	애플리케이션 폴더	98,309	휴대폰관리
25	Bubble Buster	97,504	SNS
26	네이버 웹툰	95,341	만화
27	증권통	94,824	주식
28	미니 T world	89,662	휴대폰관리
29	twitter	88,161	SNS
30	어플잠금 사생활보호	87,225	휴대폰관리

(출처 : 앱머써, 2011.11.2. 최종검색)

제3장 모바일서비스의 개인정보 이용의 문제점

모바일 단말기가 PC에 준하는 정보 처리/저장 능력을 갖추고 이용자들이 이를 적극적으로 이용하게 됨에 따라 기존의 인터넷 서비스상에서 제기되었던 것과 같은 개인정보 보호의 문제가 발생하였다.

앞서 살핀 바와 같이 스마트 미디어에서는 피쳐폰에 비하여 수집될 수 있는 정보의 양이 비약적으로 증가하는데, 이러한 정보는 다음과 같은 이유로 노트북을 비롯한 PC에서 수집된 정보보다 더욱 강하게 개인적 성격을 지닌다. 즉, 모바일 단말기에서는 기기에 대한 정보가 곧 개인정보가 된다. 예컨대 IP address나 MAC address는 PC와 모바일 단말기 양자 모두에서 수집이 가능한 기기정보이나, 개인 PC라 하더라도 해당 기기와 직접적으로 연결되는 개인정보 데이터베이스는 일반적으로 존재하지 않는다. 그러나 스마트폰이나 태블릿 PC 등 통신사업자의 서비스를 매개로 하는 스마트 미디어는 MAC address나 IMEI 번호, USIM 번호가 통신사업자가 보유하는 이용자의 개인정보 데이터베이스와 일대일로 매칭된다. 따라서 PC의 경우와 달리 모바일기기상의 정보는 “해당 정보만으로는 특정 개인을 알아볼 수 없어도 다른 정보와 쉽게 결합하여 알아볼 수 있는”⁴⁶⁾ 것에 해당하여 우리 법상 개인정보의 지위를 갖는다. 이는 현재까지 우리 법원의 입장과도 일치한다.⁴⁷⁾

또한 개방형 운영체제를 사용하는 스마트 미디어의 특성상 기기로부터 정보를 수집할 수 있는 주체 역시 다변화되었다. 개인정보 보호의 관점에서 스마트 미디어를 통한 모바일서비스가 갖는 가장 중요한 특성은 개방성에 따른 서비스 주체의 다양화라 할 수 있다. 과거의 이동통신 시장은 하드웨어 제조업체와 이동통신사업자만이 통신서비스 이용자와 직접적 관계를 맺었으며, 나아가 일단 기기가 소비자에게 양도된 이후 통신의 문제는 이동통신사업자와 이용자 양자간의 문제로 한정되었다.⁴⁸⁾ 그러나 스마트미디어

46) 정보통신망법 제2조; 개인정보보호법 제2조.

47) 서울중앙지법 판결 2010고단5343.

48) 스마트폰이 활성화되기 직전 단계에서 유통되었던 이른바 프리미엄폰의 경우에도 무

는 하드웨어 자체에 내장된 기능보다는 구매 후 사용자가 앱을 설치하여 이용하게 되면서 앱 공급자들의 역할과 영향이 증대하였다. 즉, 과거 피쳐폰에서의 앱에 해당하는 부가기능 설치가 통신사업자를 통해서 하거나 개별적인 온라인 사이트를 통해 이루어졌던 반면, 스마트기기 앱은 애플리케이션 오픈마켓을 통해 공급되면서 오픈마켓 운영자와 앱을 개발하여 해당 마켓에 출시하는 앱 개발자의 중요도가 높아진 것이다. 애플의 경우 자신의 기기에 설치할 수 있는 앱의 공급 경로를 자신이 직접 운영하는 앱스토어로 한정하고 인증된 앱개발자만이 앱을 판매할 수 있도록 하면서 영향력을 더욱 높여가고 있다. 국내에서 애플과 스마트기기 보급의 양대산맥을 이루는 삼성전자 역시 애플리케이션 마켓의 직접 운영을 강화하면서 영향력을 높이고 있으며, 이에 더해 티스토어, 올레마켓과 같은 이동통신사 중심의 마켓 역시 급성장하고 있는 추세이다. 그러나 안드로이드 마켓이나 기타 국내 앱 마켓과 같은 개방형 프로그램의 경우에는 이동통신사에서 소프트웨어의 안전성을 보장할 수 있는 폐쇄형 관리와 달리 사용자가 직접 개발에 참여하여 안전성 보장이 미흡한 현실이다.

위와 같이 스마트기기는 애플리케이션을 중심으로 사용되기 때문에 스마트기기 이용시 개인정보 보호의 관점에서 모바일 애플리케이션에 대한 관리는 매우 중요하다. 최근의 한 연구에서 밝혀졌듯이, 이용자들이 스마트폰을 구입하는 이유 중 가장 높은 비중을 보인 것이 “다양한 모바일 애플리케이션을 마음대로 사용하고 싶어서”(61.6%)라는 것이다.⁴⁹⁾ 동 연구에서 응답자들 중 23%에 달하는 수가 스마트폰 이용시 개인정보 유출이 우려된다는 입장이었으며, 또한 애플리케이션 마켓에 대해서는 40.3%에 달하는 응답자가 앱에 대한 정보가 상세하지 않다고 대답하여 애플리케이션 관리에 대한 우려를 간접적으로 드러냈다.⁵⁰⁾ 특히 안드로이드 마켓에 등록된 애플리케이션 중 20%가 사용자의 개인정보에 접속하며, 5%는 통화가 가능한 권한을 가지는 등 앱에 의한 개인정보 유출 우려는 현실화되고 있다.

선 데이터 송수신을 통한 정보처리가 가능하였으며 이를 위한 프로그램 역시 활성화된 바 있고, 폴터치스크린이 도입되는 등 스마트폰과 유사한 점이 없지 않으나, 개방형 운영체제 기반의 현행 스마트폰에는 해당하지 않으므로 논외로 한다.

49) 한국정보통신진흥협회, “이용자 관점의 스마트폰 이용실태분석 및 사후규제방안 연구”. 2010.12.31., p.35.

50) *Ibid*

이와 더불어 모바일기기는 빠른 처리속도와 저장용량을 가진 휴대용 기기라는 특성상 주소록이나 일정, 신용카드 정보 등 방대한 정보를 저장하게 되어 기기를 분실하거나 악성코드를 통한 해킹의 경우 개인정보가 한꺼번에 유출될 수 있다는 점도 많은 이용자들이 가지는 우려 중 하나이다. 특히, 바이러스나 스파이웨어, 피싱웨어 등의 악성코드 중에는 배터리 소모량을 증가시키거나 일회적으로 결제를 유도하는 등 비교적 단순한 것들도 있는 반면에, SMS나 이메일 해킹툴을 설치하게 하거나, 주소록을 가로채는 것, 신용카드 정보를 탈취하는 것 등 개인정보를 직접적으로 유출하는 종류도 기승을 부리고 있다. 이러한 악성코드는 주로 앱 설치를 통해 이용자의 기기에 주입되게 되어, 앱 설치시 해당 앱의 접근권한과 기능을 확실하게 고지하고 확인하는 것이 필요하다.

본 장에서는 이와 같은 모바일기기의 특성에 따라 모바일서비스에서 개인정보를 이용하는 경우 발생할 수 있는 문제점을 서비스 이용자의 인식도 조사와 국내외 사례 분석, 그리고 유럽, 미국 등 해외 입법 동향에 대한 고찰을 통하여 찾아보도록 한다.

제1절 모바일 환경의 도래에 따른 주요국의 동향

1. 유럽연합

가. 기존 개인정보보호지침과 E-Privacy지침

유럽연합(European Union, 이하 EU)에서 모바일 개인정보에 대한 보호는 1995년 개인정보보호지침과 2009년 개정된 2002년 지침에 의하여 크게 다루어지고 있다. 기존 유럽연합의 회원국은 개별적으로 개인정보 보호를 위한 법 제도를 가지고 있었지만, 각 회원국의 사정과 전통에 따라 개인정보 보호에 차이를 두고 있었다. 이러한 회원국 간의 차이를 좁히기 위하여 1995년 10월 개인정보보호지침⁵¹⁾이 채택되었고 동 지침을 중심으로 스웨덴, 영국을 비롯한 각 회원국의 입법조치가 시행되면서 기존의 서로 다른 국내법들은 EU차원의 개인정보보호 정책으로 통합되어가고 있다. 또한 EU는 이에 그치지 않고 회원국에 직접 적용이 되는 규정(regulation)⁵²⁾의 형식을 통하여 각 회원국의 개인정보보호지침에 대한 국내법 개정 및 제정의 이행을 확보하고 있다.

또한 1995년 제정된 동 지침이 온라인을 통한 개인정보 피해를 구체적이고 효율적으로 규율하는데 한계를 드러내자 EU는 2002년 「프라이버시 및 전자통신지침」(Directive on privacy and electronic communications, 이하 E-프라이버시지침)⁵³⁾을 제정하고 2009년 이를 개정하여 무단전자메시지(unsolicited electronic message)의 발송, 인터넷 쿠키의 사용, 공공 디렉토리에서의 개인정보 포함 등과 같은 새로운 형태의 정보처리로부터 개인의 사생활 침해를 방지하고자 노력하고 있다.

EU의 개인정보법은 민간부분과 공적부분을 가리지 않는 통합적 규율체제를 표방하고 있다는 특징을 가지고 있다.⁵⁴⁾ 이는 2011년 9월 개인정보보호법이 발효됨과 동시에

51) Directive 95/46/EC.

52) Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.

53) Directive 2002/58/EC on privacy and electronic communications.

54) Ryan Moshell, *And There Was One: The Outlook for a Self-Regulatory United States*

폐지된 「공공기관의 개인정보보호에 관한 법률」이 개인정보처리자를 공공기관에 한정시켰던 것과 대비되며 후술하게 될 미국의 민간자율형 규율방식과도 크게 대조된다.

나. 모바일 기술에 따른 개인정보 보호의 필요성 인식

개인정보에 대한 통합적이고 총체적인 법률체계를 구비하고 있는 EU에서도 모바일 환경의 도래에 따른 새로운 양태의 개인정보 피해는 심각한 우려의 대상이 되고 있다. 2010년 4월 유럽위원회는 'EU에서 개인정보보호에 대한 포괄적인 접근방식'(Comprehensive approach on Personal Data Protection in the European Union)이라는 제목으로 급속한 과학기술의 발전과 세계화가 현행 개인정보보호법제에 새롭고 커다란 위협을 야기하고 있다고 우려한 바 있다.⁵⁵⁾ 유럽위원회는 특히, 컴퓨터 기술을 기반으로 한 모바일서비스의 개인정보보호를 효율적으로 다룰 수 있는 법 제정의 필요성을 느끼고 2009년부터 모바일 기술에 따른 법개정안에 대한 연구를 시행하고 있다.⁵⁶⁾ 이에 따르면 위원회는 개인정보보호지침과 E-Privacy지침이 내포하고 있는 기본 원칙들은 모바일 환경에서도 여전히 유효하게 적용될 수 있다고 발표하면서도, 개인정보 접근성을 비롯한 정보주체의 일부 권리는 새로운 환경에서 보장되지 못할 수 있다는 우려를 표명하였다.⁵⁷⁾

이외에도 최근 모바일서비스에 특정된 제29조작업반(Article 29 Working Party)⁵⁸⁾의 연

Amidst a Global Trend Toward Comprehensive Data Protection, 37 Tex. Tech. L. Rev. 357, p.368.

55) European Commission Com(2010)609 Final, Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, A Comprehensive approach on Personal Data Protection in the European Union, p. 6.

56) *Ibid*

57) *Ibid*

58) 개인정보보호지침 제29조에 근거하여 설치된 제29조작업반(Article 29 Working Party)은 개인정보의 처리에 관하여 자문을 하는 독립된 기관이다. 제29조작업반에 관하여 자세한 내용은 http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm 참조.

구는 EU내에서 모바일 개인정보에 대한 불안이 증가하고 있음을 보여준다. 제29조작업반은 모바일 환경에서 주로 나타나는 IP 주소, 이용자 아이디(user name) 등과 같은 형태의 정보가 개인정보보호지침 제2조⁵⁹⁾에 따라 무조건적으로 개인정보에 해당하는 것이 아니라 동의(consent), 목적(purpose), 그리고 결과(result)에 의하여 개별적으로 파악되어야 한다고 밝히고 있다.⁶⁰⁾ 또한 제29조작업반은 2011년 5월 보고서를 통하여 개인정보 처리에 대한 책임을 사업자(telecom provider)와 정보사회서비스공급자(information society service provider)로 구분하여 각각에 대한 적용가능한 법률에 대하여 개별적으로 검토하고 있다.⁶¹⁾ 이는 기존의 개인정보보호지침의 적용만으로는 모바일 개인정보 처리에 대한 책임소재의 파악이 어려워지고 있기 때문이다.

2. 영국

영국은 1998년 개인정보보호법(Data Protection Act)을 제정하여 EU의 1995년 개인정보보호지침을 이행하였다. 회원국의 입법조치는 해당 지침의 목적과 그 내용에서 벗어날 수 없으므로 두 법률의 큰 골격은 상이하지 않다.⁶²⁾

영국 개인정보보호법은 제6조에서 정보보호위원(Information Commissioner) 제도를 규정하고 있다.⁶³⁾ 영국의 정보보호위원회(Information Commissioners Office, 이하 ICO)는 개인정보보호법 뿐만 아니라 2000년 제정된 정보자유법(Freedom of Information Act) 등의 개인정보보호 법률을 총괄하는 기관이며, 관련 규정을 해석하고 개인정보보호지침을 연구 및 수립하여 이에 대한 해설서를 제공하는 등 중추적인 역할을 수행한다.

모바일 개인정보에 대한 중요성은 ICO의 연구에서도 확연히 드러난다. ICO는 모바일

59) Directive 95/46/EC, Art. 2.

60) Opinion 4/2007 on the concept of personal data, 01248/07/EN WP 136, pp. 16-17.

61) 881/11/EN WP185, Opinion 13/2011 on Geolocation services on smart mobile device.

62) 그러나 각 회원국은 지침이 달성하도록 요구하는 목적을 자신의 국내실정에 맞는 형식과 수단에 따라 이행하여야 하기 때문에 그 구체적인 내용은 회원국에 따라 조금씩 차이를 보인다.

63) UK Data Protection Act, Art 6.

휴대전화는 차세대 주요 인터넷 접속장비로서 이용될 것이며, 이용자들이 자신의 휴대 장비를 스스로 프로그램화하기 어렵다는 사실에 근거하여 사생활 보호 기술(Privacy Enhancing Technology)의 개발이 모바일 기술과 함께 동시에 이루어져야 한다고 밝히고 있다.⁶⁴⁾ 또한 2008년 RSA 컨퍼런스에서 ICO의 정보보호위원인 리차드 토마스(Richard Thomas)는 오늘날 개인정보보호가 맞이한 새로운 위기는 법률로서 포섭될 수 없는 기술의 급속한 증가임을 언급하고 있다.⁶⁵⁾ 그는 또한 이러한 위기를 극복하기 위하여 행정당국은 항상 기술의 파괴력과 모바일환경에 대한 위협성을 인지해야만 하며 새로운 기술을 이용함에 있어 그 위협을 최소화하는 방법을 생각하여야 한다고 주장하였다.⁶⁶⁾

3. 미국

가. 민간자율형 규율

모바일 개인정보가 논란이 되면서 미국도 그와 관련된 입법을 서두르고 있다. 그러나 개인정보보호의 법제와 관련하여 미국은 유럽과 달리 개인정보를 포괄하는 총체적인 법률을 가지고 있지 않으며, 민간자율형(self-regulatory) 규율의 방식을 취하고 있다.⁶⁷⁾ 이러한 민간자율형 규제방식은 특정 논란에 대한 개별 산업에 따른 해결방안을 구체적인 도출해 낼 수 있다는 장점을 가진다. 모바일서비스의 사용과 관련하여 미국은 「2003년 무선랜 프라이버시 보호법」(Wireless Privacy Protection Act of 2003)을 제정하였다. 이에 따라 스마트폰과 같은 무선인터넷을 기반으로 한 모바일기기로부터의 정

64) UK Information Commissioner Study Project: Privacy & Law Enforcement, Technology development and its effect on privacy & law enforcement (2004), p. 14.

65) Richard Thomas, Information Commissioner, Speech to RSA Conference Europe on data breaches, 29 October 2008, at http://www.ico.gov.uk/upload/documents/pressreleases/2008/rsa_speech_oct08_final.pdf

66) *Ibid*

67) Ryan Moshell, *And Then There was One: The Outlook for a Self-Regulatory United States Amidst a Global Trend Toward Comprehensive Data Protection*, 37 Tex. Tech L. Rev. 357, p. 359.

보처리는 유선인터넷과 구별되어 동 법의 규제를 받는다.

그러나 파편화된 법제와 각기 다른 주법을 통하여 다루는 개인정보의 보호는 일률적이고 통일적이지 못하다는 단점을 가지게 된다.⁶⁸⁾ 예를 들어 개인정보유출에 대한 통지의 경우, 현재 45개주에서 개인정보 유출 통지에 대한 주법을 마련한 반면 알라바마, 켈터키, 미시시피, 뉴멕시코, 사우스다코다 등의 주에서는 이에 대한 입법이 이루어지고 있지 않다.⁶⁹⁾ 연방법과 주법의 우선순위를 고려할 때, 통일적인 연방법의 부재와 서로 다른 주법의 공존은 법적 안정성의 혼란을 불러일으킬 소지가 있다.

이러한 문제점은 모바일 개인정보에서도 나타난다. 예컨대, 통합적 규율 체계를 채택하고 있는 EU 및 영국, 그리고 한국의 개인정보보호법은 각각의 법에서 개인정보 ‘처리’(process)에 대한 개념을 매우 넓게 정의하고 있다.⁷⁰⁾ 이에 따라 개인정보를 다루는 개인정보처리자의 모든 행위가 관련법의 적용대상이 된다고 보아도 무방하다. 또한 국내 개인정보보호법 제3조와 같이, 통합적 규율체계는 모바일 서비스 분야와 같은 개별적이고 세부적인 영역들을 포괄적으로 규율할 수 있는 개인정보 처리에 대한 기본원칙 조항이 존재한다. 이처럼 적용대상과 범위가 넓은 EU 및 영국, 그리고 한국의 개인정보보호법 체계와 달리 민간자율형 규제에 따른 사안해결적인 접근을 하는 경우, 어떠한 관련 법률에도 포섭되지 못하는 새로운 현상에 대하여 적용 가능한 법적 기준을 제시할 수 없다.⁷¹⁾

나. 미국에서의 모바일 개인정보에 대한 문제 인식

최근 스마트폰의 보급이 증가하면서 애플, 구글과 같은 IT기업들이 개인의 위치정보를 이용자의 동의 없이 추적하여 수집한 사실이 밝혀지면서 모바일 개인정보를 보호하

68) 김범수, 미국의 개인정보 유출 통지 제도의 현황과 시사점, 人@Internet 2009년 9·10월, 한국인터넷진흥원, 51쪽.

69) 위의 글, 51쪽.

70) 개인정보보호법 제2조 2호, 영국개인정보보호법 제1조(1), EU 개인정보보호지침 제2조 (b).

71) Chris Lefkow, US senators unveil mobile privacy, data theft bills, (AFP) - Jun 15, 2011.

는 법안(bill)이 미국 의회에서 잇달아 상정되고 있다. 2011년 5월 미 상원 상무위원회 위원장인 제이 록펠러(Jay Rockefeller) 의원은 「온라인 추적 금지법」(Do-Not-Track Online Act of 2011)을 상정하였다. 동 법안은 선택적 동의절차(opt-out)를 통하여 정보 주체의 개인정보 자기통제를 강화하는 한편, 미 연방거래위원회(FTC)와 주(state)로 하여금 위반에 대한 민사집행을 시행하도록 규정하고 있다.⁷²⁾

록펠러 의원의 법안이 모바일서비스를 포함한 모든 온라인 환경에서 적용되는 반면, 2011년 6월 알 프랭클린(Al Franken) 미네소타 상원의원은 모바일기기에 한하여 적용되는 보다 세부적인 두 가지 법안을 상정하였다. 이에 따르면 「위치사생활보호법안」(The Location Privacy Protection Act)은 위치정보에 국한되어 애플, 구글 등의 통신사가 이용자의 위치정보를 제3자에게 제공하거나 공유하기 전에 명시적인 동의(express consent)를 반드시 받도록 규율하고 있다.⁷³⁾ 또 다른 법안인 「정보보안 및 위반통보 법안」(The Data Security and Breach Notification Act)은 비영리단체를 포함한 정보처리자의 민감한 정보에 대한 강력한 보안을 의무화하고, 해당 개인정보 유출과 같은 피해가 발생하였을 때 이를 정보주체에게 반드시 통보하도록 규정하고 있다.⁷⁴⁾ 위치정보뿐만 아니라 개인정보 수집 및 이용에 대한 동의, 개인정보 보유기간의 명시, 개인정보 파기 등을 다루고 있으며 미 연방거래위원회(FTC)로 하여금 해당 법률을 위반한 정보처리자에 대하여 그 이행을 강제할 수 있도록 하는 집행 조항을 포함하고 있다.⁷⁵⁾

이와 같은 미 의원들의 입법 움직임은 모두 현행 미국법이 모바일 개인정보에 대한 충분한 보호를 확보하고 있지 않은데서 기인한다. 이처럼 모바일 개인정보에 대한 우려는 비단 국내에서 그치는 것이 아니라 새로운 모바일 기술을 향유하고 있는 모든 국가에서 벌어지고 있는 공통된 문제이다.

72) Eric Chabrow, Rockefeller Submits Do Not Track Online Act, May 9, 2011, Government Information Security Articles, available at http://www.govinfosecurity.com/articles.php?art_id=3619.

73) Chris Lefkow, US senators unveil mobile privacy, data theft bills, (AFP) - Jun 15, 2011.

74) *Idid*

75) *Idid*

제2절 모바일서비스 개인정보 이용에 대한 이용자 인식도 조사를 통해 드러난 문제점

1. 조사의 목적과 방법

이용자 인식도에 대한 설문조사의 목적은 크게 세 가지로 나뉜다. 첫 번째 목적은 모바일서비스 개인정보에 대한 이용자의 전반적인 인식을 조사하는데 있다. 다음으로 현재 통신서비스사업자 및 앱 공급자에 의하여 제공되고 있는 개인정보 취급방침에 대한 이용자의 인식을 파악하고, 개인정보 취급방침 개선에 대한 이용자의 견해를 조사하여 개인정보 동의획득 절차에 있어서 세부적인 기준을 정하기 위한 참고자료로 활용하는데 있다.

본 설문조사는 2011년 9월 고려대학교 학생들을 대상으로 실시된 자체설문조사에 바탕을 두었다. 설문조사는 스마트폰과 태블릿 PC 등을 통하여 모바일서비스를 이용하고 있는 국내 대학생 100명을 대상으로 하였으며 온라인을 통한 응답방식으로 진행되었다.⁷⁶⁾ 또한 본 연구는 국내 모바일서비스 이용 현황을 자세히 파악하고 모바일 개인정보에 대한 해외 이용자 인식도를 비교하기 위하여 한국인터넷 진흥원이 실시한 2011년 상반기 스마트폰이용실태조사⁷⁷⁾ 및 2011년 4월 실시된 미국 해리스 인터랙티브의 설문조사⁷⁸⁾ 등의 기타 설문조사 결과 또한 반영하였다.

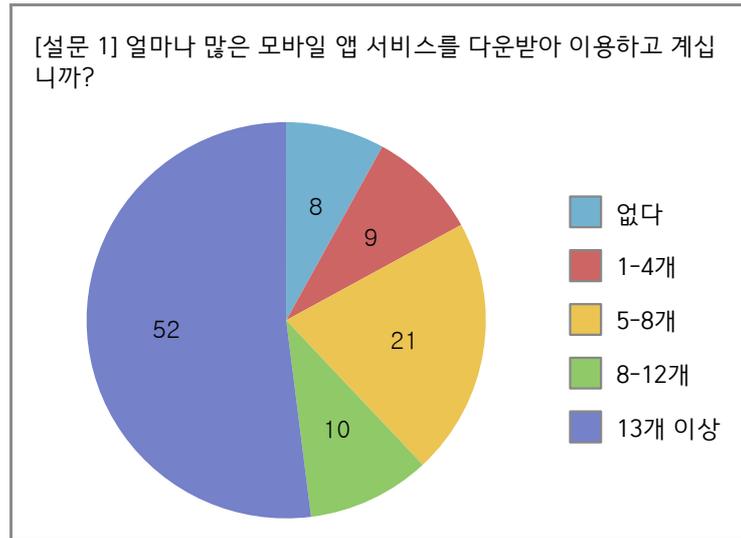
2. 설문조사 결과

가. 모바일 개인정보에 대한 이용자의 전반적인 인식

76) 설문조사 대상은 고려대학교 학부생으로 “SNS와 현대사회”라는 과목을 통하여 모바일 개인정보에 대한 간단하고 기초적인 배경지식을 가지고 있었다.

77) 한국인터넷 진흥원이 만 12세에서 59세까지의 스마트폰 이용자 4,000명을 대상으로 실시한 조사.

78) 스마트폰을 이용하는 1000명의 성인 미국인을 대상으로 미국 해리스 인터랙티브(Harris Interactive)가 실시한 조사.

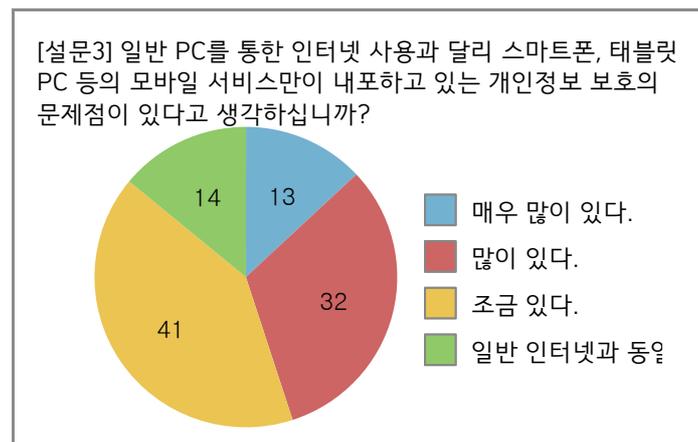
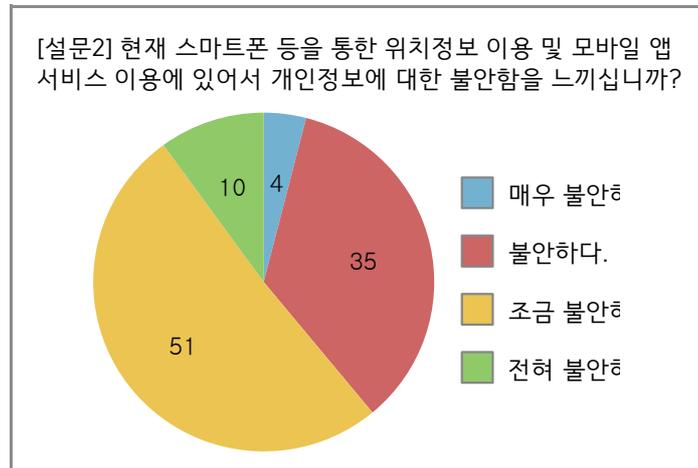


<설문 1>에서 나타나는 바와 같이 얼마나 많은 모바일 앱을 다운로드받아 이용하고 있는지에 대하여 응답자의 절반이 넘는 52%가 13개 이상의 앱을 이용하고 있다고 답하였다. 2011년 한국인터넷진흥원에서 실시한 상반기 스마트폰이용실태조사에 따르면 주 평균 다운로드받는 모바일앱은 평균적으로 6개에 달하며 최근 1개월 이내에 모바일 앱을 다운로드받은 이용자는 전체 스마트폰 이용자의 76.6%에 달하였다.⁷⁹⁾

이처럼 스마트폰과 태블릿PC의 등장으로 인터넷을 이용하여 기기 외부에서 다운로드 받는 모바일앱의 이용이 대폭 증가하면서 모바일서비스에 특정된 개인정보 보호 문제점에 대한 우려 또한 증가하고 있는 실정이다. <설문 2>에서 나타나는 바와 같이 위치정보 및 모바일 앱 서비스를 사용함에 있어서 개인정보에 대한 불안감을 가지는 이용자는 전체 응답자의 90%이며 이 가운데 매우 불안하다고 답한 이는 4%, 불안하다고 답한 이는 35%, 조금 불안하다고 답한 이는 51%에 이르는 반면 전혀 불안하지 않다고 응답한 이용자는 10%에 불과하였다. 이는 직접적인 피해를 입지 않았거나 개인정보에 대한 전문적인 지식이 없더라도 기술의 발전이 가져오는 편리함 이면에 자리 잡고 있는 모바일 개인정보에 대한 대중의 불안함을 반영한 결과라고 해석할 수 있다. 아직까지 모바일서

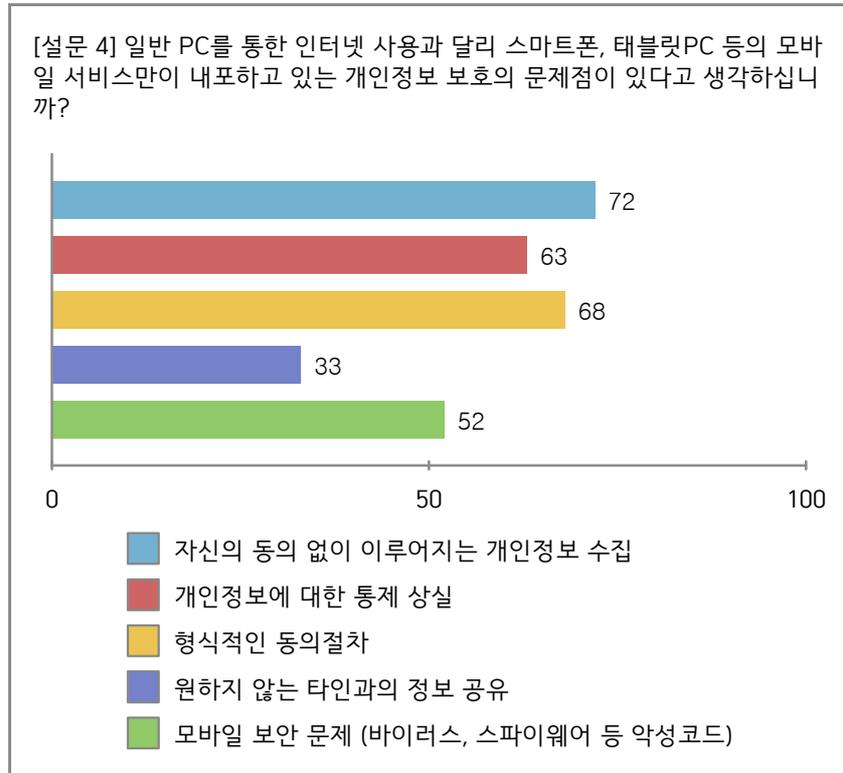
79) 한국 인터넷진흥원, 2011년 상반기 스마트폰이용실태조사, 11쪽.

비스를 이용한 개인정보의 피해사례의 발생횟수는 그리 많지 않다는 사실을 비추어볼 때, 향후 실제 피해사례가 증가하는 경우 이용자의 불안감 또한 증가할 것으로 전망된다.



<설문 3>에 따르면 일반 PC를 통한 인터넷 사용과 달리 모바일서비스만이 내포하고 있는 개인정보 보호의 문제가 있는지에 대하여 전체 응답자의 45%가 매우 많이 있거나 (13%) 많이 있다고(32%)고 답하였고, 41%가 조금 있다고 답한 반면, 일반 인터넷과 동일하다고 답한 응답자는 14%에 불과하였다.

나. 모바일 개인정보에 있어서 우려되는 사안



모바일 개인정보에 있어서 우려가 되는 사안은 무엇인가라는 질문에 대하여 전체 응답자의 72%에 해당하는 이들이 자신의 동의 없이 이루어지는 개인정보의 수집 및 이용을 선택하였다. 그 다음으로 응답자는 개인정보 취급방침에 있어서 형식적인 동의절차(68%), 누가 자신의 개인정보를 수집하고 이용하는 지에 대하여 알 수 없는 개인정보에 대한 통제 상실(63%), 바이러스 스파이웨어, 해킹, 모바일 악성코드를 통한 모바일 보안의 위협(52%) 등이 우려된다고 답변하였다. 개인정보 관련 정책에 대한 이용자 자신의 무지가 모바일 개인정보의 불안으로 나타난다고 답변한 응답자가 절반에 가까운 47%를 차지한 반면, 페이스북, 트위터 등의 SNS 서비스를 통한 타인과의 정보공유에 대하여는 복수응답 항목 가운데 가장 적은 33%의 응답자가 우려의 대상이 된다고 답변하였다.

이러한 이용자의 인식은 미국의 경우도 크게 다르지 않다. 헤리스 인터랙티브의 설문 조사에 따르면, 스마트폰의 모바일 앱 서비스를 이용하면서 가장 우려되는 사안은 무엇인가라는 질문에 대하여 응답자 가운데 38%가 프라이버시(privacy), 26%가 보안(security), 19%가 정체성(identity), 그리고 14%가 공유(sharing)를 선택하였다.⁸⁰⁾ 여기서 프라이버시란 개인정보의 보호를 포함하는 것이며 이용자의 동의 없이 개인정보를 수집·이용하는 행위는 대표적인 사생활 침해에 해당한다.⁸¹⁾ 또한 정체성이란 이용자의 개인정보를 통하여 이용자를 식별하는 행위를 말하며, 공유란 이용자의 동의 여부와 상관 없이 SNS 서비스의 이용 등을 통하여 개인정보를 타인과 공유하는 것을 뜻한다.

개인정보의 동의 없는 무단수집과 이용이 개인정보의 공유, 공유를 통한 개인의 식별, 모바일 보안의 문제보다 이용자의 불안감을 더욱 더 조장시킨다는 사실은 스마트폰과 같은 모바일기기의 발달로 인해 발생하는 개인정보보호의 문제점이 전세계적으로 공통된 분모를 가지고 있음을 뜻하며 현행법을 보완함에 있어서 가장 시급한 문제 가운데 하나가 모바일을 통한 개인정보의 무단 수집을 방지하는데 있음을 보여준다.

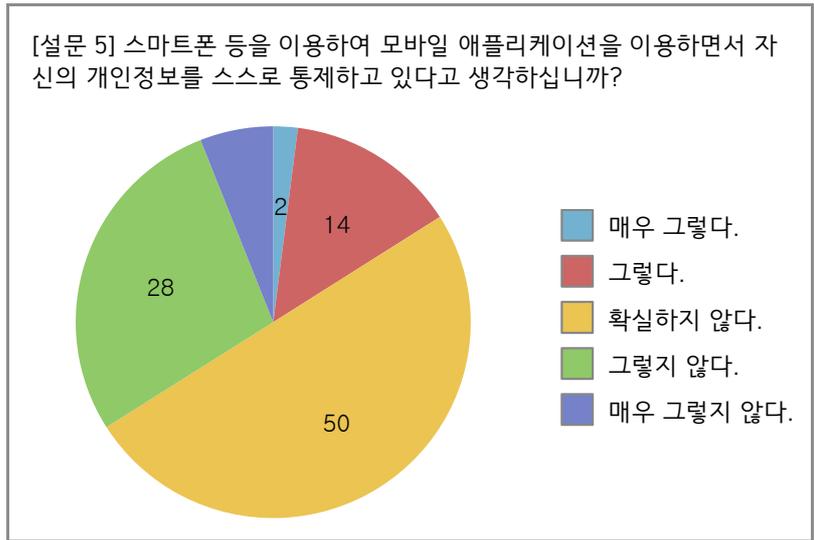
1) 개인정보자기결정권

자신의 개인정보에 대하여 알 권리는 정보통신망법의 이용자, 개인정보보호법의 정보주체에게 부여되는 권리이다. 이처럼 자신에 관한 정보가 언제 누구에게 어느 범위까지 알려지고 또 이용되도록 할 것인지를 이용자 또는 정보주체가 스스로 결정할 수 있는 권리를 개인정보자기결정권(Right of informational self-determination) 또는 자기정보통제권이라 하며 최근 헌법재판소는 이러한 권리를 개인의 기본권으로서 인정하였다.⁸²⁾

80) Harris Interactive, Mobile Privacy: A User's Perspective, p. 6.

81) *Ibid*, p. 6.

82) 헌재 2005. 5. 26., 99헌마513, 2004헌마190(병합)



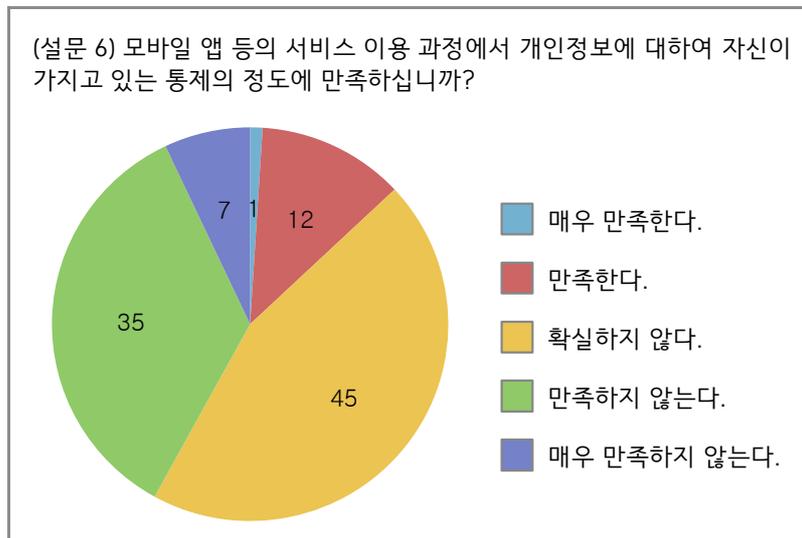
<설문 5>는 모바일 앱을 이용하면서 자신의 개인정보를 스스로 통제하고 있다고 생각하는지에 대한 설문조사의 결과이다. 이에 따르면 응답자의 절반인 50%가 확실하지 않다는 입장을 나타내고 있다. 또한 자신의 개인정보를 스스로 통제하고 있다는 생각에 찬성한 응답자는 16%(매우 그렇다 2%, 그렇다 14%)에 해당하는 반면, 통제하고 있지 않다고 답한 응답자는 34%(매우 그렇지 않다 6%, 그렇지 않다 28%)에 달하였다.

이는 미국 설문조사의 결과와 크게 다르지 않다. 모바일 단말기를 이용하는 과정에서 현재 자신이 개인정보를 스스로 통제하고 있음에 동의하는가라는 질문에 이용자의 36%(매우 동의한다 5%, 동의한다 31%)만이 개인정보를 통제하고 있다고 답한 반면, 응답자의 42%는 '동의하지도 않고 반대하지도 않는다'고 답하여 개인정보 통제에 대하여 확신이 없는 이용자가 대다수인 것으로 밝혀졌다.⁸³⁾

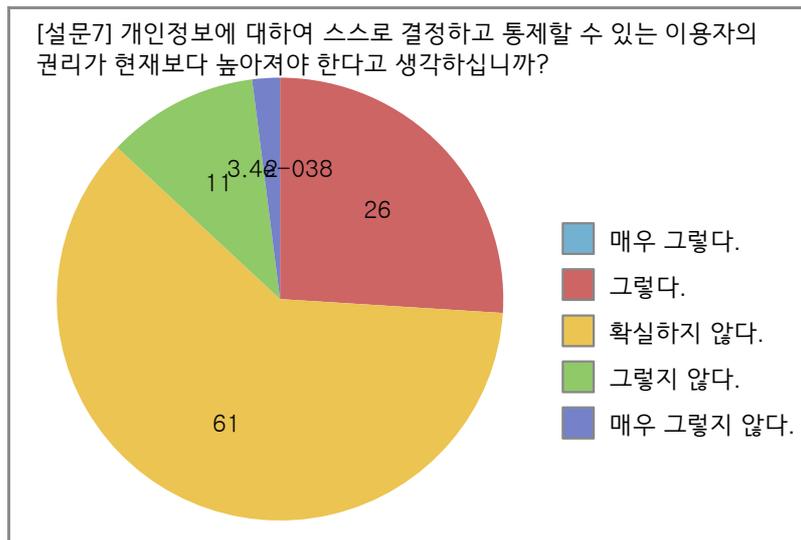
이처럼 대다수의 응답자가 개인정보자기결정권에 대하여 확실하지 않다고 답한 이유는 새로운 기술에 따른 구체적인 피해사태가 아직 많이 나타나지 않았다는 점과 정보통신망법 및 개인정보보호법에 규정된 이용자의 권리를 아직까지 대다수의 이용자가 인지

83) Harris Interactive, Mobile Privacy: A User's Perspective, p. 23.

하고 있지 못하다는 사실이 작용한 것으로 보인다. 이러한 해석의 근거는 다음의 설문 결과를 통하여 드러난다.



그<설문 6>에 따르면 모바일서비스 이용과정에서 자신이 가지고 있는 통제에 정도에 만족하는지에 대하여 확실하지 않다고 응답한 이용자는 45%, 만족하지 않는다고 답한 이용자는 42%(매우 만족하지 않는다 7%, 만족하지 않는다 35%)에 달한 반면, 만족한다고 응답한 이용자는 13%(매우 만족한다 1%, 만족한다 12%)에 불과하였다. 개인정보자기 결정권을 가지고 있는지에 대하여 질의한 <설문 5>와 비교하여, 확실하지 않다는 입장을 취한 응답자가 5% 감소한 반면, 통제권을 가지고 있다고 답한 응답자와 통제권에 만족한다고 답한 응답자는 3%의 차이를 보였다. 즉, 통제권을 가지고 있다는 답한 응답자의 비율보다 통제권에 만족하고 있다는 응답자의 비율이 줄어든 것이다. 또한 통제권을 가지고 있지 않다고 응답한 이용자가 34%였던 반면 통제의 정도에 만족하지 않는다고 응답한 이용자는 42%로 양자 사이에 8%의 차이가 나타나고 있다. 이러한 차이는 이용자가 설사 통제권을 가지고 있다하더라도 그러한 현재의 통제권에 만족을 하지 않음에 따라 발생하는 것이라 분석된다. 이러한 사실은 다음의 설문에서 확인된다.



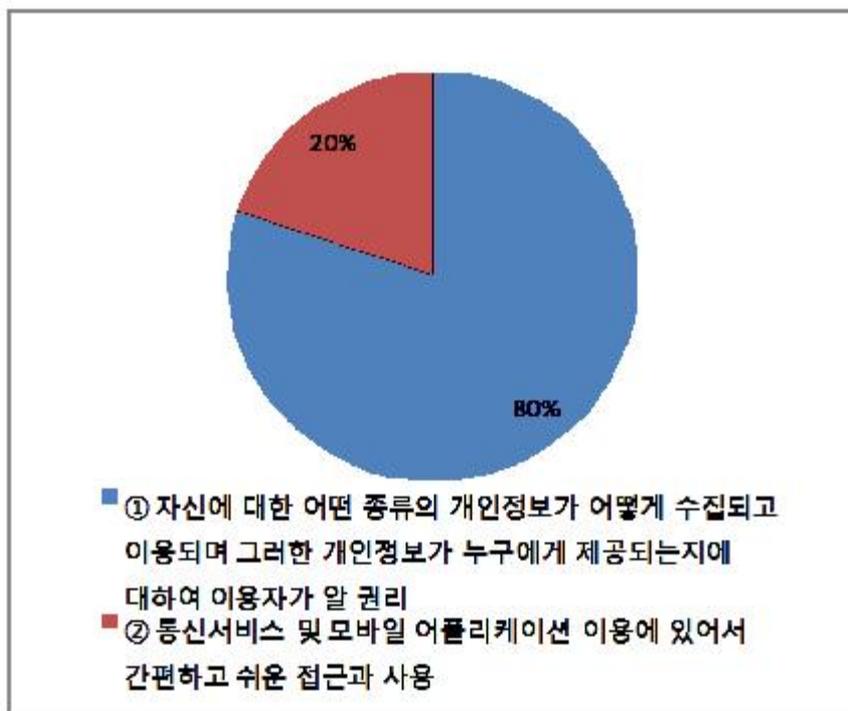
향후 모바일 개인정보보호에 있어서 자기정보결정권이 더욱 강화되어야 한다는 입장에 87%의 응답자가 긍정적으로 답한 반면, 확실하지 않다고 응답한 이용자는 11%에 그쳤고, 강화된 개인정보자기결정권에 반대하는 이용자는 2%에 불과하였다. 즉, 자기정보결정권의 여부보다 그 만족의 정도를 묻는 질문에서, 만족의 정도를 묻는 질문보다 향후 개인정보 보호의 나아갈 방향을 묻는 설문에서 이용자는 자신의 개인정보 통제에 대한 긍정적이고 강한 의식을 가지고 있음을 발견할 수 있다. 이러한 설문결과는 모바일 이용자의 인식이 기존 정보통신망법의 개정과 2011년 9월말 발효된 개인정보보호법을 토대로 개인정보에 대한 보호를 더욱 강화하려는 최근의 법률 및 정책의 방향과 부합하고 있음을 나타낸다.

미국인을 대상으로 한 설문조사의 결과도 이와 비슷하다. 전체 응답자 다운데 99%의 응답자가 자신의 어떠한 개인정보가 수집되고 처리되는지에 대하여 아는 것이 중요하다고 답변하였고, 매우 중요하다고 답변한 응답자 역시 74%에 해당하고 있기 때문이다.⁸⁴⁾

84) Harris Interactive, Mobile Privacy: A User's Perspective, p. 11.

이용자들은 개인정보의 수집 및 이용에 대한 방침을 제공받는 것뿐만 아니라 모바일 앱을 이용하는 과정에서 개인정보의 공유 여부를 용이하게 결정하는 것 또한 중요하게 생각하고 있다. 이는 각각 정보주체의 권리에서 개인정보 처리에 관한 정보를 제공받을 권리와 개인정보 처리의 동의에 관하여 결정할 권리에 해당한다.

<그림 3-8> 개인정보자기결정권과 편리한 모바일서비스의 이용



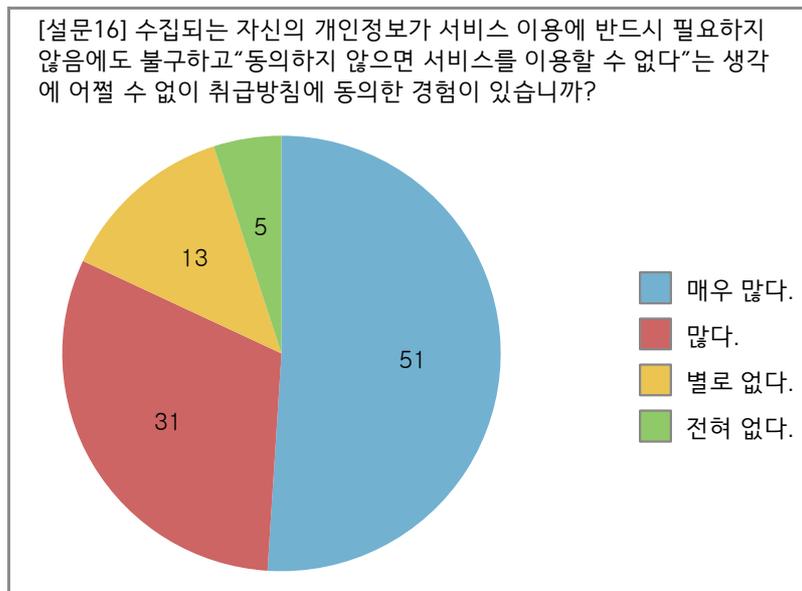
통신서비스 제공자에게 부여되는 이용자 개인정보의 보호의무가 강화될수록 이용자 또한 기존에 비해 보다 까다롭고 복잡한 절차에 놓이게 될 수 있다. 제공자가 정당하고 적법한 개인정보 수집의 동의를 구하기 위하여 이용자가 거쳐야 하는 동의획득절차가 복잡해질 수 있는 것은 이러한 예이다. 따라서 서비스의 간편하고 용이한 접근과 이용은 일면 개인정보자기결정권의 확보와 대립되는 가치를 가지게 된다.

이처럼 모바일서비스 이용에 있어서 대립될 수 있는 두 가지 가치에 대하여 <설문 8>의 결과는 개인정보자기결정권의 중요성이 새로운 기술의 출현에 따른 쉽고 간편한 모

바일서비스의 접근과 이용보다 이용자에게 더욱 중요한 문제로 인식되고 있음을 보여준다.

다. 개인정보 동의 획득 절차

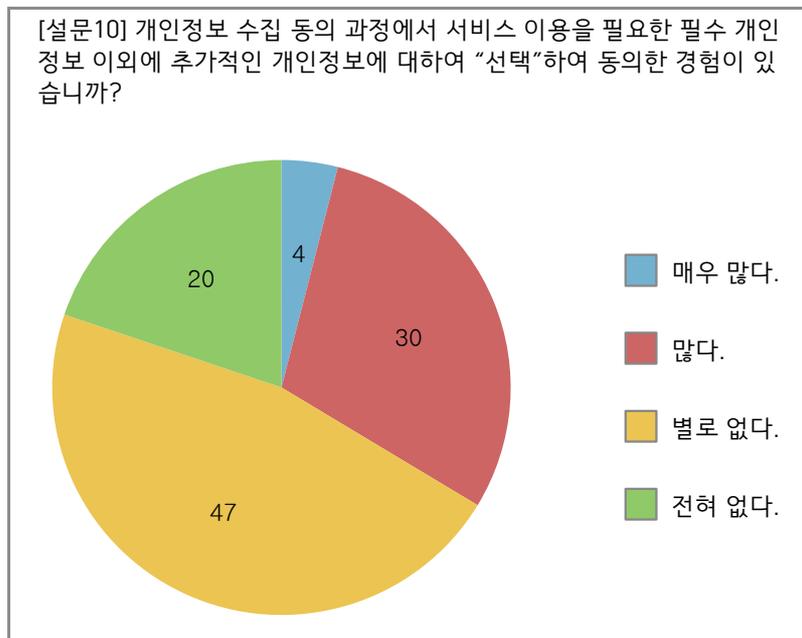
위의 <설문 4> 내지 <설문 6>에서 확인된 바와 같이 이용자들이 자신이 가지고 있는 개인정보자기결정권에 만족하지 못하고 이에 대한 우려를 표시하는 가장 큰 이유는 이용자의 동의 없는 개인정보의 무단 수집·이용과 형식적인 동의절차 때문이다. 이를 근거로 모바일 환경에서의 모바일앱 등의 서비스를 이용하기 위하여 제공되는 약관과 그에 따른 동의절차에 대하여 이용자들이 어떠한 인식을 가지는지 파악하기 위하여 다음과 같은 설문조사를 실시하였다.



<설문 9>는 수집되는 자신의 개인정보가 서비스 이용에 반드시 필요하지 않음에도 불구하고 ‘동의하지 않으면 서비스를 이용할 수 없는 방식’ 즉, 하거나 말거나(take it or leave it)식의 동의 획득절차에 대한 경험을 물어보고 있다. 이에 따르면 동의를 하지

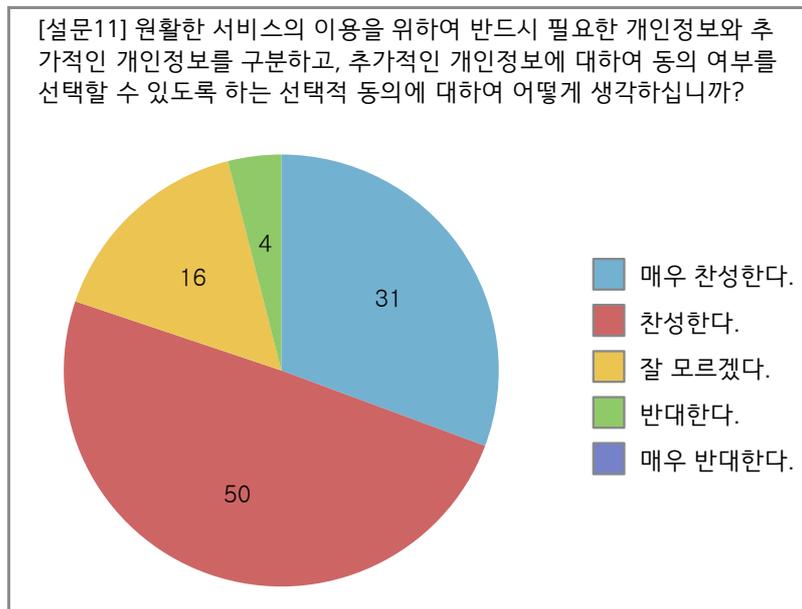
않는 경우 원하는 서비스를 이용하지 못하기 때문에 어쩔 수 없이 개인정보 수집에 동의한 경험이 '매우 많다'고 답변한 응답자가 전체의 반이 넘는 51%를 차지하였다. 또한 31%의 응답자가 그러한 경험이 '많다'고 답하여 전체 응답자의 82%가 하거나 말거나 식의 동의절차를 자주 경험한 것으로 나타났다.

개인정보 수집에 동의하는 과정에서 이처럼 이용자에게 선택권이 부여되지 않는 약관 및 개인정보 취급방침에 대하여 어떻게 생각하는지에 대하여 정보통신서비스 제공자가 해당 개인정보 취급방침을 통하여 개인정보를 보호한다면 크게 신경 쓰지 않는다고 답한 응답자가 20%에 그친 반면, 취급방침에 동의하지 않는 경우 서비스의 이용자체를 불가능하게 만드는 것은 부당하다고 응답한 이용자는 80%에 달하였다.



개인정보의 수집·이용에 동의하는 과정에서 이른바 선택적 동의(opt-in, opt-out)을 경험한 적이 있는가에 대한 질문에 총 34%의 응답자가 긍정적인 반응(매우 많다 4%, 많다 30%)을 보인 반면, 총 66%의 응답자가 그러한 경험이 별로 없거나 전혀 없다고

답하여 선택적 동의 획득 절차가 아직까지 국내에 보편화되어 있지 않다는 사실을 보여 주었다.



<설문 11>은 서비스의 이용을 위하여 반드시 필요한 개인정보와 추가적인 정보를 구분하고, 후자에 대한 개인정보 수집에 있어서 동의 여부를 이용자의 선택에 맡기는 방안 에 대한 응답자의 견해를 반영하고 있다. 이에 따르면 선택적 동의에 대하여 ‘매우 찬성한다’라고 답한 비율이 31%, ‘찬성한다’고 답한 비율이 49%에 달하여 총 80%의 응답자가 선택적 동의 절차에 대하여 긍정적인 반응을 보이고 있음을 알 수 있다.

선택적 동의 획득 절차에 대한 미국인 이용자의 반응도 이와 크게 다르지 않다. 특히 모바일 광고에 있어서 해리스 인터랙티브의 설문조사 결과에 따르면 유효표본 1,000명 가운데 850명 가까이에 달하는 응답자가 타겟형 모바일 광고의 경우 선택적 동의 절차를 통하여 이용자에게 광고 수신 여부에 대한 선택권이 주어져야 한다고 응답하였다.⁸⁵⁾

85) Harris Interactive, Mobile Privacy: A User's Perspective, Q1050, "Are you interested

라. 모바일 앱의 개인정보 취급방침

개인정보 취급방침은 개인정보의 수집·이용 목적, 수집하는 개인정보의 항목 및 수집방법, 개인정보를 제3자에게 제공하는 경우 제공받는 자의 성명, 제공받는 자의 이용목적과 제공하는 개인정보의 항목, 개인정보의 보유 및 이용 기간, 개인정보의 파기절차 및 파기방법 등을 이용자 및 정보주체가 알 수 있도록 알리는 기능을 한다. 이러한 개인정보 취급방침이 모바일 환경에서 이용자에게 어떻게 인식되고 있는지를 살펴보기 위하여 다음과 같은 설문조사를 실시하였다.

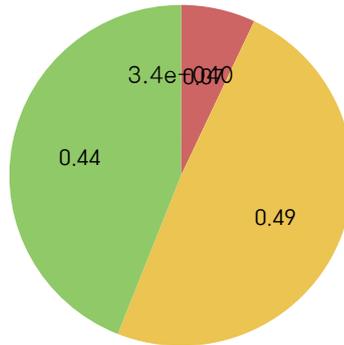
1) 개인정보 취급방침에 대한 이용자의 접근성

모바일서비스를 이용하기 전에 이동통신사 또는 모바일 어플리케이션 제공자가 제시하는 읽어본 경험이 있는지에 대한 질문에 대하여 <설문 12>의 결과에서 나타나는 바와 같이 전혀 읽지 않고 동의만 한다는 응답자가 44%, 가끔 읽지만 대부분의 경우 읽지 않고 동의한다는 응답자가 49%에 달하여 개인정보 취급방침에 대한 이용자의 접근성이 현저하게 떨어지고 있음을 보여주었다.

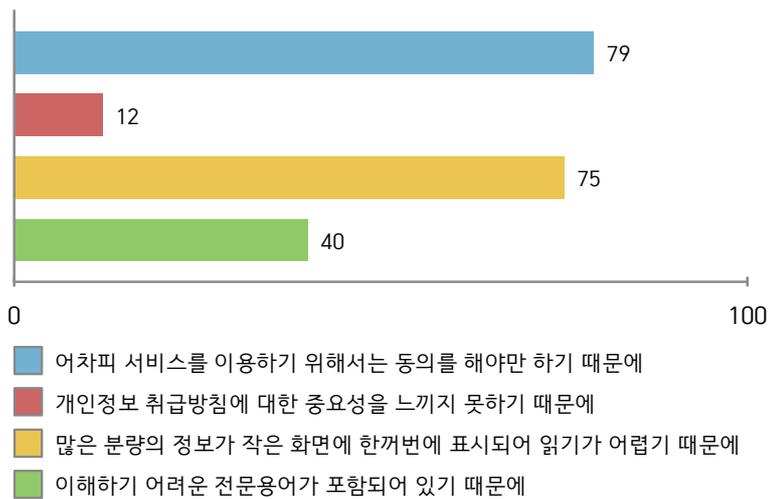
한국인터넷진흥원이 발표한 개인정보 취급방침의 이용 현황도 이와 크게 다르지 않다. 이에 따르면 모바일앱의 다운로드 시 개인정보 취급방침을 접한 경험자는 32.2%에 그쳤고 이 가운데 24.5%가 때때로 읽는다고 반면, 취급방침을 항상 읽는 이용자는 7.7%에 불과하였다.⁸⁶⁾ 또한 취급방침을 전혀 읽지 않는 이용자의 수가 13.4%에 달하여 개인정보 취급방침에 대한 이용자의 접근성이 매우 낮음을 알 수 있다.

in being able to opt in or opt out of targeted mobile ads?", p. 24.
86) 한국인터넷진흥원, 2011년 상반기 스마트폰이용실태조사, P. 28.

[설문 12] 특정 모바일 서비스를 사용하기 전에 이동통신사 또는 모바일 어플리케이션 제공자가 제시하는 “개인정보 취급방침”을 읽어보셨습니까?

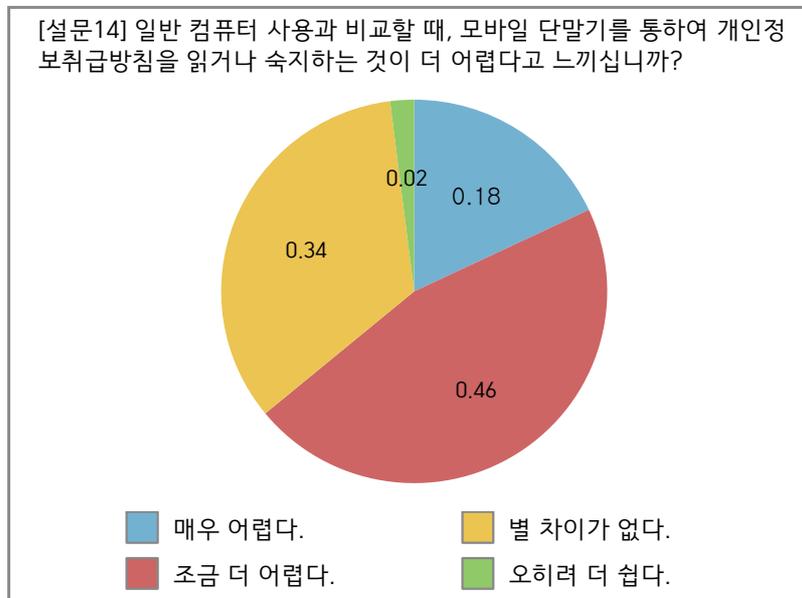


[설문 13] 읽지 않고 동의하였다면 그 이유는 무엇입니까?



개인정보 취급방침을 읽지 않고 이용약관이나 취급방침에 동의하는 응답자를 대상으로

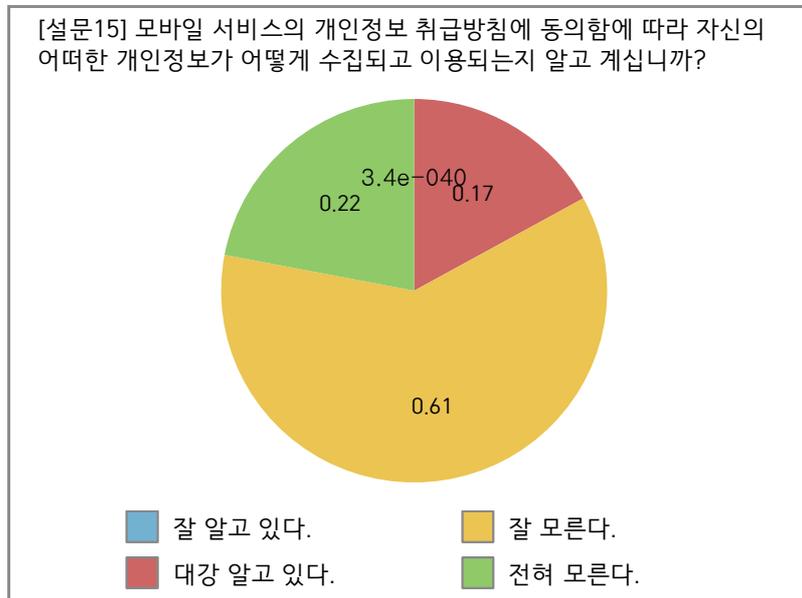
로 실시한 복수응답 설문결과 100명 가운데 79명에 달하는 응답자가 서비스를 이용하기 위해서는 동의가 불가피하다는 이유를 들었다. 다음으로 많은 분량의 정보가 작은 화면에 한꺼번에 표시되어 읽기 용이하지 않다는 이유가 두 번째로 높은 비중을 차지하였고, 40명의 응답자가 이해하기 어려운 전문용어로 인한 숙지의 어려움을 들어 취급방침을 읽지 않는다고 답하였다. 이와 달리 개인정보 취급방침의 중요성을 느끼지 못한다고 답변한 응답자는 12명에 그쳤다.



모바일서비스의 특성 상 개인정보 취급방침은 작은 화면에 표시될 수밖에 없다. 이러한 특성으로 인하여 이용자가 취급방침에 대한 접근에 어려움을 느낀다는 사실은 취급방침의 낮은 접근성이 단순히 통신서비스 제공자를 규제하는 법적 문제에만 근거하는 것이 아니라 모바일기기의 기술적 특성에도 기인하고 있음을 보여준다. <설문 14>에서 나타나는 바와 같이 모바일기기의 사용과 일반 컴퓨터의 사용을 비교할 때, 응답자의 64%가 모바일 환경에서 개인정보 취급방침을 읽거나 숙지하는 것에 더 어려움을 느끼고 있다고 답하였다. 전체 응답자의 18%가 모바일을 통한 취급방침 접근이 '매우 어렵

다’, 46%가 ‘조금 더 어렵다’고 답한 반면, ‘별 차이가 없다’고 답한 응답자는 34%에 그쳤다.

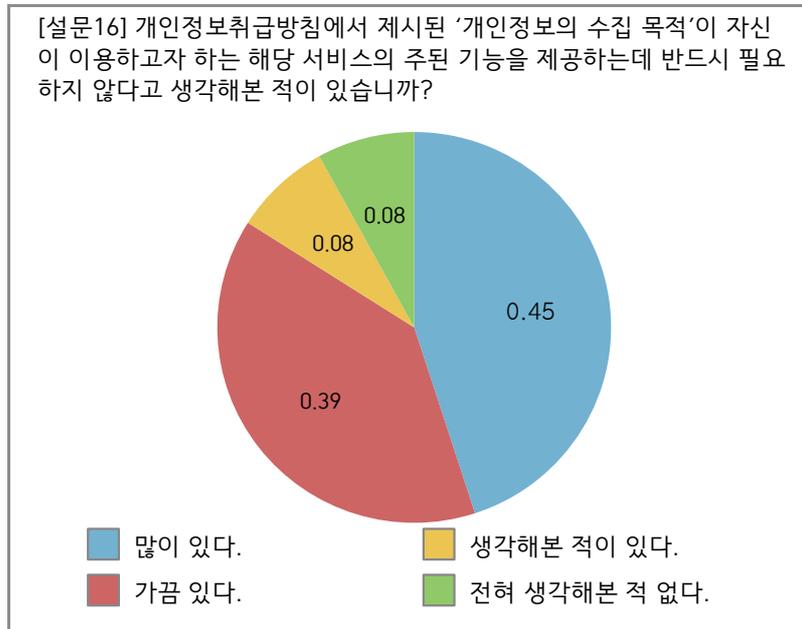
2) 개인정보방침의 효율성



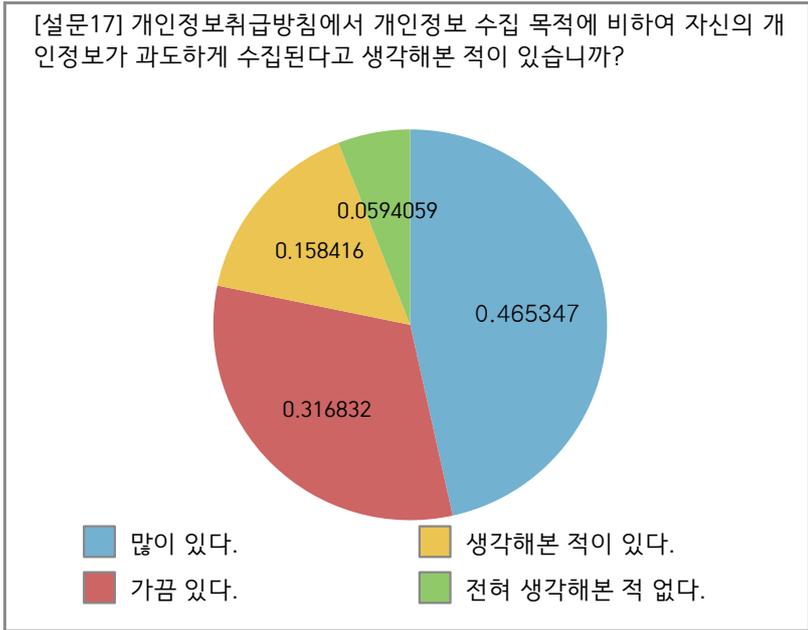
개인정보 취급방침은 개인정보의 수집·이용 목적, 수집하는 개인정보의 항목 및 수집방법 등을 이용자가 쉽게 알 수 있도록 알리는 목적을 가지고 있다. 그러나 <설문 15>에 따르면 개인정보 취급방침의 내용을 잘 알고 있다고 답한 응답자는 전무하였으며, 17%에 달하는 응답자만이 자신의 어떠한 개인정보가 어떠한 목적으로 수집되는지에 대하여 대강 알고 있다고 답하였다. 반면, 개인정보 취급방침에 대한 숙지여부와 상관없이 이용자의 83%가 세부내용을 모르고 있는 것으로 나타났고, 이 가운데 22%에 해당하는 응답자가 취급방침의 내용을 전혀 모른다고 답하여 모바일 개인정보 취급방침의 실용성에 대한 심각한 문제를 제기하였다. 또한 개인정보 취급방침을 전혀 모르거나 잘 모른다고 답한 응답자의 89%가 취급방침의 내용을 모른다는 사실로 인하여 불안함을

느끼고 있는 것으로 나타났다.

3) 개인정보 취급방침의 정당성

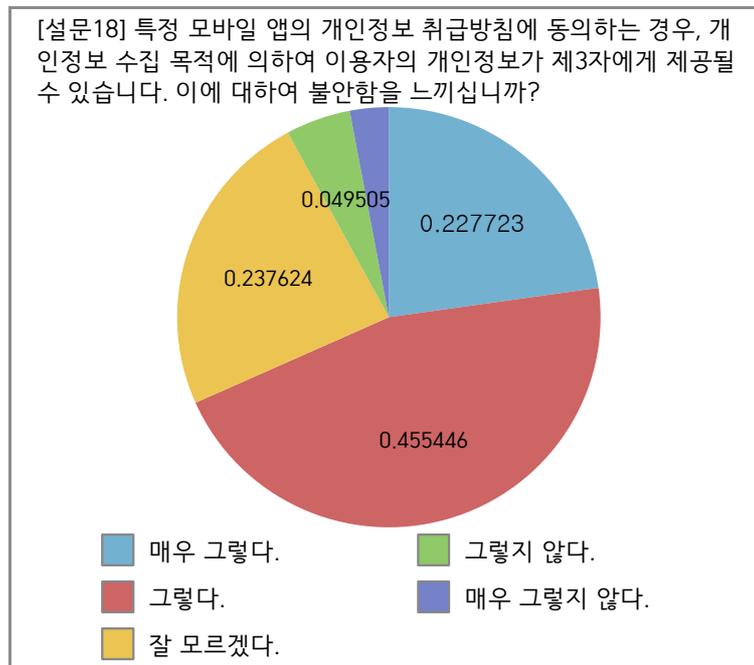


<설문 16>은 개인정보 취급방침에서 제시된 개인정보의 수집 목적 자체가 해당 서비스의 주된 기능을 제공하는데 반드시 필요한 것이 아니라는 생각을 해본 경험이 있는지에 대하여 묻고 있다. 이에 대하여 45%의 응답자가 '많이 있다', 32%의 응답자가 '가끔 있다', 16%의 응답자가 '생각해본 적 있다'라고 답한 반면, 한 번도 생각해본 적이 없다는 응답은 6%에 불과하였다.

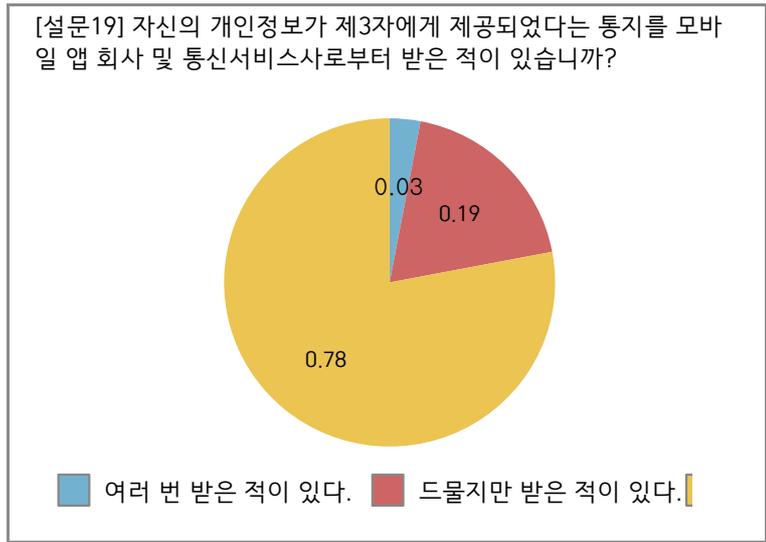


<설문 17>은 개인정보 취급방침에서 제시된 수집목적에 비하여 이용자의 개인정보가 과도하게 수집되었다고 느낀 경험이 있는지를 묻고 있다. 이에 따르면 ‘많이 있다’고 답한 응답자가 <설문 16>과 유사한 반면, ‘가끔 있다’라고 답한 응답자의 비율이 32%, ‘생각해 본 적 있다’고 답한 응답자의 비율이 16%로서 <설문 16>과 약간의 차이를 보인다.

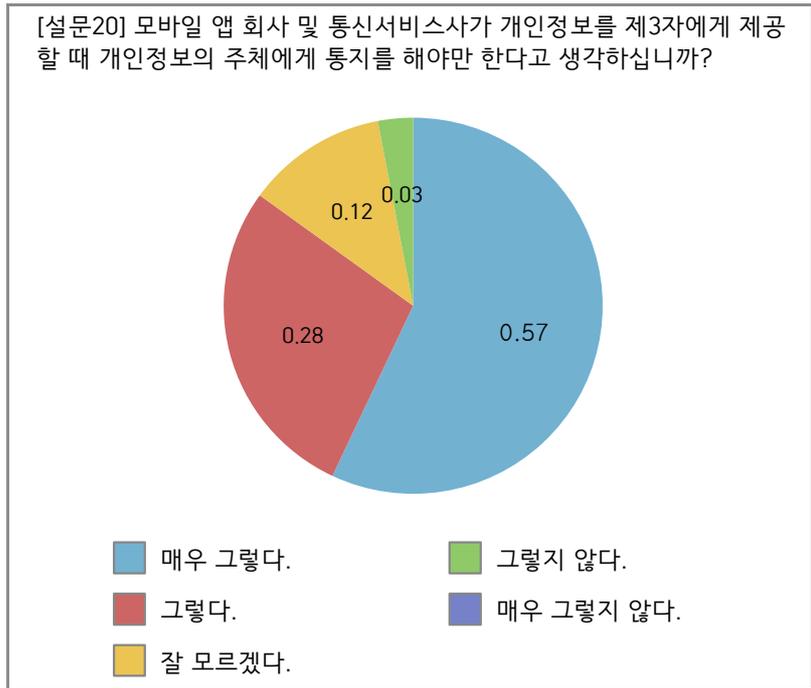
다. 개인정보의 제3자 제공



<설문 18>은 특정 모바일서비스에 동의하는 경우, 취급방침에 따른 개인정보 수집 목적에 의하여 이용자의 개인정보가 제3자에게 제공될 수 있다는 사실에 불안감을 느끼는 지에 대하여 묻고 있다. 이에 따르면 응답자 가운데 68%가 개인정보의 제3자 제공에 대하여 불안감을 느끼고 있는 것으로 나타났으며, '잘 모르겠다'고 답한 응답자가 24%의 비중을 차지하는 가운데 불안감을 느끼지 않는다고 답한 이는 8%에 불과하였다.



이처럼 이용자의 대부분이 제3자에 대한 개인정보 제공에 불안감을 느끼는 이유는 제3자에 대한 정보의 제공이 가능하다는 것을 알지만 정작 제3자 제공에 대한 통지를 받은 경험은 없기 때문으로 해석된다. <설문 19>에서 나타나는 바와 같이 전체 응답자의 78%는 자신의 개인정보가 제3자에게 제공되었다는 고지를 모바일 앱 제공자 또는 이동통신서비스 회사로부터 받은 적이 전혀 없다.

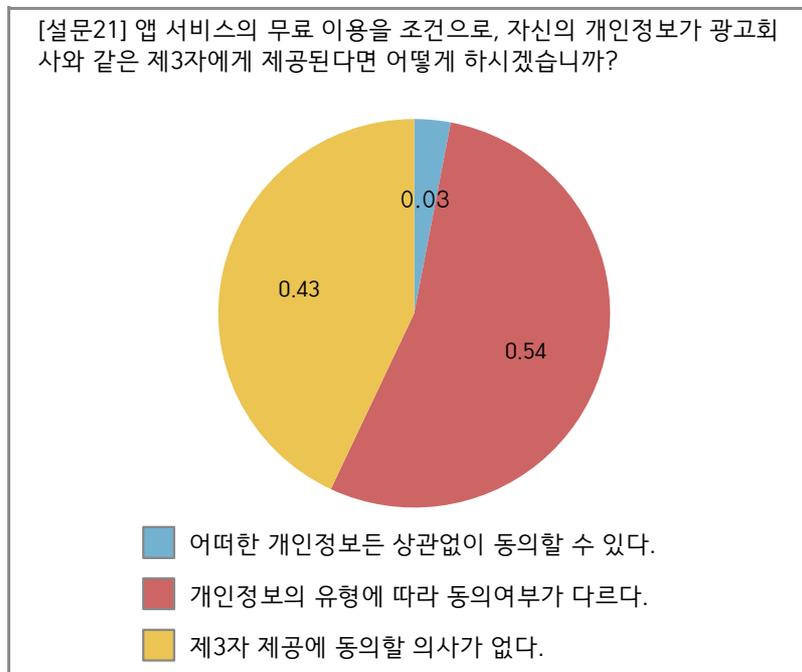


정보통신서비스 제공자는 이용자에게 개인정보 제3자 제공에 대한 사실을 알리고, 이에 대한 동의를 획득함에 따라 필요한 목적의 범위 내에서 이용자의 개인정보를 제3자에게 제공할 수 있다.⁸⁷⁾ 그럼에도 불구하고 <설문 20>은 개인정보의 제3자 제공에 대한 이용자의 우려와 불안감을 잘 나타내고 있다. 이러한 이유는 서비스를 최초로 이용할 때 내리는 자신의 동의가 제3자에 대한 정보제공을 적법한 행위로 만든다는 것을 이용자들이 완벽히 인지하고 있지 못하다는 사실을 보여준다. 또한 대부분의 모바일 환경에서 동의를 하고 난 후에야 접근할 수 있는 개인정보 취급방침의 상세한 내용을 제대로 숙지하지 못한 결과, 자신의 개인정보가 누구에게 제공되는지에 대하여 대부분의 이용자가 알 수 없게 되는 문제점을 드러내고 있다.

87) 정보통신망법 제24조의 2.

바. 무료 모바일서비스를 통한 개인정보의 수집

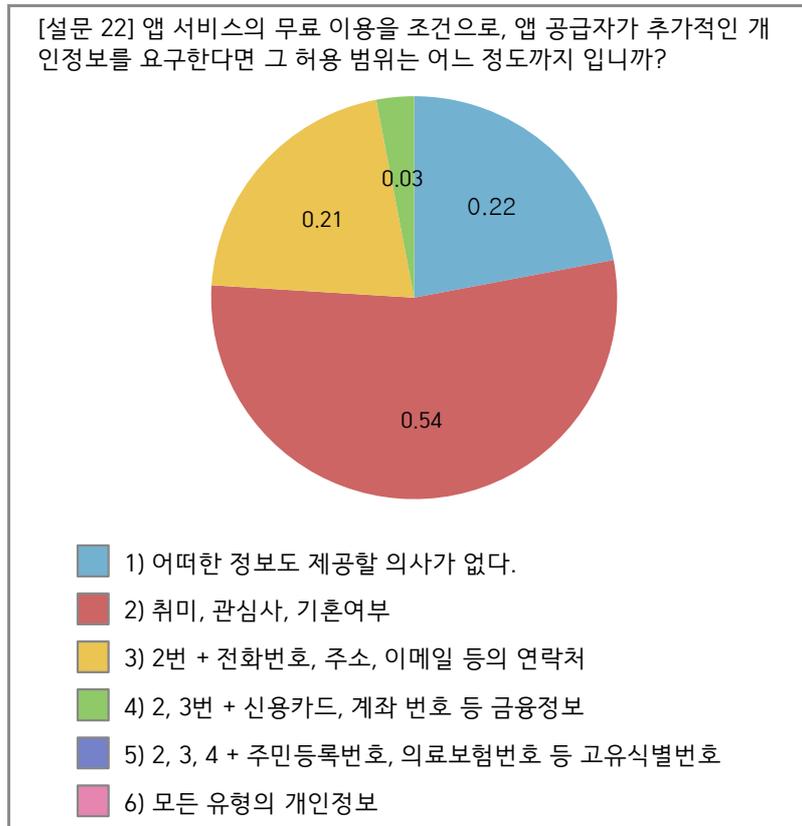
오늘날 다수의 모바일앱이 서비스의 무료이용을 조건으로 과도한 개인정보를 수집하여 이를 광고에 이용하거나 제3자에게 제공하고 있는 것으로 나타났다.⁸⁸⁾ 이와 관련하여 무료 모바일서비스에서의 개인정보의 처리가 어떻게 제한되는 것이 바람직한 것인지를 묻기 위하여 다음의 설문조사를 실시하였다.



<설문 21>은 모바일앱 서비스의 무료 이용을 조건으로 자신의 개인정보가 광고회사와 같은 제3자에게 제공된다면 이에 대한 개인정보의 수집에 동의할 것인지에 대하여 묻고 있다. 이에 따르면 응답자의 54%가 개인정보의 유형에 따라 동의여부가 다르다고 답하

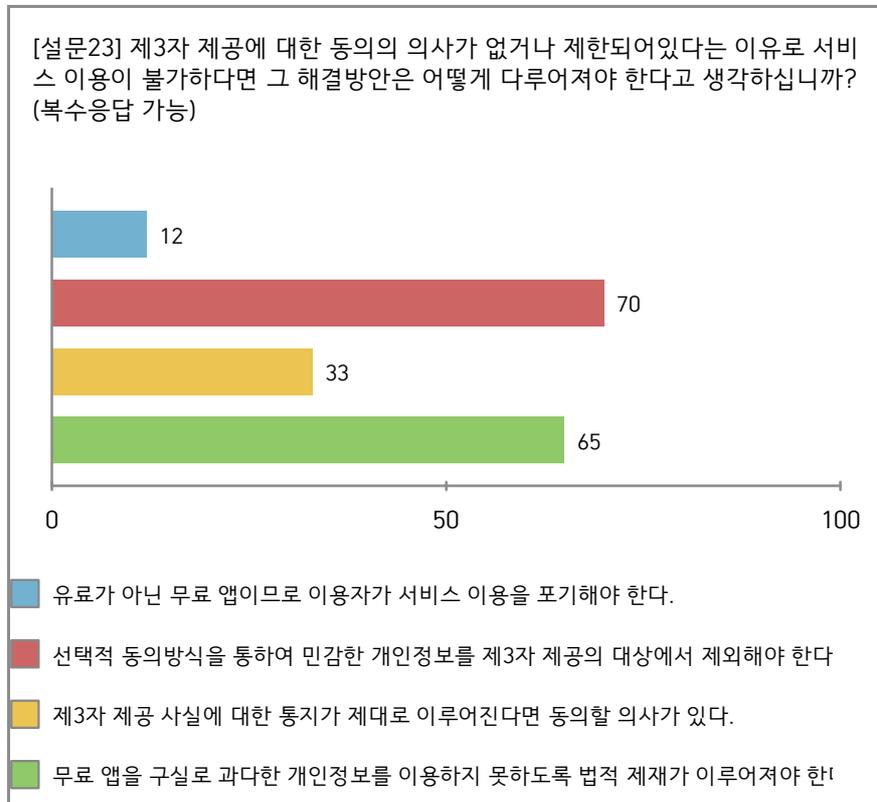
88) 최인수, 스마트폰 앱 1,400개 뿌려 80만명 위치정보 수집, 연합뉴스, 2011년 4월 11일자, <http://www.nocutnews.co.kr/show.asp?idx=1786932>.

였고, 43%가 광고를 목적으로 하는 제3자 제공에 동의할 의사가 없다고 답하였다.



무료 모바일서비스 이용을 조건으로 요구되는 개인정보의 허용범위를 묻는 질문에서 22%의 응답자가 어떠한 추가정보도 제공할 의사가 없다고 밝혔고, 절반이 넘는 54%의 응답자가 취미, 관심사, 기혼여부에 해당하는 정보만을 제공할 의사가 있다고 답하여 무료 모바일서비스를 통한 과도한 개인정보의 제공에 민감한 반응을 보였다. 전화번호, 주소, 이메일 주소 등과 같이 개인을 구체적으로 식별할 수 있는 개인정보를 제공할 수 있다고 답변한 응답자가 21%에 그친 반면, 신용카드, 계좌번호와 같은 금융정보, 주민등록번호와 같은 고유식별번호까지 추가적으로 제공하겠다고 답한 응답자는 전무하였다.

이러한 결과는 무료 모바일서비스에 대한 이용자의 인식과 실제 이용자의 이용행태가 다르다는 것을 증명한다. 즉, 광고를 위한 제3자 개인정보 제공 및 추가정보 제공에 대한 이용자의 인식은 개인정보 보호에 치우친 반면, 오늘날 많은 이용자들이 사용하고 있는 무료 모바일서비스의 개인정보 취급방침은 해당 개인정보의 처리가 가능함을 적시하고 있어, 이용자의 인식과 현실 사이에 많은 차이가 있음을 보여주었다.

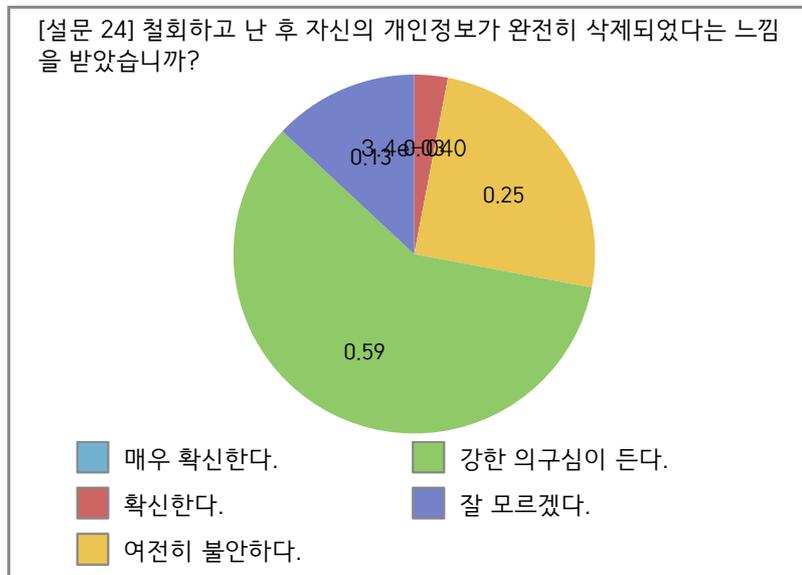


<설문 23>은 광고를 위한 제3자 제공을 시행하는 무료 모바일앱 서비스의 개인정보 취급방침에 동의하지 않는다는 이유로 서비스 이용이 불가한 경우, 그 해결방안에 대한 이용자의 견해를 반영하고 있다. 이에 따르면 무료 서비스의 특성상 이용자가 서비스의

이용을 포기해야한다는 견해가 12%에 그친 반면, 선택적 동의방식을 통하여 제3자에게 제공되는 개인정보는 최소화되어야 한다는 견해가 응답자의 70%에 이르는 가장 많은 반응을 얻었고, 무료 앱을 구실로 과도한 개인정보를 수집하지 못하도록 법적 제재가 이루어져야한다는 견해 또한 65%의 높은 비율을 보였다.

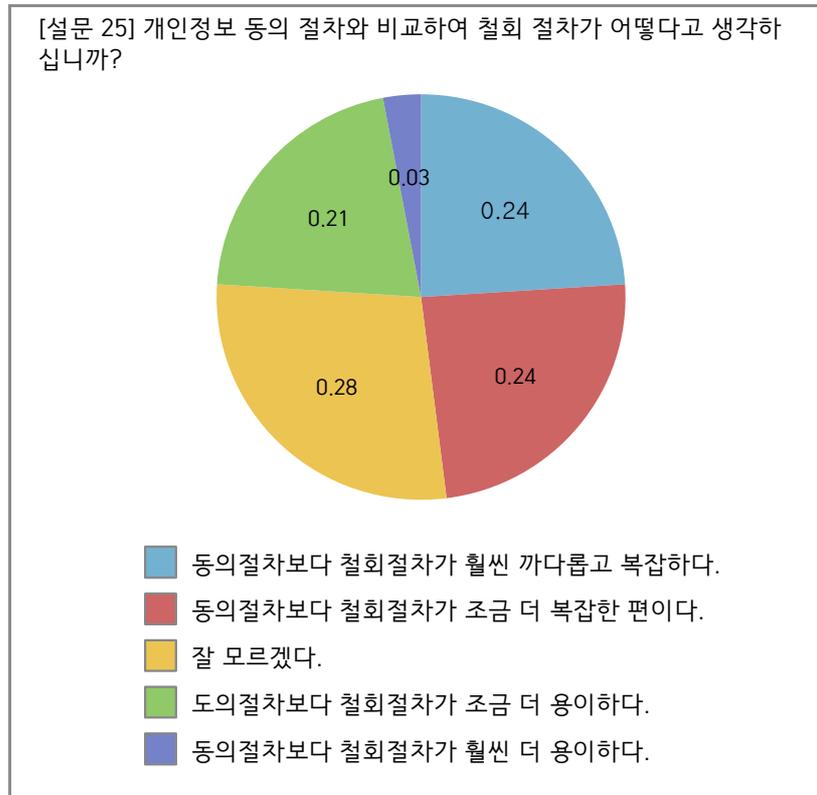
사. 개인정보 처리 동의에 대한 철회

다음의 설문조사는 모바일 환경에서 개인정보 동의의 철회에 대한 이용자의 인식을 조사하기 위하여 실시되었다. 전체 응답자 가운데 개인정보의 수집·이용에 대한 동의 후 이를 철회한 경험이 있는 응답자는 26%, 철회의 경험이 없는 응답자는 74%에 해당하였다.

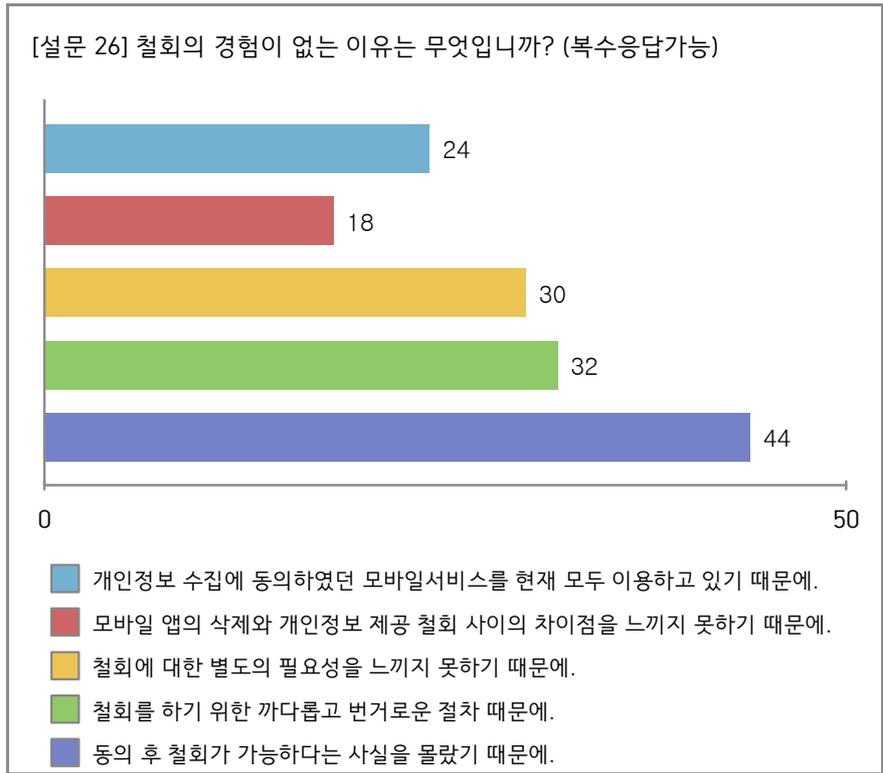


<그림 3-24>는 철회의 경험이 있는 응답자를 대상으로 하여 정보통신망법 제30조 제3항의 내용을 설문한 결과이다. 이에 따르면 개인정보 처리에 대한 동의의 철회 이후 자신의 개인정보가 완전히 삭제되었다는 느낌을 받았는지에 대하여 확신한다고 답한 응답자는 전체 응답자 가운데 3%에 그친 반면, 여전히 불안하다고 답한 응답자는 25%, 개인정보 파기에 강한 의구심이 든다고 답한 응답자가 59%에 해당하여 동의의 철회 후 개인정보의 삭제 및 파기 등 사후관리에 대하여 대부분의 이용자가정보통신서비스 제공자

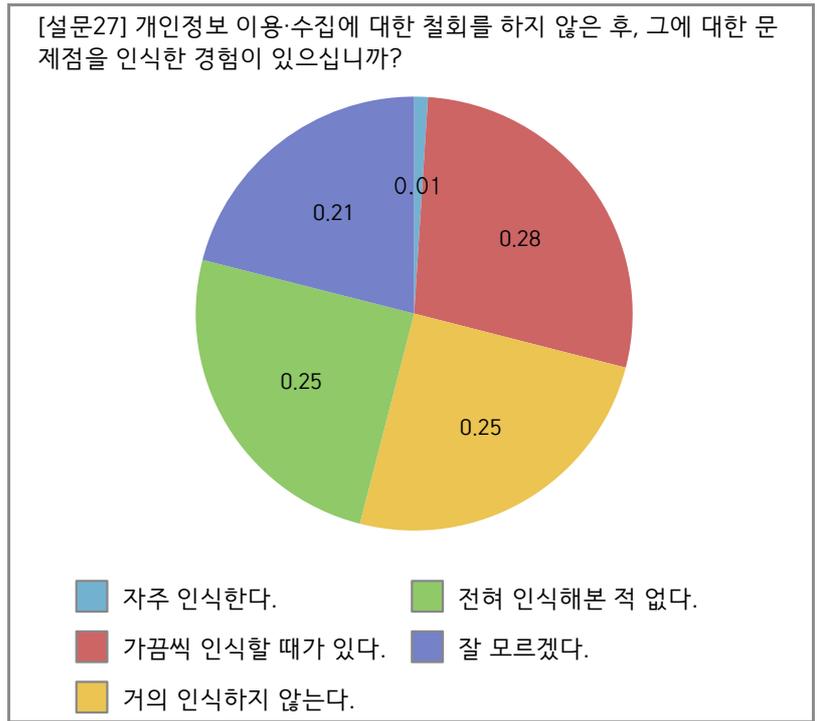
를 신뢰하지 못하는 것으로 나타났다.



<설문 25>는 정보통신망법 제30조 제6항에 대한 이용자의 인식을 조사하기 위한 설문이다. 개인정보 동의 절차와 비교하여 철회의 절차에 대한 용이함을 설문한 결과, 이용자의 48%가 동의 절차보다 철회 절차가 훨씬 또는 조금 더 복잡하거나 까다롭다고 답하였고, 28%의 응답자가 이에 대한 확신이 없었으며, 24%의 응답자만이 철회 절차가 동의 절차보다 더 쉽고 간편하였다고 지적하였다.



위 문항은 철회의 경험이 없는 응답자를 대상으로 그 이유를 묻고 있다. 복수응답으로 실시된 설문 결과에 따르면 가장 많은 62%의 응답자가 동의 후 철회가 가능하다는 사실을 몰랐기 때문이라고 답변하여 모바일 개인정보 보호와 관련된 현행 법제에 대한 이용자의 인식이 심각한 수준에 놓여있음을 보여주었다. 이 밖에 철회를 하기 위한 까다롭고 복잡한 절차, 철회의 필요성에 대한 인식의 부족 순으로 철회를 하지 않는 이유가 드러났고, 별도의 철회 없이 모바일 앱을 삭제하는 방법을 택한다고 답변한 응답자는 18%에 불과하였다.

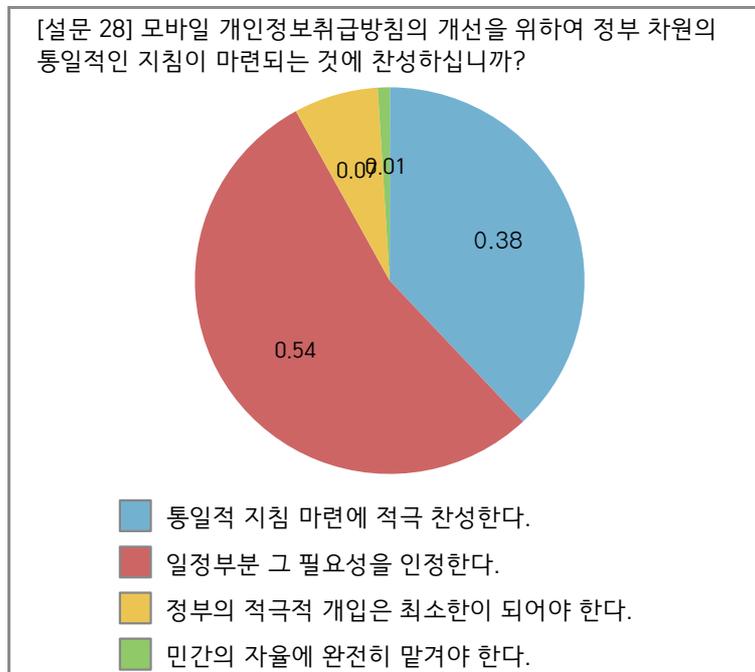


<설문 27>은 철회의 경험이 없는 응답자를 대상으로, 철회를 하지 않은 후 그에 따른 문제점을 인식한 경험이 있는지에 대하여 결과를 보여주고 있다. 이에 따르면 파기되지 않고 정보통신서비스 제공자에 의하여 보관되어지는 개인정보와 같은 문제점을 ‘자주 인식한다’고 답한 이는 1%, ‘가끔씩 인식할 때가 있다’고 답한 이는 28%에 그친 반면, 절반에 해당하는 50%의 응답자가 동의에 대한 철회를 하지 않음으로 인해 생기는 문제를 거의 인식하지 않거나(25%) 전혀 인식하지 않는 것(25%)으로 드러났다.

위의 <설문 24>와 비교하여 볼 때, <설문 27>의 결과는 이용자 사이의 개인정보 보호 의식이 양극화되고 있다는 분석을 가능하게 한다. 즉, 개인정보의 처리에 대한 동의의 철회 경험이 있는 이용자는 자신의 개인정보가 파기되었는지에 대하여 여전히 불안해하는 반면, 철회의 경험이 없는 이용자의 경우, 동의에 대한 철회가 가능한 것인지도 모르는 경우가 많았고 철회를 하지 않음으로 인해 생기는 불안감 또한 대부분 없는 것으로

드러나 개인정보 보호의식에 대한 이용자 간의 차이가 존재하는 것으로 나타났다. 즉, 동의의 철회 등을 통하여 개인정보의 처리에 대한 자기결정권을 행사하는 이용자가 그렇지 않은 이용자보다 개인정보 보호의식이 더 강한 것을 알 수 있다.

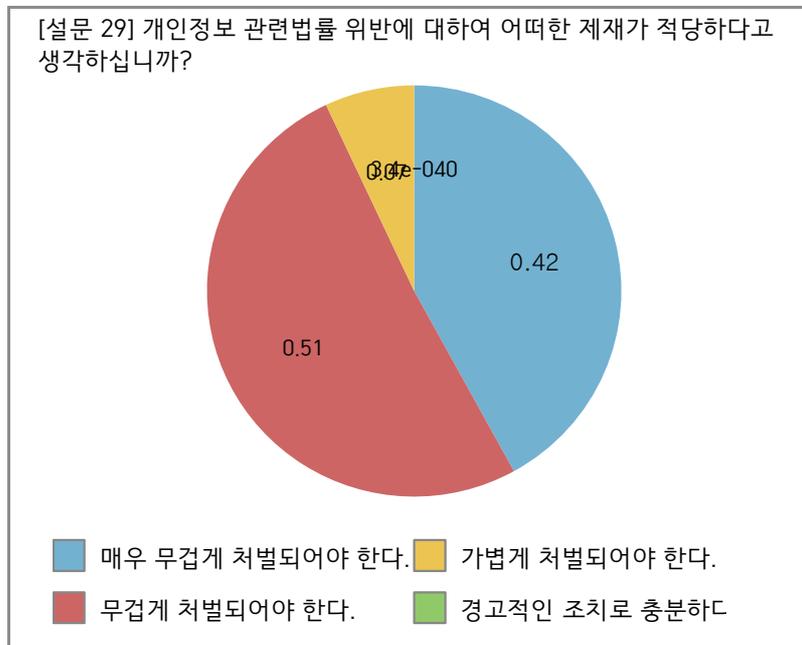
아. 모바일 개인정보의 나아갈 방향



마지막으로 설문조사는 향후 모바일 환경에서의 개인정보 법률 및 정책의 나아갈 방향에 대하여 이용자 및 정보주체의 견해를 반영하고자 하였다. 이에 따라 설문조사의 응답자가 현행 법률과 정책의 내용을 숙지하지 못한다는 가정 하에, 정부차원의 통일적 지침 마련의 당위성, 개인정보 관련 법률 위반에 대한 처벌의 정도, 향후 법률 개정 및 정책 개선에 있어서 이용자의 관심이 가장 큰 사안이 무엇인지에 대하여 다음과 같은 설문을 실시하였다.

설문조사가 집중적으로 다룬 모바일 개인정보 취급방침의 문제점을 개선하기 위하여 정부차원의 통일적인 지침이 마련되는 것에 대하여 38%가 적극 찬성한다고 답하였으며,

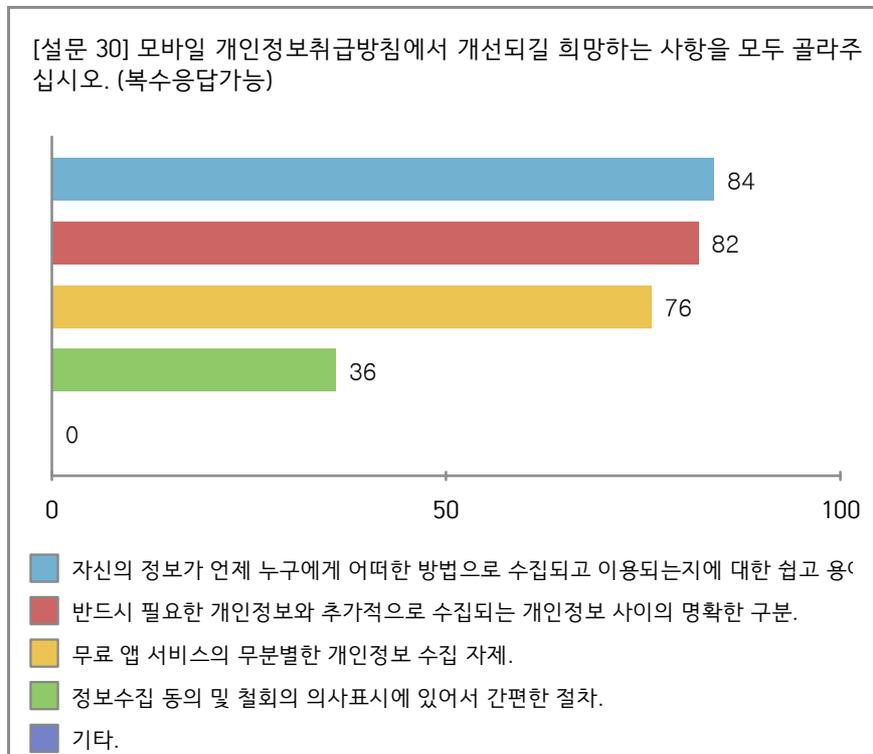
54%가 일정 부분 그 필요성을 인정한다고 답하여 총 92%의 응답자가 통일적인 지침 마련에 긍정적인 반응을 보였다. 반면, 정부의 개입이 최소한이 되어야 한다고 응답하거나 민간의 자율로서 모바일 개인정보가 규율되어야 한다는 견해는 각각 7%, 1%에 불과하였다. 이는 앞서 진행된 설문조사의 결과를 비추어 분석해 볼 때, 이용자와 정보통신 서비스 제공자 사이에 존재하는 정보 또는 권한의 불균형, 제공자의 개인정보 처리에 대한 이용자의 불신, 개인정보자기결정권을 확보하고자 하는 정보주체로서의 이용자의 인식 등이 작용하였기 때문으로 해석된다.



<설문 29>의 결과는 개인정보의 유출, 동의 없는 무단 수집·이용 등과 같은 위법행위에 대하여 어떠한 제재가 적당인지에 대한 이용자의 견해를 나타내고 있다. 이에 따르면 정보통신망법, 개인정보보호법, 위치정보법 등의 관련 법률을 위반한 행위에 대하여 가볍게 처벌되어야 한다고 응답한 이가 7%에 그친 반면, 매우 무겁게 처벌되어야 한다고 답한 이가 42%, 무겁게 처벌되어야 한다고 답한 이가 51%에 달하여 전체 응답자

의 93%가 높은 처벌의 수위를 요구하고 있는 것으로 드러났다.

양형 기준에 대한 전문적인 법률지식이 없는 이용자들이 이처럼 강력한 수위의 처벌 기준을 요구하는 이유는 새로운 모바일 환경에 대한 두려움에 근거하는 것으로 보인다. 모바일기기를 통한 개인정보의 수집이 어떻게 이루어지는지 모르는 일반 이용자의 입장에서, 개인정보 보호법제에 대한 자신의 무지와 제공자와의 상대적 관계에서 절대적 을 에 속한다고 생각하는 이용자의 인식이 위법행위에 대한 높은 처벌 수위로서 반영되고 있는 것이다.



마지막으로 모바일 개인정보 취급방침에서 개선되길 희망하는 사항에 대하여 가장 많은 응답자인 84%가 자신의 정보가 언제 누구에게 어떠한 방법으로 수집되고 이용되는지에 대하여 알 권리, 즉 개인정보자기결정권이 강화되기를 희망하는 것으로 나타났다. 이에 못지않게 82%의 응답자가 주된 서비스의 기능을 고려하여 반드시 필요한 개인정

보와 추가적인 개인정보를 서비스의 제공자가 구분하여 제시하기를 희망하였고, 76%의 응답자가 무료 모바일 앱 서비스의 무분별한 개인정보 수집의 자체를 개선사항으로 선택하였다. 이에 반해 정보 수집 동의 및 철회에 있어서 간편한 절차를 희망하는 응답자는 36%로서 다른 세 문항에 비해 상대적으로 적은 선택을 받았다.

3. 설문조사 분석

설문조사의 결과는 다음과 같이 요약될 수 있다. 첫째, 대부분의 이용자는 개인정보 보호를 위한 법률 및 정책에 대하여 친밀감을 가지고 있지 않다. 정보통신망법에서 다루어지는 이용자의 보호, 개인정보보호법에 규율하는 정보주체의 보호는 모두 사회의 전문화 및 기능분화에 따라 탄생된 개인정보라는 고유한 영역을 규율하는 개별법으로서 일반인들이 쉽게 다가갈 수 없는 전문법에 해당하기 때문이다.⁸⁹⁾ 개인정보법제에 대한 이용자의 친밀도는 다음의 설문결과에 근거한다. 이용자들은 개인정보에 있어서 자신의 동의가 정보통신서비스 제공자의 어떠한 행위들을 적법하게 만드는지에 대하여 그 중요성을 인식하지 못하고 있다. 개인정보의 수집·이용에 대한 동의를 하면서도 개인정보 취급방침을 읽지 않거나 숙지하지 않는 이용자의 수가 절대적으로 많았다.⁹⁰⁾ 개인정보 취급방침에 무지한 결과, 광고를 위한 개인정보의 제3자 제공에 대하여 강한 거부감을 가지고 있으면서 실제 이용자들이 이용하고 있는 대다수의 모바일 앱이 자신의 동의를 통하여 제3자에게 제공되고 있다는 사실을 인지하지 못하고 있다.⁹¹⁾ 또한 대다수의 이용자들이 처리 가능한 개인정보의 허용범위의 기준을 상대적으로 엄격하게 설정하고 있으면서도 오늘날 대다수의 모바일 앱이 그보다 더 많은 양의 개인정보를 처리하고 있다는 사실을 알지 못하였다.⁹²⁾ 또한 자신이 동의한 개인정보 취급방침에 대하여 철회가 가능하다는 사실을 모르는 이용자 또한 상당하였다.⁹³⁾ 관련법제에 대한 이용자의 무지

89) 이상돈, 기초법학, 제2판, 548쪽.

90) 설문 12, 설문 13.

91) 설문 18, 설문 19, 설문 20.

92) 설문 16, 설문 17, 설문 22.

93) 설문 26.

는 동의 획득 절차가 보다 간소한 모바일 환경에서 더 심각한 문제를 야기한다. 한 번의 버튼 클릭으로 제공자로 하여금 모든 개인정보의 처리를 가능하게 만들뿐더러 작은 휴대용 화면을 통한 표시방식은 이용자의 개인정보 취급방침에 대한 접근성을 더욱 떨어트리기 때문이다.

둘째, 이용자들은 개인정보법제에 대한 이해가 부족하지만, 모바일 환경에서의 개인정보 보호에 대하여 결코 무관심하지 않으며 오히려 많은 우려를 표시하고 있다. 설문조사에서 나타나듯이 대다수의 응답자들은 일반 컴퓨터 사용과 달리 모바일 환경에서의 개인정보 보호에 대한 전문적이고 개별적인 검토의 필요성을 인정하고 있다.⁹⁴⁾ 또한 대부분의 응답자들은 형식적인 동의절차로 인하여 자신에게 선택권이 주어지지 않는 상황에 대하여 불만을 가지고 있으며,⁹⁵⁾ 주된 서비스의 기능과 별개로 추가적인 개인정보를 수집하고 이용하는 개인정보 취급방침에 의문을 제기하고, 선택적 동의 절차에 깊은 관심을 보이고 있다.⁹⁶⁾ 대부분의 이용자들은 모바일서비스의 편리한 이용보다 자신의 개인정보에 대한 통제에 더 많은 가치를 부여하고 있고,⁹⁷⁾ 동의 후 정보통신서비스 제공자가 자신의 개인정보를 완전히 파기하는 등의 적절한 조치를 취하고 있는지에 대하여 의구심을 가지고 있으며,⁹⁸⁾ 무료 모바일앱의 무분별한 개인정보 수집에 대한 우려와 함께 정부차원의 통일적인 지침을 마련하여 이러한 문제점이 해결되길 바라고 있다.⁹⁹⁾

셋째, 모바일 환경을 제대로 반영하지 않은 현행 법률 및 정책은 이상의 두 가지 문제점이 가지고 있는 격차를 좁히기 위한 해결책을 완벽하게 제시하지 못하고 있다. 개인정보를 규율하는 개별법에 대한 무지와 이로 인해 발생하는 이용자의 불안감을 해소하기 위해서는 모바일 고유의 환경에서 발생하는 개인정보 처리의 문제점을 파악하고 이를 법률 및 정책으로써 포섭시켜야만 한다. 이처럼 법제도의 정비가 기술의 속도를 따라잡지 못하기 때문에 발생하는 문제점을 해결하기 위하여 본 연구는 설문결과에 대한 분석을 바탕으로 현재 많은 이용자들이 이용하고 있는 모바일서비스를 예로 들어 다

94) 설문 3.

95) 설문 9.

96) 설문 11.

97) 설문 8.

98) 설문 24.

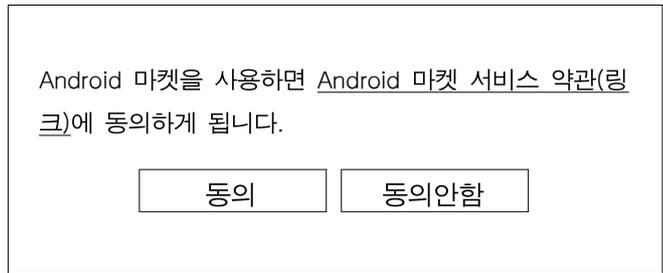
99) 설문 28.

음과 같은 세부적인 문제점을 제시한다.

가. 형식적이고 강압적인 동의절차

이용자들이 개인정보 처리에 대한 자신의 동의에 대하여 큰 의미를 부여하지 않는 가장 큰 이유는 정보통신서비스 제공자의 소위 ‘하거나 말거나’(take it or leave it) 식의 고압적인 태도 때문이다.¹⁰⁰⁾ 이와 같은 결과가 나온 이유는 개인정보를 수집하고 이용하는 권한이 이용자 또는 정보주체의 동의에 맞추어져 있지 않고 정보통신서비스 제공자의 일방적인 권리로서 행사되고 있기 때문이다. 다음은 2011년 9월에 변경된 안드로이드 마켓의 개인정보 약관 동의 획득 절차이다.

<표 3-1> 안드로이드 마켓 서비스 약관 동의 획득 절차



화면에서 ‘동의안함’을 클릭하는 경우, 이용자의 화면이 바로 전환됨과 동시에 안드로이드 마켓을 이용하는 것 자체가 불가능해진다. 이러한 상황에서 이용자는 링크되어 있는 서비스 약관을 개별적으로 살펴볼 필요성을 느끼지 못하고 서비스 이용을 위해서 타율적으로 동의 버튼을 클릭할 수밖에 없다. 문제는 아이폰의 ‘앱스토어’나 안드로이드 기반 스마트폰에서의 ‘안드로이드 마켓’은 모바일 앱을 다운로드받기 위해서 반드시 접속해야만 하는 서비스라는 점에 있다. 즉, 약관의 내용이 어떻게 변경되었는지에 대한 실제적 내용과 상관없이 이용자들은 반드시 동의를 해야만 하는 강제적인 상황에 놓이게 되고 이는 관련 서비스의 제공자가 임의로 약관을 변경하더라도 이에 저항할

100) 설문 13.

수 있는 제도적 장치가 이용자에게 존재하지 않음을 뜻한다.

2011년 9월 카카오톡의 개인정보 취급방침 변경 사례는 해당 서비스 제공자와 이용자 사이의 권력 불균형의 문제를 단적으로 보여준다. 국내에서만 2600만 명이¹⁰¹⁾ 넘는 이용자를 보유하고 있는 카카오톡은 개인정보보호법이 발효되기 이전에 기존 수집하던 개인정보 이외에 이메일 주소 등을 추가로 수집하겠다는 변경된 약관을 공지하면서 다음과 같은 화면을 제공하였다.

101) 국가인권위원회 보도자료, 인권위, 기업의 강제적 개인정보 수집 관련 일제 점검 및 가이드라인 제정 권고, 1쪽
http://www.humanrights.go.kr/04_sub/body02.jsp?NT_ID=24&flag=VIEW&SEQ_ID=603153

<그림 3-31> 2011년 9월 카카오톡 이용약관 변경



출처: 전자신문(2011.9.9.)¹⁰²⁾

카카오톡은 이처럼 ‘동의하지 않으시면 서비스를 이용할 수 없습니다. 카카오톡 계정을 삭제하시겠습니까?’라는 문구와 함께 ‘계정을 삭제하면 회원님의 모든 데이터가 삭제되고 친구들과 채팅도 할 수 없게 됩니다’라는 문구를 삽입하여 기존 이용자들이 변경된 취급방침에 동의하도록 종용하였다. 이처럼 기존의 서비스를 통하여 확보된 넓은 이용자층과 인프라를 기반으로 변경된 개인정보 취급방침에 동의하지 않는 이용자들에게 서비스 혜택을 강제로 차단하는 행위는 이용자로 하여금 동의에 대한 선택권을 사실상 박탈하는 행위와 크게 다르지 않다. 이는 다음과 같은 문제점을 야기한다.

102) "이메일 안주면 카카오톡 못쓴다" 이상한 약관강요 논란, 전자신문, 2011.9.9

1) 정보통신서비스 제공자에 대한 면죄부

정보통신망법 제22조 및 개인정보보호법 제15조에 의하여 적법한 개인정보의 수집 및 이용에 있어서 이용자의 동의는 필수불가결한 구성요건에 해당한다. 이러한 이용자의 의사표시와 법률행위를 모바일 환경을 통하여 강요하는 것은 정보통신서비스 제공자의 무분별하고 자의적인 개인정보 수집과 이용에 면죄부를 부여하는 격이 된다.

예를 들어 고유식별번호를 포함한 개인금융정보의 경우, <설문 22>에서 나타나는 바와 같이 이용자가 바람직하다고 여기는 개인정보의 허용기준 범위를 초과하고 있음에도 불구하고, 제공자의 강압적인 동의 절차에 의하여 '적법하게' 수집될 여지가 있다.

개인정보의 제3자 제공도 마찬가지이다. <설문 21>은 모바일앱의 무료 이용을 조건으로 개인정보가 광고회사와 같은 제3자에 제공되는 것에 대하여 43%의 응답자가 동의할 의사가 없다는 사실을 보여주고 있다. 그러나 모바일앱의 최초 구동 시 이용자가 주는 동의에 의하여 개인정보 취급방침에 따라 이미 정해진 제3자에게 자신의 개인정보가 제공될 수 있다는 사실을 이용자는 알 수 없다. 모바일 환경의 특성 상 동意的 의사결정을 내리기 전에 개인정보 취급방침이 이용자에게 미리 제공되지 않기 때문이다. 이처럼 형식적인 동의절차는 제3자에게의 개인정보 제공에 대한 이용자의 의사여부와 상관없이 해당 개인정보의 처리를 적법한 행위로 간주시킨다.

개인정보의 수집은 적법한 동시에 정당하여야만 한다.¹⁰³⁾ 이러한 맥락에서 강제되는 동의, 즉, 적법하나 정당하지 못한 동의의 획득 절차는 개인정보보호법제의 근본적 목적과 보호법익을 퇴색시키는 결과를 불러일으킨다.

2) 이용자의 개인정보 자기 통제의 상실

<설문 4>에서 나타나듯이 전체 응답자 가운데 63%에 해당하는 이용자가 자신에 관한 정보가 언제 누구에게 어느 범위까지 알려지고 또 이용되는지에 대하여 모르는 것을 우려하고 있다. <설문 5> 내지 <설문 8>의 설문결과에서 대부분의 이용자는 자신이 개인정보에 대한 통제 정도에 만족하지 않고 향후 이러한 이용자의 권한이 확대되어야 한다고 응답하여 개인정보자기결정권에 대한 중요성을 인식하고 있는 것으로 드러났다.

103) 개인정보보호법 제3조 1항.

3) 주기적으로 교체, 반복되는 모바일 앱 서비스

<설문 1>에서 나타나는 바와 같이 이용자는 평균적으로 많은 양의 모바일 앱 프로그램을 사용하고 있으며, 주기적으로 여러 앱 프로그램을 다운로드받고 삭제하는 행위를 반복하고 있는 것으로 드러났다.¹⁰⁴⁾ 일반 개인PC 프로그램과 달리 프로그램을 다운로드 받고 이내 삭제하는 반복적인 이용자의 행태는 이용자로 하여금 여러 제공자에 대한 개인정보 처리 동의를 여러 차례에 걸쳐 되풀이하게끔 만든다. 이러한 상황에서 ‘하거나 말거나’ 식의 강압적인 동의 절차에 이용자가 익숙해지게 된다면 이용자의 개인정보에 대한 통제는 매우 악화될 수밖에 없다. 여러 종류의 프로그램에 대한 형식적인 동의 절차를 반복해가는 과정에서 자신의 개인정보 현황에 대한 실질적이고 포괄적인 파악이 사실상 불가능해지기 때문이다.

4) 개인정보 취급방침에 대한 이용자의 친밀도 하락

개인정보의 자기 통제는 개인정보 취급방침을 숙지함으로써 실질적으로 강화될 수 있다. 그럼에도 불구하고 이용자들이 개인정보 취급방침을 제대로 읽지 않는 이유는 다른 아닌 형식적인 동의절차에서 비롯된다. 이와 관련하여 <설문 13>은 취급방침을 읽지 않는 응답자 가운데 79%가 서비스를 이용하기 위해서는 반드시 동의가 필요하므로 취급방침을 따로 읽을 필요성을 느끼지 못하고 있음을 보여주고 있다. 이처럼 ‘하거나 말거나’ 식의 동의절차는 이용자로 하여금 개인정보 취급방침의 중요성을 인지하는 것을 저해하여 결과적으로 자신의 개인정보에 대한 통제를 상실하는 결과를 초래한다.

5) 개인정보 보호의식의 약화

정보통신망법과 개인정보보호법이 보호하는 대상은 정보통신서비스 제공자, 정보처리자가 아닌 이용자와 정보주체이다. 그러나 이러한 법률의 기본원칙은 현행 모바일 환경에서 준수되고 있지 않다. 예컨대, 2011년 9월 개정된 카카오톡의 개인정보 취급방침은 그 절차가 일방적이고 강압적이었을 뿐만 아니라 변경에 대한 사전 공지가 전혀 없었다는 점도 논란의 여지가 되었다.¹⁰⁵⁾ 이는 개인정보에 대한 동의 획득과 수집항목을 결정

104) 한국인터넷 진흥원, 2011 상반기 스마트폰 이용실태조사, 11쪽.

105) 김동훈, 카카오톡이 고압적인 개인정보수집에 나선 까닭, 한국경제, 2011년 9월 18일자, <http://www.hankyung.com/news/app/newsview.php?aid=201109154360g>

하는 과정에서 이용자에게 실질적으로 어떠한 권한이 주어지지 못하고 있다는 사실을 반영한다. 설문조사의 결과는 이처럼 모바일서비스 제공자와 이용자 간의 관계에 있어서 절대적 약자에 놓인 이용자의 불만과 함께 개인정보 보호에 있어서 이용자가 소극적이고 수동적인 입장을 가질 수밖에 없는 현실을 반영하고 있다.¹⁰⁶⁾

나. 모바일 개인정보 취급방침에 대한 낮은 접근성

이용자가 자신의 개인정보가 어떻게 수집되고 이용되는지를 파악하기 위해서는 개인정보 취급방침의 내용에 대한 숙지가 요구된다. 그러나 <설문 12>에서 나타난 바와 같이 모바일 화면을 통하여 개인정보 취급방침을 읽거나 숙지하는 이용자의 수는 그리 많지 않으며, 취급방침에 대한 이용자의 접근성을 저해하는 요소 또한 다수 존재한다.¹⁰⁷⁾

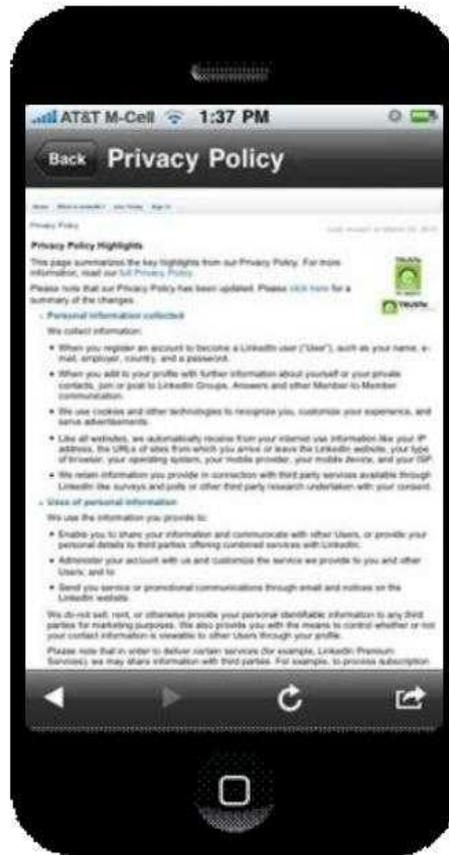
1) 작은 화면을 통한 방대한 정보의 표시

이용자가 모바일 앱을 다운로드한 후 개인정보 취급방침을 접할 때 가지는 문제점 가운데 하나는 숙지의 난해함에 있다. 이는 일반 컴퓨터 모니터를 통하여 다루어지던 기존의 개인정보 취급방침이 스마트폰과 같은 작은 모바일 단말기에도 동일한 방식으로 제공되기 때문이다.

106) 설문 5, 설문 6, 설문 7, 설문 9.

107) 설문 12, 설문 13, 설문 14.

<그림 3-32> 아이폰에 나타나는 개인정보 취급방침의 예



<그림 3-32>는 애플의 실제 아이폰 크기에 맞추어 표시되고 있는 개인정보 취급방침의 예이다. 이처럼 일반 사무용 디스플레이에서 적용되는 형식의 약관을 모바일 스크린에 동일하게 적용하는 경우, 이용자는 작은 화면에 나타나는 많은 양의 정보를 읽는데 주저하게 되는 경향이 있다. <설문 13>은 전체 응답자 가운데 75%가 이러한 모바일기기의 특성을 개인정보 취급방침을 읽지 않는 이유로 답하였음을 보여준다.¹⁰⁸⁾

정보통신망법시행령 제14조 제1항에 따르면 인터넷 홈페이지의 첫 화면 또는 첫 화면

108) <그림 3-18> 참조.

과의 연결화면을 통하여 개인정보 취급방침을 제공하는 경우 정보통신서비스 제공자 등은 ‘글자 크기, 색상 등을 활용하여 이용자가 개인정보 취급방침을 쉽게 확인할 수 있도록 표시’하여야 한다. 그러나 조사 결과, 카카오톡, 다음, 네이버 등 대다수의 모바일 서비스가 제공하는 개인정보 취급방침은 아직까지 이러한 모바일 환경의 특성을 제대로 반영하고 있지 않은 것으로 나타났다. 다음은 삼성의 스마트폰 갤럭시S2를 기준으로 (주)다음(Daum)의 모바일 메신저 앱 프로그램인 ‘마이피플’의 개인정보 취급방침을 실제 크기로 표시한 것이다.

<그림 3-33> 한 화면에 나타나는 개인정보 취급방침



그림에서 알 수 있듯이, 한 화면에 나타나는 개인정보 취급방침은 그 글자의 크기가 상당히 작을 뿐만 아니라 포함하고 있는 내용의 분량 또한 상당히 방대하다. 또한 마이

피플 앱의 경우 이러한 해당 화면을 손가락 터치를 통하여 확대 및 축소할 수 없는 것으로 드러났다. 전혀 읽을 수 없는 미세한 글자들이 확대할 수 없는 상황에서 하나의 작은 화면 안에 방대하게 들어가 있는 것이다. 이처럼 마이피플을 비롯하여 로드뷰, 스토어뷰 등 (주)다음에서 제공되는 여러 모바일 앱의 경우 이용자는 사실상 개인정보 취급방침의 내용을 확인하기 불가능하며 동 취급방침의 자세한 내용을 알기 위하여 일반 모니터 혹은 태블릿PC 등을 따로 이용해야만 하는 번거로움을 가지게 된다.

2) 필수항목에 대한 인지의 어려움

많은 분량의 내용을 일괄적으로 제공하는 것은 해당 서비스의 이용자가 반드시 알아야만 하는 중요한 내용과 그렇지 않은 부가적인 내용의 구분을 어렵게 만든다. 정보통신망법 제27조의 2는 개인정보 취급방침에 반드시 포함되어야만 하는 항목을 다음과 같이 규정하고 있다.

<표 3-2> 정보통신망법 제27조 2에 따른 개인정보 취급방침 필수항목

-
1. 개인정보의 수집·이용 목적, 수집하는 개인정보의 항목 및 수집방법
 2. 개인정보를 제3자에게 제공하는 경우 제공받는 자의 성명, 제공받는 자의 이용 목적과 제공하는 개인정보의 항목
 3. 개인정보의 보유 및 이용 기간, 개인정보의 파기절차 및 파기방법
 4. 개인정보 취급위탁을 하는 업무의 내용 및 수탁자
 5. 이용자 및 법정대리인의 권리와 그 행사방법
 6. 인터넷 접속정보파일 등 개인정보를 자동으로 수집하는 장치의 설치·운영 및 그 거부에 관한 사항
 7. 개인정보 관리책임자의 성명 또는 개인정보보호 업무 및 관련 고충사항을 처리하는 부서의 명칭과 그 전화번호 등 연락처
-

그러나 특정 항목에 관하여 추가적인 정보를 제공하고 이를 자세하게 상술하고 있는 현행 개인정보 취급방침의 표기방식은 오히려 이용자로 하여금 필수항목에 대한 정확한

인식을 하지 못하도록 방해하고 있다. 다음은 모바일게임 개발사 게임빌의 개인정보 취급방침이다.

<그림 3-34> 모바일게임 개발사 게임빌 개인정보 취급방침

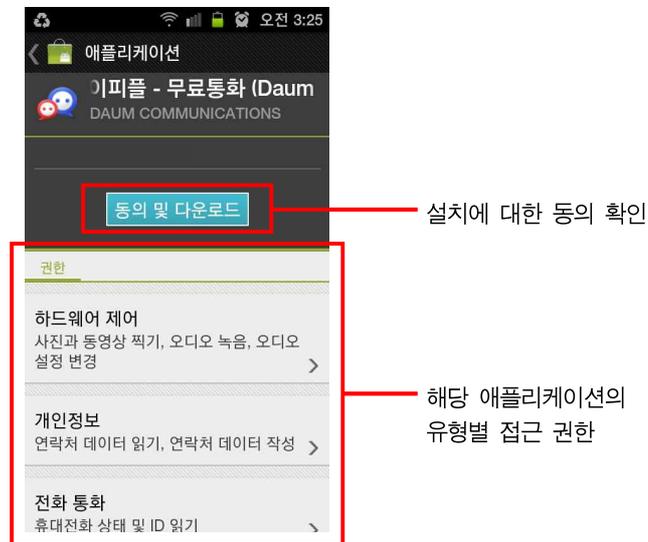


<그림 3-34>에서 나타나는 바와 같이 게임빌의 개인정보 취급방침은 자사의 개인정보 처리 사항을 긴 설명문의 형식을 통하여 공개하고 있다. 이러한 전달방법은 이용자로부터 하여금 <표 3-4>에서 다루고 있는 취급방침의 핵심적인 항목에 대하여 정확한 인지를 하기 어렵게 만든다.

3) 모바일 개인정보 취급방침의 후 공개

모바일서비스에 개인정보 취급방침은 개인정보처리자가 개인정보 수집에 대한 동의를 획득하고 난 후에야 비로소 공개가 되는 문제점이 있다. 안드로이드 체제를 기반으로 한 스마트폰에서 모바일 앱을 다운로드 받는 경우 대부분의 앱은 현재 다음과 같은 다운로드 방식을 취하고 있다.

<그림 3-35> 안드로이드 마켓에서 모바일 앱의 다운로드 방식



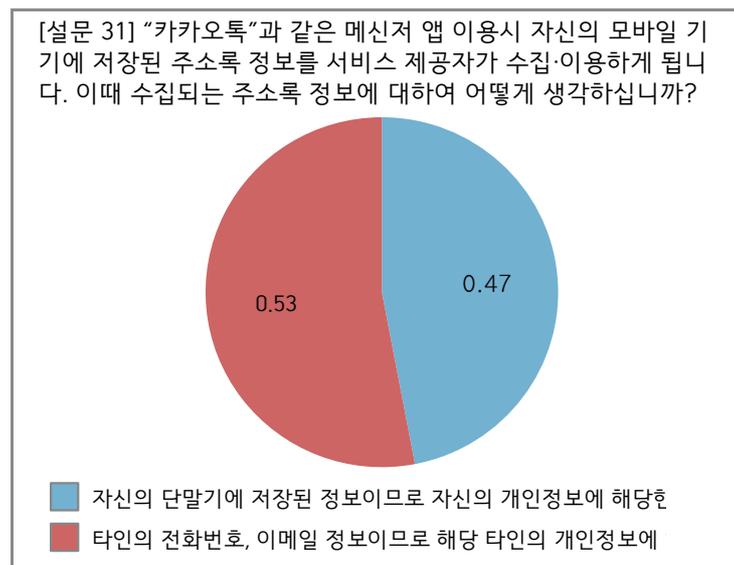
위와 같은 절차를 통하여 모바일 앱을 다운로드받는 경우 이용자는 개인정보 취급방침에 접근할 수 있는 기회를 상실하게 된다. 개인정보 취급방침이 개인정보의 수집·이용 목적, 수집되는 개인정보의 항목 등을 설명하는 것과 달리 하드웨어 제어 등과 같은 접근권한은 단지 특정 모바일 앱이 모바일 단말기에 대하여 어떠한 액세스가 가능한지를 설명하는 것에 불과하기 때문이다.

이러한 방식을 통한 개인정보의 수집은 이용자로 하여금 개인정보 취급방침에 대한 이해가 없이 동의와 함께 앱 다운로드를 동시에 하도록 종용한다. 모바일 앱을 다운로드받고 실행시킨 사후에 이용자가 개인정보 취급방침을 읽을 수 있다하더라도 동의가 이미 이루어졌다는 점에서 개인정보를 보호할 수 있는 기회는 상실된다.

다. 모바일 기술에 대한 법적 기준의 혼란

<설문 4>에서 나타나는 바와 같이 이용자의 동의 없는 개인정보의 무단 수집·이용은 국내외를 막론하고 모바일 개인정보에서 가장 심각한 문제이다. 정보통신망법과 개인정보보호법에 따라 예외사항을 제외하고 이용자의 동의 없는 개인정보의 처리는 위법으로서 법률의 실효성에 대한 문제가 아니다. 그러나 최근 급속도로 성장하는 기술의 발달과 독특한 아이디어의 결합은 기존의 법률이 포섭할 수 없는 새로운 개인정보의 수집양태를 생산하고 있다. 현행 법률이 이러한 특정 모바일 앱의 개인정보 수집방식 또는 수집목적 등에 대하여 그 적법성에 확신을 가질 수 없게 되면서 모바일 개인정보의 보호에 대한 혼란은 증가할 전망이다.

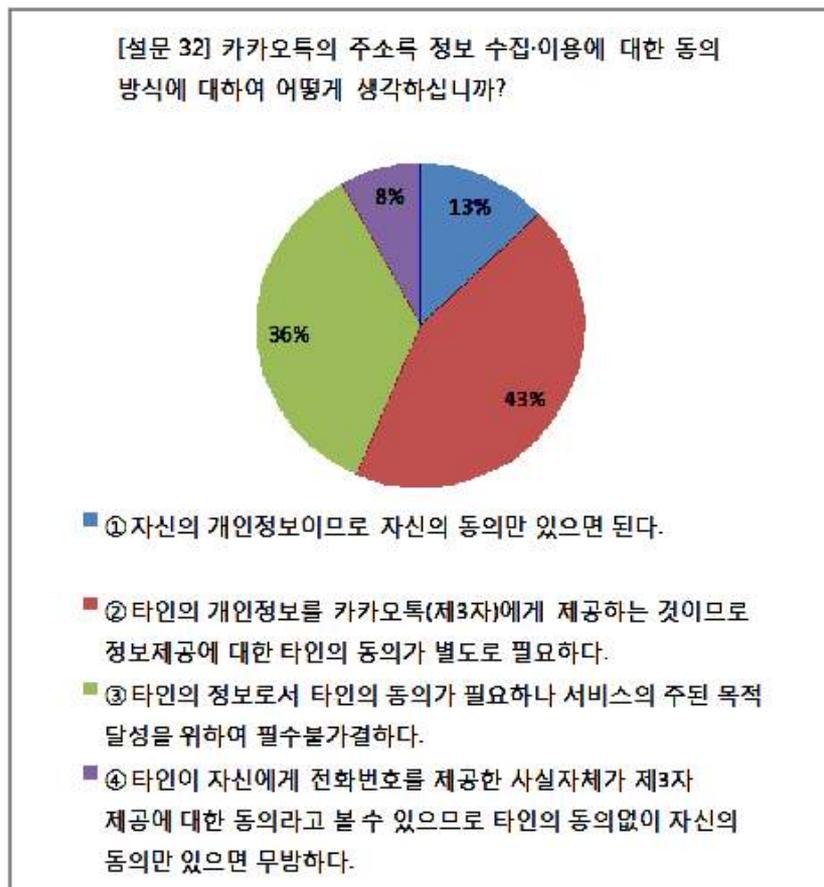
이용자의 주소록 내에 저장된 제3자의 전화번호를 제3자의 동의 없이 수집할 수 있도록 규정하고 있는 카카오톡의 취급방침은 이러한 대표적 예이다.¹⁰⁹⁾ 이와 관련하여 먼저 카카오톡 개인정보 수집방법과 친구추천 기능에 대하여 이용자의 인식도를 조사하였다.



109) 카카오톡 개인정보 취급방침 1항 가.

<설문 31>은 카카오톡 이용에 동의한 이용자의 스마트폰 주소록을 통하여 자동적으로 수집되는 제3자의 전화번호가 누구의 개인정보에 해당하는지에 대한 응답자의 견해를 반영한다. 이에 따르면 전체 응답자 가운데 53%에 해당하는 응답자가 주소록에 저장된 타인의 전화번호는 자신의 모바일기기에 저장되어 있다 하더라도 자신의 정보가 아닌 타인의 개인정보라고 답하였다.

<그림 3-37> 카카오톡 주소록 개인정보 수집에 대한 이용자의 인식



카카오톡의 개인정보 처리 동의 방식에 대한 이용자의 인식은 <설문 32>가 보여주는

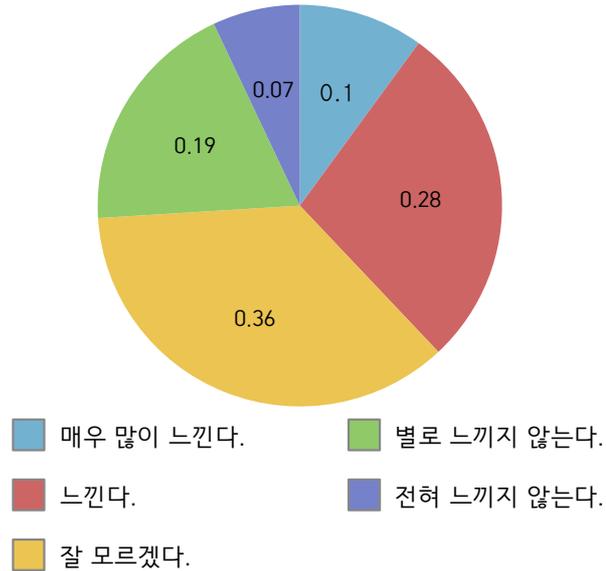
바와 같다. 이에 따르면 가장 많은 43%의 응답자가 자신의 주소록에 저장된 타인의 전화번호에 대하여 해당 이용자의 별도의 동의가 필요하다고 답하였다. 다음으로 타인의 정보로서 타인의 동의가 필요하지만 카카오톡 서비스의 주된 목적 달성을 위해서는 어쩔 수 없다고 응답한 이가 36%에 해당하였다. 이는 이용자가 일일이 상대방의 전화번호를 입력하지 않아도 자동적으로 프로그램이 이용자의 대화상대 리스트를 만들어주는 기능의 필요성의 인정을 의미한다. 반면 타인이 자신에게 전화번호를 제공한 사실 자체가 카카오톡에 대한 개인정보 제공에 대한 동의로 볼 수 있다고 답한 이용자가 13%, 자신의 개인정보이므로 자신의 동의만 있으면 된다고 답한 이는 전체 응답자의 8%에 불과하였다.

정보통신망법 제2조 제1항 제6호 및 개인정보보호법 제2조 제1항에 따르면 개인정보란 생존하는 개인에 관한 정보로서 개인을 알아볼 수 있는 정보를 뜻한다. 이에 따라 제3자의 휴대전화번호는 당연히 제3자의 개인정보에 해당한다. <설문 32>의 결과는 스마트폰 기술의 발전에 따라 특정 개인의 주소록에 저장된 제3자의 전화번호 추출이 가능해지면서 이용자가 가지게 되는 기준의 혼란을 반영하고 있다.

정보통신서비스 제공자의 입장에서 이용자의 동의 없이 개인정보를 수집하기 위해서는 정보통신망법 제22조 제2항의 요건을 충족시켜야 한다. 이에 따르면 정보통신서비스 제공자는 동 서비스 제공에 관한 계약을 이행하기 위하여 필요한 개인정보로서 경제적·기술적인 사유로 통상적인 동의를 받는 것이 뚜렷하게 곤란한 경우 동의의 획득을 얻지 않고도 개인정보를 수집할 수 있다. 또한 개인정보보호법 제15조 제1항 제4호는 정보주체와의 계약의 체결 및 이행을 위하여 불가피하게 필요한 경우 정보주체의 동의 없이 개인정보를 수집할 수 있다.

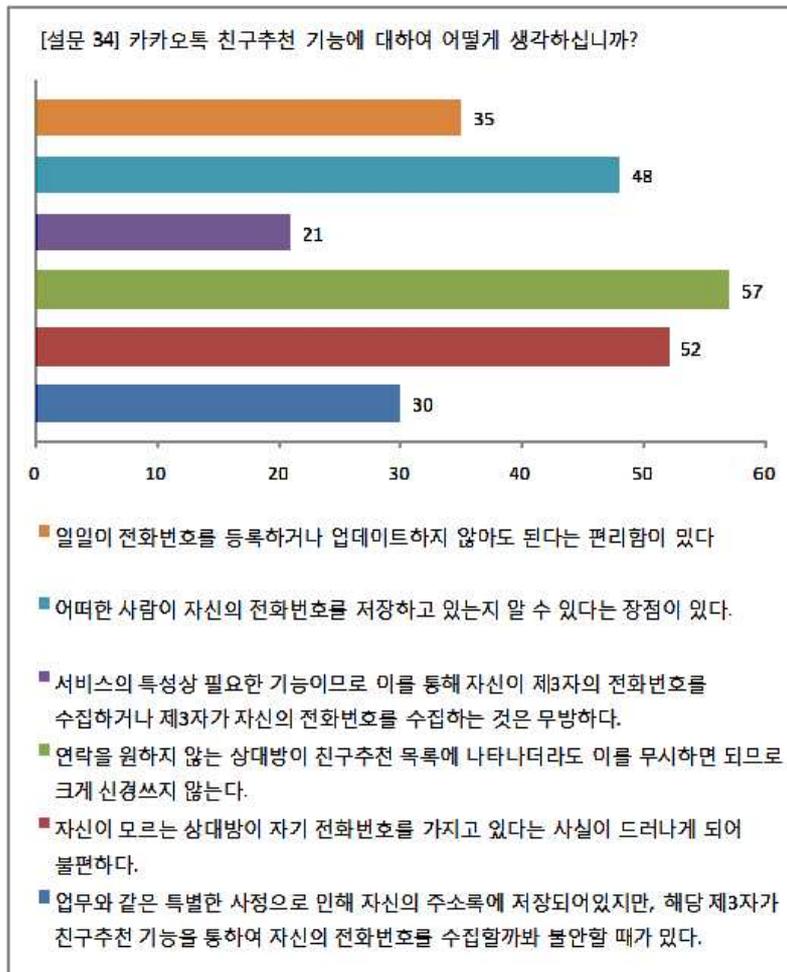
그러나 이용자의 주소록을 통하여 제3자에 대한 전화번호를 수집하는 행위가 해당 법률의 내용을 충족시키는지에 대해서는 논란이 있다. 제3자의 입장에서는 카카오톡 이용자에게 전화번호를 제공하였다는 사실만으로 어떠한 동의 절차 없이 자신도 모르는 사이에 개인정보가 수집되기 때문이다.

[설문 33] 카카오톡 “친구추천” 기능과 관련하여 개인정보에 대한 불안감을 느낀 적이 있습니까?



카카오톡의 친구추천 기능은 이용자가 상대방의 전화번호를 보유하고 있지는 않지만 상대방이 이용자의 전화번호를 보유하고 있는 경우, 자신의 전화번호를 가지고 있는 이용자들의 정보를 이용자의 친구추천 목록에 표시하는 기능이다. 이러한 친구추천 기능에 대하여 개인정보에 대한 불안감 여부를 설문한 결과, 전체 응답자 가운데 38%에 해당하는 응답자가 불안감을 많이 느끼거나 느낀다고 답하였고, 이와 비슷한 36%의 응답자가 확실하지 않다는 반응을 보였다. 불안감을 별로 느끼지 않거나 전혀 느끼지 않는다고 답한 응답자 또한 각각 19%, 7%에 해당하여 친구추천 기능에 대한 응답자의 견해가 어느 한쪽으로 치우치지 않고 다양하게 분포되어 있음을 보여준다.

<그림 3-39> 카카오톡 친구추천 기능에 대한 이용자의 인식



친구추천 기능에 대한 이용자의 의견을 복수응답 형식으로 설문한 결과, 연락을 원하지 않는 상대방이 친구추천 목록에 표시되더라도 이를 무시하면 되므로 크게 신경 쓰지 않는다는 설문이 가장 많은 호응을 얻었다. 다음으로 52%의 응답자가 자신이 모르는 상대방이 자기 전화번호를 가지고 있다는 사실에 대하여 불편함을 느낀다고 답변한 반면, 48%의 응답자는 어떤 사람이 자신의 전화번호를 저장하고 있는지 알 수 있다는 장점이

있다고 답변하여 동일한 기능에 대한 엇갈린 반응이 유사한 비율로 나타나고 있음을 알 수 있다. 또한 일일이 전화번호를 등록하거나 업데이트하지 않아도 된다는 편리함이 있다고 답한 이가 35%, 업무와 같은 특별한 사정으로 인해 주소록에 저장이 되었지만, 해당되는 제3자가 친구추천 기능을 통하여 자신의 전화번호를 수집할까봐 불안할 때가 있다고 답한 응답자는 30%에 달하였다.

설문조사의 결과는 친구추천 기능에 대한 이용자의 상반된 견해를 동시에 반영하고 있다. <설문 33>에서 드러나는 바와 같이 일부 이용자가 친구추천 기능으로 인한 개인정보의 불안감을 드러내는 반면, 해당 기능에 대하여 긍정적인 반응을 보이는 응답자 또한 적지 않았다. 또한 <설문 34>에서 다수의 응답자들은 해당 서비스의 역기능과 함께 순기능 또한 존재하고 있다는 의견을 나타내고 있다.

친구추천 서비스는 모르는 사람의 전화번호, 이메일, 사진에 대하여 이용자의 접근을 가능하게 한다는 점에서 개인정보 보호에 취약성을 가지고 있다. 카카오톡 뿐만 아니라 오늘날 다수의 이용자가 이용하고 있는 트위터, 페이스북 등의 SNS앱 또한 이용자가 모르는 사람에 대한 개인정보를 쉽게 접근할 수 있도록 비슷한 기능의 서비스를 제공하고 있다. 페이스북의 '알 수도 있는 사람', 싸이월드의 '이메일 주소로 친구찾기' 서비스가 이러한 예이다.

문제는 모바일 인터넷을 이용한 새롭고 편리한 아이디어가 여러 이용자들의 호응을 얻고 있는 상황에서 개인정보 보호를 근거로 이러한 새로운 서비스 형태를 어떤 기준을 통하여 어느 정도로 규율할 것인지에 대하여 법과 정책의 기준이 확립되지 않았다는 것이다. 서비스마다 다른 개인정보 수집행태를 통일적으로 규율하기도 힘들고, 현행 법률이 규정하고 있는 일반적인 원칙을 근거로 개별 취급방침에 대하여 위법성 여부를 일일이 판단하는 것 또한 쉽지 않기 때문이다.

라. 무분별한 개인정보의 수집

정보통신망법 제23조 제2항에 따르면 정보통신서비스 제공자가 이용자의 개인정보를 수집하는 경우에는 정보통신서비스의 제공을 위하여 필요한 최소한의 정보를 수집하여야만 한다. 개인정보보호법 제16조 제1항 역시 이러한 최소 정보 수집의 원칙을 규정하

여 개인정보처리자로 하여금 ‘목적에 필요한 최소한의 개인정보’를 수집하도록 하고 있으며 이러한 정보처리자의 의무는 동법 제3조 제1항과 제2항의 개인정보 보호 원칙에 의하여 재차 확인된다.

1) 개인정보 수집 목적과 무관한 개인정보의 수집

수집된 개인정보가 반드시 필요한 최소한의 개인정보인지를 판단하는 기준은 개인정보 수집·이용의 목적에 근거한다.¹¹⁰⁾ 따라서 목적에 필요한 최소한의 개인정보 이외의 부가적인 정보를 수집·이용하는 것은 현행법의 위반을 구성한다. 그러나 <설문 16>에 서 나타나는 바와 같이 대다수의 응답자가 수집 목적과 무관한 개인정보의 수집에 대하여 인지하고 있는 것으로 드러났다. 다음은 2010년 9월 논란이 되었던 카카오톡의 개인정보 취급방침이다.¹¹¹⁾

<표 3-3> 카카오톡의 변경 전 개인정보 취급방침

개인정보의 수집·이용 목적	가. 카카오톡 기본 기능의 제공 나. 서비스 제공에 관한 계약 이행 및 서비스 제공에 따른 요금 정산 다. 회원관리 라. 신규 서비스 개발 및 마케팅·광고에의 활용
수집하는 개인정보의 항목	- 중략 -
	넷째, 유료 서비스 이용 과정에서 아래와 같은 정보들이 수집될 수 있습니다. 휴대폰 결제시 이동전화번호, 통신사, 결제승인번호 등 신용카드 결제시 카드사명, 카드번호 등 계좌이체시 은행명, 계좌번호 등

110) 정보통신망법 제23조, 개인정보보호법 제3조 및 제16조.

111) 이에 대한 논란이 끊이지 않자 결국 카카오톡은 2010년 10월 초 공지사항에서 “방송통신위원회 권고로 법률적 검토를 거쳐 개인정보 취급방침이 변경되었다”며 “실명, 주민등록번호, 주소, 이메일 주소, 타서비스 이용 아이디 또는 계정 정보는 현재는 수집하지 않는 정보며, 서비스에 꼭 필요할 경우 회원 동의 과정을 거친 후 동의한 회원에 한해 해당 정보를 직접 입력하는 경우에만 수집이 가능하고 자동으로 수집되지는 않는다”고 설명했다.

<표 3-5>에 제시된 개인정보 취급방침은 정보통신서비스 제공자로 하여금 휴대폰 결제 이동전화번호, 통신사, 결제승인번호, 신용카드 결제시 카드사명, 카드번호, 계좌이체시 은행명, 계좌번호와 같은 개인금융정보를 수집할 수 있도록 규정하여 개인정보의 수집 목적의 범위를 벗어난 것이 아니냐는 논란을 불러일으켰고, 결국 방송통신위원회의 권고를 통하여 변경되었다.

2) 광범위한 개인정보 수집·이용 목적

정작 문제가 되는 것은 수집 목적 자체를 과도하게 설정하는 것에 있다. 정보통신망법과 개인정보보호법은 개인정보 수집 목적을 벗어나는 범위에서의 개인정보 수집을 금지하고 있지만 어떠한 목적을 설정하는지에 대하여는 규율하지 않는다.

<표 3-5>의 예를 들어, 카카오톡의 '신규서비스 개발 및 마케팅·광고에의 활용'이라는 목적은 정보통신서비스 제공자 자신이 설정한 목표이며 이러한 목표가 모바일 메신저라는 해당 앱의 주된 기능에 반드시 필요한 지에 대하여 판단 할 수 있는 주체는 없다. 이에 따라 정보통신서비스 제공자는 정보통신망법 제24조 및 개인정보보호법 제16조 위반을 면하기 위하여 처음부터 목적의 범위를 광범위하게 설정할 수 있다. 즉, 서비스 목적을 먼저 설정하고 그 범위 내에서 개인정보를 수집하는 것이 아니라, 수집하기를 희망하는 개인정보를 구체적으로 설정한 후 그에 맞는 개인정보 수집·이용 목적을 도출해내는 것도 가능하다.

3) 선택적 동의 절차

이처럼 광범위한 수집 목적에 의해 또는 목적의 범위를 벗어난 수집항목의 설정에 의해 무분별한 개인정보의 수집이 이루어질 수 있는 가장 큰 원인은 동의의 획득 과정에서 선택적 동의(opt-in 또는 opt-out)제도가 국내에 확실하게 정착되지 않았기 때문이다. 개인정보보호법 제22조에 제2항에 따라 개인정보처리자는 개인정보의 처리에 대하여 정보주체의 동의를 받을 때에는 정보주체와의 계약 체결 등을 위하여 동의 없이 처리할 수 있는 개인정보와 정보주체의 동의가 필요한 개인정보를 구분하여야만 한다.¹¹²⁾ 또한 동조 제4항은 개인정보처리자는 정보주체가 선택적으로 동의할 수 있는 사항을 동의하

112) 개인정보보호법 제22조 제2항

지 아니한다는 이유로 정보주체에게 재화 또는 서비스의 제공을 거부할 수 없음을 규정하고 있다.¹¹³⁾

<설문 9> 내지 <설문 11>의 결과에서 나타났듯이 대다수의 응답자들은 이처럼 필수적으로 필요한 개인정보와 추가적인 목적을 위하여 수집되는 부가정보의 구분을 통한 선택적 동의 절차에 대하여 많은 관심을 보이고 있다.

카카오톡의 주된 서비스는 이용자로 하여금 전화번호를 공유하고 있는 친구와 1:1 또는 그룹채팅을 무료로 즐길 수 있도록 메신저 기능을 제공하는 것에 있다. 이에 비추어 볼 때 ‘이벤트 및 광고성 정보 제공 및 참여기회 제공’이라는 개인정보의 수집 목적¹¹⁴⁾은 주된 메신저 기능과는 별개의 목적이라고 볼 수 있다. 이처럼 개인정보 처리의 목적이 구분되는 경우 채팅이라는 목적에 따라 필요한 최소한의 개인정보(예를 들어 전화번호)는 필수적 동의사항으로 규정하되, 마케팅·광고에의 활용이라는 목적에 따라 수집되는 이메일 주소 등의 추가적인 개인정보는 그 동의에 대한 여부를 이용자의 선택에 맡기는 것이 바람직하다.

마. 개인정보 동의에 대한 철회

정보통신망법 제30조 제1항은 이용자가 정보통신서비스 제공자에 대하여 언제든지 개인정보 수집·이용·제공 등의 동의를 철회할 수 있음을 규정하고 있다.¹¹⁵⁾ 또한 동조 제3항은 제1항에 따라 이용자가 동의를 철회하면 지체 없이 수집된 개인정보를 파기하는 등 필요한 조치를 하여야 함을 명시하고 있으며, 동조 제6항은 정보통신서비스 제공자가 제시하는 철회의 방법이 개인정보의 수집방법보다 더 용이하게 이루어져야할 것을 규정하고 있다.¹¹⁶⁾

113) 개인정보보호법 제22조 제4항

114) 카카오톡 개인정보 취급방침 2. 개인정보의 수집 및 이용목적 라. 신규 서비스 개발 및 마케팅·광고에의 활용 신규 서비스 개발 및 맞춤 서비스 제공, 통계학적 특성에 따른 서비스 제공 및 광고 게재, 서비스의 유효성 확인, 이벤트 및 광고성 정보 제공 및 참여기회 제공, 접속빈도 파악, 회원의 서비스이용에 대한 통계

115) 정보통신망법 제30조 1항.

116) 정보통신망법 제30조 3항 및 6항.

또한 정보통신망법 제26조에 따르면 정보통신서비스 제공자 등이 영업의 전부 또는 일부의 양도·합병 등으로 그 이용자의 개인정보를 타인에게 이전하는 경우에는 인터넷 홈페이지 게시, 전자우편 등 대통령령으로 정하는 방법에 따라 개인정보를 이전하려는 사실, 개인정보를 이전받는 자의 성명·주소·전화번호 및 그 밖의 연락처, 그리고 이용자가 개인정보의 이전을 원하지 아니하는 경우 그 동의를 철회할 수 있는 방법과 절차를 이용자에게 알려야 한다.

그러나 정보통신망법 제30조의 규정과 달리, <설문 25>는 실제 개인정보 동의에 대한 철회 절차가 동의 절차보다 더 까다롭고 복잡하다는 이용자의 인식을 반영하고 있다. 이하의 표는 2011년 10월 1일자로 분할되는 SK 텔레콤(주)의 개인정보 이전과 관련하여 개인정보 제공 동의를 철회에 대한 이용자의 접근성을 도식화 한 것이다.¹¹⁷⁾

117) 삼성 갤럭시 S2 스마트폰 이용자 대상.

<표 3-4> 스마트폰을 이용한 철회의 절차

<p><1단계> 문자메세지</p>	<ul style="list-style-type: none"> - 개인정보이전 안내문 소개 - 안내문에 대한 웹사이트 주소가 링크되어 간편하게 안내문에 접속이 가능
<p><2단계> 링크를 통한 안내문 접속</p>	<ul style="list-style-type: none"> - 사업자 분할에 따른 개인정보 이전 안내 - 어떠한 개인정보가 누구에게 이전되는지에 대하여 비교적 상세한 설명하고 있음 - 기존 개인정보의 수집·이용에 대한 동의에 대하여 이용자가 철회할 수 있다는 사실과 그 절차에 대하여 적시하지 않음 - 자세한 사항에 대하여 링크가 불가능한 웹사이트 주소를 기재하여 소개
<p><3단계> 이용자가 직접 해당 웹사이트에 접속하는 경우</p>	<ul style="list-style-type: none"> - 분할에 대한 동의 철회가 가능하다는 사실과 철회의 절차가 설명되어 있음 - 동의를 철회하기 위해서는 이용자의 이동전화번호, 개인정보 제공동의 철회 요청 메일을 특정 이메일 주소로 발송해야 함
<p><4단계> 메일 발송을 하는 경우</p>	<ul style="list-style-type: none"> - 본인확인 등 필요절차를 거쳐 동의 철회

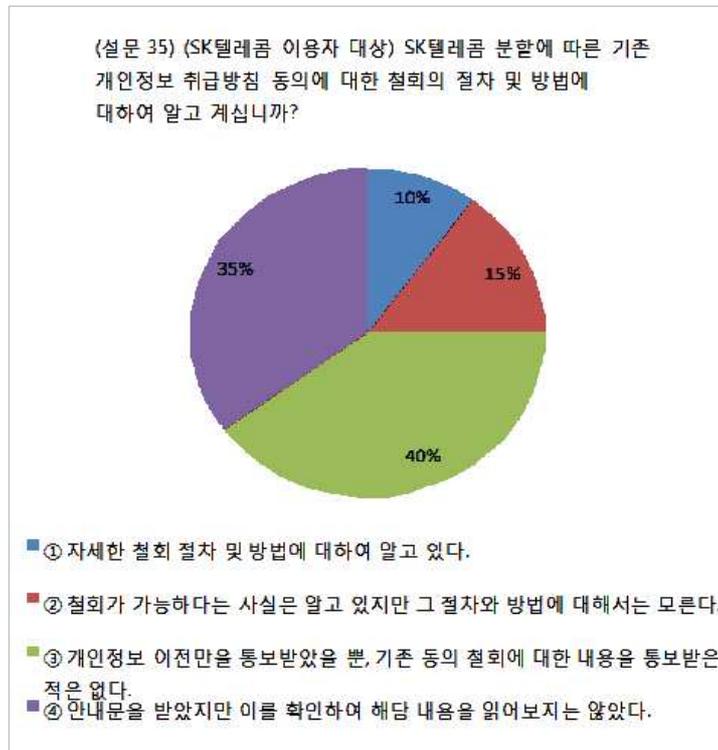
SK 텔레콤(주)는 스마트폰을 사용하는 자사고객에게 정보통신사업자 및 개인정보처리자가 변경된다는 사실과 어떠한 개인정보가 누구에게 이전되는지에 대하여 이용자에게 설명하고 있다. 그러나 <표 3-6>에서 나타나듯이 동 안내문은 개인정보처리자가 변경될 때 이용자가 기존의 개인정보 수집·이용에 대한 동의를 철회할 수 있다는 사실을 알리지 않고 있다. 이 경우, 개인정보 이전과 관련하여 자신에게 어떠한 권리가 주어지는지에 대하여 제대로 알지 못하는 이용자들은 해당 안내문만을 읽고 동의의 철회가 가능하다는 사실을 파악하기 힘들다. 이러한 소극적이고 형식적인 통보 방식의 결과, <설문 26>에서 나타나는 바와 같이 철회의 경험이 있는 자보다 없는 자가 더 많은 비율을 차지하고 있으며, 동의 후 철회가 가능하다는 사실을 모르는 이용자가 전체 응답자 가운데

데 44%에 달하였다.

또한 기존 개인정보 제공 동의에 대한 철회 및 철회 절차에 대하여 SK 텔레콤(주)는 “분할에 관한 자세한 사항은 www.sktelecom.com 또는 www.tworld.co.kr 를 참조하시기 바랍니다”라는 언급만을 하고 있고, 해당 웹주소를 링크시켜 놓지 않음에 따라 이용자가 휴대하고 있는 단말기의 웹 브라우저를 통한 간편하고 용이한 접근성을 저해하고 있다.

정보통신사업자의 이러한 통보절차가 통용된다면 결국 이용자의 권리는 확보될 수 없다. 개인정보의 이전에 따른 기존 동의의 철회가 가능하다는 사실을 이용자가 처음부터 인지하기 매우 어렵고, 동의 철회의 절차를 파악하기 위해서는 안내문에 소개된 웹사이트의 주소를 별도의 웹 브라우저를 통해 이용자가 일일이 입력해야만 한다는 번거로움이 따르기 때문이다.

<그림 340> SK텔레콤 개인정보 이전 통보 및 철회 절차에 대한 인지도



<설문 35>는 SK 텔레콤(주)로부터 개인정보 이전 통보를 받은 이용자들이 철회의 절차 및 방법에 대하여 얼마나 인지하고 있는지를 나타내고 있다. 이에 따르면 자세한 철회 절차 및 방법에 대하여 알고 있다고 응답한 비율이 전체의 10%에 그친 반면, 35%의 응답자가 안내문을 받았지만 해당 내용을 읽어보지는 않았다고 답하였고, 40%의 응답자가 개인정보 이전만을 통보받았을 뿐, 기존 동의 철회에 대한 내용을 통보받은 적이 없다고 답하여 앞서 언급된 문제점의 심각성을 반영하고 있다.

제3절 사례를 통하여 드러난 문제점

1. 모바일서비스상 개인정보 불법수집 사례

모바일서비스를 통한 개인정보의 불법수집 사례는 그리 많지 않다. 그러나 스마트폰을 비롯한 모바일기기가 일반 대중에게 널리 보급된 시점이 불과 2년 전이라는 사실을 감안할 때, 모바일 이용에 따른 프라이버시 및 개인정보의 침해는 향후 증가할 전망이다.

가. 증권통 사건¹¹⁸⁾

1) 사실관계

안드로이드 서비스를 기반으로 한 증권정보 애플리케이션 ‘증권통’은 사용자의 동의여부와 상관없이 ‘국제모바일 단말기 인증번호(IMEI)와 범용 가입자식별모듈(USIM) 일련번호의 조합’ 정보를 자동으로 추출하도록 설계되었다. 또한 운영체제와 단말기의 차이에 따라 USIM 일련번호를 가져오지 못하는 경우에는 ‘IMEI와 사용자 개인 휴대전화번호의 조합’ 정보를 해독하여 증권통을 운영하는 회사 서버에 저장하였다. 이처럼 저장된 번호의 조합은 서비스 이용자가 다시 접속하는 경우 이용자의 동일성을 식별하고 별도 로그인 없이 바로 이용자가 등록해 놓은 관심종목을 보여주는 용도로 활용되었다.¹¹⁹⁾ 증권통 앱을 공급하는 이토마토사는 해당 앱을 통하여 IMEI와 USIM 일련번호 82,413건, IMEI와 개인용 휴대전화번호 1,003건을 수집하였다.¹²⁰⁾

2) 피고인의 주장

정보통신망법 제22조 위반을 근거로 검찰이 기소한 동 사건에서 피고인은 1) IMEI와 USIM과 같은 단말기 고유번호가 휴대전화번호와 같은 개인정보에 해당하지 않으며, 2)

118) 2010고단5343.

119) 2010고단5343.

120) 2010고단5343.

해당 정보가 개인정보라 할지라도 정보통신망법 제22조 제2항 제1호¹²¹⁾ 및 방송통신위원회 개인정보보호지침 제5조 제1항¹²²⁾에 따라 서비스이용계약의 이행을 위하여 필요한 개인정보의 수집은 이용자의 동의를 얻을 필요가 없다고 주장하였다. 또한 피고인은 3) 단말기 고유번호가 정보통신망법 제27조의2 제2항 제6호에서 규정한 인터넷 접속정보파일에 불과하여 같은 항 제1호의 개인정보와는 달리 별도의 동의를 얻을 필요가 없으며, 4) 스마트폰에 증권통 앱을 설치하는 경우 안드로이드 운영체제에서 제공하는 안내문에 따라 이용자로부터 동의를 받았다고 주장하였다.

3) 법원의 판단

서울중앙지법은 우선 IMEI와 USIM과 같은 단말기 고유번호가 개인정보에 해당한다고 판시하였다. 정보통신망법 제2조 제1항 제6호에 따르면 개인정보란 생존하는 개인에 관한 정보로서 성명·주민등록번호 등에 의하여 당해 개인을 알아볼 수 있는 부호·문자·음성·음향 및 영상 등의 정보이다. 또한 동조는 해당 정보만으로는 특정 개인을 알아볼 수 없더라도 ‘다른 정보와 쉽게 결합하여 알아볼 수 있는 경우’에는 그 정보는 개인정보에 속한다고 규정하고 있다. 휴대전화번호와 달리 IMEI 및 USIM은 해당값 자체만으로는 이용자에 대한 정보를 확인하거나 개인을 식별해내는 것이 불가능하다. 문제는 이러한 단말기 고유번호가 다른 정보와 쉽게 결합하여 특정 개인을 알아볼 수 있는 정보에 해당하는가이다. 이에 대하여 법원은 ‘쉽게 결합하여 알아 볼 수 있다’는 것은 ‘쉽게 다른 정보를 구한다’는 의미이기 보다는 구하기 쉬운지 어려운지와는 상관없이 ‘해당정보와 다른 정보가 특별한 어려움 없이 쉽게 결합하여 특정 개인을 알아볼 수 있게 되는 것’을 말한다고 하여 단말기 고유번호가 개인정보에 해당한다고 판시하였다.

121) 동 규정은 다음과 같다:

“정보통신서비스의 제공에 관한 계약을 이행하기 위하여 필요한 개인정보로서 경제적·기술적인 사유로 통상적인 동의를 받는 것이 뚜렷하게 곤란한 경우에는 이용자의 동의를 얻지 않아도 된다.”

122) 동 규정은 다음과 같다:

“서비스의 이행을 위하여 필요한 경우에는 개인정보를 수집하는 것에 이용자의 동의를 얻을 필요가 없다.”

이러한 법원의 해석은 개인정보의 범위를 설정하는데 있어 매우 중요한 기준을 제시한다. 사안에서 IMEI는 각 휴대폰에 부여된 기기고유번호로서, 그 사용이 가능한 IMEI의 목록은 앱의 공급자가 아닌 이동통신서비스업체가 관리한다. 따라서 앱의 개발자 또는 배포자가 IMEI를 통하여 개인을 식별하기 위해서는 통신사가 소유하고 있는 정보에 대한 접근성을 확보해야만 한다. 이와 관련하여 법원은 ‘쉽게’ 결합할 수 있는 정보가 ‘접근성’을 의미하는 것이 아니라 결합의 ‘용이성’을 뜻한다고 해석하여 개인정보의 범위를 넓게 해석하고 있다. 즉, 법원은 IMEI나 USIM 일련번호와 관련된 개인에 관한 정보가 각 통신사별로 그 접근에 엄격한 통제를 가하고 있다는 사실을 인정하면서도, 통신사가 소유한 정보가 앱 공급자에게 제공되는 경우 공급자가 이를 통하여 개인을 알아보는데 별다른 어려움을 가지지 않는다면 단말기 고유번호를 저장하고 있는 자체만으로도 개인정보를 수집·이용하고 있는 것이라 판단하였다.¹²³⁾

서비스이용계약의 이행을 위하여 필요한 개인정보의 수집이라는 피고인의 주장에 대하여 법원은 IMEI나 USIM 일련번호, 개인 휴대전화번호가 증권통의 서비스를 이행하기 위하여 반드시 필요한 정보라고 보이지 아니할 뿐만 아니라, 피고인들이 취득한 정보가 사용자의 동의를 받는 것이 뚜렷하게 곤란한 경우에 해당한다고 보기도 어렵다고 하여 피고인의 주장을 배척하였다.

마지막으로 이용자의 동의가 있었는지에 대하여 법원은 안드로이드 운영체제에서 제공하는 안내문에 따라 이용자가 확인버튼을 누르거나 취소버튼을 누를 수 있도록 되어 있는 사실은 인정하였다. 그러나 법원은 동 안내문이 안드로이드 운영체제를 사용하여 해당 앱을 사용하게 되는 경우 인터넷에 접속하게 된다는 등의 사정에 대한 공지일 뿐이고 정보통신망법에서 요구하는 개인정보의 수집·이용목적, 수집하는 개인정보의 항목, 개인정보의 보유·이용기간에 관한 사항에 해당할 수 없다고 설명하면서 안내문의 공지에 확인버튼을 누르는 행위가 정보통신망법 제22조 제1항에서 규정하는 개인정보 수집에 관한 동의라 볼 수는 없다고 하였다.

123) 이러한 단말기 고유번호가 개인정보라는 판단을 근거로 법원은 피고인의 세 번째 주장인 정보통신망법 제27조의2에 근거한 주장을 배척하였다.

나. 카카오톡의 개인정보 과다 수집에 대한 인권위 결정 사례

2011년 10월 28일 국가인권위원회는 카카오톡의 강제적이고 고압적인 개인정보 수집 행위가 헌법재판소를 통하여 인정된 개인정보자기결정권을 침해하고 정보통신망법에 대한 위반의 소지가 있다고 판단하여 방송통신위원회에게 모바일 개인정보에 대한 적절한 조치를 취하고 개인정보 처리에 대한 가이드라인을 제정할 것을 권고하였다.¹²⁴⁾

국가인권위원회의 권고는 앞서 이용자 인식도 설문조사 분석 결과와 유사하다. 즉, 형식적이고 강압적인 ‘하거나 말거나’ 식의 동의 절차를 통하여 이용자의 개인정보 통제를 약화시켰고, 필요한 목적의 범위를 초과하는 과도한 개인정보를 수집하였다.¹²⁵⁾ 또한 새롭게 추가된 ‘플러스 친구’ 서비스를 통하여 수집된 개인정보를 모바일 광고를 위한 제3자에게 제공하면서 ‘선 동의 후 거부방식’을 적용하였고 개인정보보호법 제22조 제2항에 규정된 선택적 동의의 획득 과정에서 ‘옵트인(opt-in)’ 방식이 아닌 ‘옵트아웃(opt-out)’ 방식을 적용하여 개인정보자기결정권을 침해할 소지를 야기하였다.¹²⁶⁾ 이러한 국가인권위원회의 권고는 개인정보의 보호 취지에서는 큰 의미를 시사한다.

다. 대리운전앱 사례

2011년 4월 모바일 광고를 목적으로 위치정보를 무단으로 수집하여 2억 건이 넘는 개인정보를 빼돌린 개인정보 유출 사례가 발생하였다. 개인정보의 유출은 많은 사람들이 이용하는 인기 앱인 ‘대리운전’, ‘알송’ 등에 위치추적 프로그램을 탑재하여 배포하는 수법으로 이루어졌다. 해당 프로그램은 GPS 좌표와 휴대전화, 주소 등을 모바일 광고사의 컴퓨터 서버에 전송하였고 이들 정보를 통해 스마트폰 사용자의 위치정보가 실시간 노출된 것으로 드러났다.¹²⁷⁾ 이러한 개인의 위치정보는 맞춤형 모바일 광고에

124) 국가인권위원회 보도자료, “인권위, 기업의 강제적 개인정보 수집 관련 일제 점검 및 가이드라인 제정 권고”, 1쪽. (http://www.humanrights.go.kr/04_sub/bo_dy02.jsp?NT_ID=24&flag=VIEW&SEQ_ID=603153)

125) *Ibid* 1-2쪽.

126) *Ibid* 2-3쪽.

127) 한국일보, 80만명 위치정보 무단수집해 광고 이용한 업체 적발,

이용되어 사용자가 심야에 유흥가에 있으면 대리운전이나 술집, 점심시간 사무실 밀집 지역에 있으면 식당 등의 위치와 연락처를 앱 화면 하단에 표출하였고 이를 통해 모바일 광고업체는 6억5,000만원의 부당이득을 챙겼다.¹²⁸⁾ 이러한 불법광고가 가능했던 이유는 휴대전화 번호만 알면 날짜와 시간대별로 단말기의 좌표가 나타나기 때문이다. 이 좌표를 구글, 네이버, 다음 등에서 무료로 제공하는 API(Application Programming Interface)에 입력하면 오차범위 1m 이내의 위치를 지도상에 표시해준다. 기존 휴대폰 위치정보의 오차범위(500m)와 비교할 수 없을 정도로 정밀해 사용자가 방문한 상점이나 숙박업소 등의 이름까지 추적이 가능하다. 게다가 GPS 기능을 꺼도 스마트폰 전원을 차단하지 않으면 위치가 실시간으로 수집된다.

위치정보법 제16조에 따라 개인위치정보는 누출, 변조, 훼손 등을 방지하기 위하여 관리적 조치를 포함하여 방화벽의 설치나 암호화 소프트웨어의 활용 등의 기술적 조치가 요구된다. 그러나 위 사례에서 이러한 기술적 조치는 이루어지지 않은 채 회사 서버에 방치되어 있었으며 이는 동법 제23조에 근거한 위치정보의 처리 직후 파기의 의무도 위반한 것이다.

라. 판도라앱 사례

미국에서는 온라인 음악 서비스업체 판도라 미디어와 아이폰용 게임 앱 펌킨 메이커(Pumpkin Maker) 등이 이용자의 동의 없이 개인정보를 유출한 것으로 드러나 미국 연방 대배심원으로부터 소환장을 받았다.¹²⁹⁾ 미국 연방 컴퓨터범죄법(Computer Fraud and Abuse Act)에 따라 사용자에게 데이터 수집에 대한 이유를 설명하지 않거나 동의 없이 개인정보를 수집하는 것은 위법이다. 동 사건은 미국 월스트리트 저널이 사용자들에게 인기 있는 101개 앱을 조사한 결과, 이 중 56개에서 스마트폰 정보를 포함한 개인정보

<http://news.hankooki.com/ArticleView/ArticleView.php?url=society/201104/h2011042717552621950.htm&ver=v002>.

128) 류철호, 스마트폰 이용해 80만명 위치정보 무단수집, 중앙일보 2011년 4월 20일자, http://article.joinsmsn.com/news/article/article.asp?total_id=5411470&ctg=1213

129) Scott Thrum et al, *Your Apps Are Watching You*, Dec 10 2011, <http://online.wsj.com/article/SB10001424052748704694004576020083703574602.html>.

가 이용자의 동의 없이 광고회사 등 제3자에게 전송되고 있다는 사실을 보도한 것이 발단이 되었다.¹³⁰⁾ 현재 판도라 미디어를 포함한 스마트폰 앱 개발자들은 개인정보 수집 및 전송 혐의에 대하여 뉴저지주 연방 검사들의 조사를 받고 있다.¹³¹⁾

마. IT기업의 위치정보 수집

1) 위치정보 수집에 대한 논란

2011년 4월 애플의 아이폰을 비롯하여 구글의 안드로이드 운영체제가 탑재된 스마트폰 및 태블릿 PC 등이 사용자의 위치정보¹³²⁾를 수집하는 것이 프라이버시 침해에 해당 하는지에 대하여 사회적 논란이 제기되었다.¹³³⁾ 실제 애플은 한국 국내법원에서 2011년 7월 위치추적 관련 위자료 청구 소송에서 패소해 아이폰 사용자인 원고에게 100만원의 위자료를 지급한 사실이 있다.¹³⁴⁾ 또한 2011년 8월에는 아이폰 위치추적에 대하여 1인당 100만원씩 위자료를 청구하는 대규모 집단소송이 진행되어 2만 7612명이 현재 소송에 참여하고 있다.¹³⁵⁾

모바일 단말기를 통한 위치정보의 수집은 2005년 제정된 위치정보법에 의하여 규율되고 있다. 그러나 2011년 9월 발효된 개인정보보호법에 따르면이라도 위치정보는 제2조 제

130) Amir Efrati et al, *Mobile-App Makers Face U.S. Privacy Investigation*, Wall Street Journal, 5 Apr 2011, <http://online.wsj.com/article/SB10001424052748703806304576242923804770968.html>

131) *Ibid*

132) 위치정보란 휴대성을 지닌 물건 또는 개인이 특정한 시간에 존재하거나 존재하였던 장소에 관한 위치 이동 기록 정보이다.

133) 윤희중, '아이폰 위치정보 수집 불법성 논란', 매일경제 2011년 7월 26일자, <http://news.mk.co.kr/newsRead.php?year=2011&no=483811>

134) 동 사건에서 애플은 아무런 이의를 제기하지 않았고 위자료를 지급하였다. 연합뉴스, "아이폰 위치추적 집단소송 1인당 100만원씩 청구", 2011년 7월 14일자 <http://www.yonhapnews.co.kr/bulletin/2011/07/14/0200000000AKR20110714174000052.HTML>

135) 김명환, '아이폰 위치추적' 2만7천명 집단소송, 매일경제 2011년 8월 17일자, <http://m.mk.co.kr/view.php?tm=&sc=&cm=%BD%BA%B8%B6%C6%AE%C6%F9&year=2011&no=534284&selFlag=&relatedcode=&mc=ES>

1항에 따라 개인정보에 해당한다. 위치정보는 사용자의 휴대전화 번호 또는 신용카드 번호와 같은 고유식별정보에 해당하지는 않지만 다른 정보와 쉽게 결합하여 개인을 식별 가능케 하기 때문이다.¹³⁶⁾

2) 방송통신위원회의 행정처분

2011년 8월 방송통신위원회는 모바일 단말기를 통하여 이용자의 위치정보를 수집하는 행위에 대하여 세계 최초로 행정제재를 부과하였다. 방송통신위원회는 위치정보법 제15조 1항 및 제16조 1항의 위반을 근거로 사용자가 동의를 철회한 경우에도 위치정보를 수집한 애플코리아에 대하여 300만원의 과태료를 부과하는 한편, 모바일 단말기에 암호화되지 않은 채 저장되는 위치정보 수집방법을 시정할 것을 애플코리아와 구글코리아에게 권고하였다.¹³⁷⁾

애플 아이폰의 경우 위치정보 수집에 대한 사용자의 동의는 1) 이동통신사 가입신청서에 게재된 이용약관, 2) 소프트웨어 사용계약서, 3) 위치기반 애플리케이션 초기 구동시 “현재 위치 확인” 등의 절차를 통하여 얻어지고 있다.¹³⁸⁾ 그러나 사용자가 위치서비스의 설정을 해제하여 이러한 동의를 철회하여도 일부 아이폰은 기기 주변의 기지국 및 무선랜(WiFi) AP 위치정보를 애플서버로 전송하였고, 애플서버는 해당 Wi-Fi AP 및 기지국의 위경도 값을 아이폰으로 전송하였다는 사실이 방송통신위원회의 조사결과 드러났다.¹³⁹⁾ 이는 개인 또는 소유자의 동의를 얻지 아니하고 당해 개인 또는 이동성이 있는 물건의 위치정보를 수집·이용 또는 제공하는 행위를 금지하는 위치정보법 제15조 제1항의 위반을 구성한다.

또한 방송통신위원회는 애플과 구글이 위치정보 서비스의 효율성을 높이기 위하여 위치정보 DB의 일부가 이용자의 모바일 단말기에 캐쉬(cache)파일로 저장되도록 설계하였으나 이 과정에서 위치정보 캐쉬파일을 암호화하지 않은 채 저장하고 있다는 사실을 발견하였다.¹⁴⁰⁾ 이는 위치정보법 제16조에 따른 위치정보의 누출, 변조, 훼손 등을 방지하

136) 위치정보법 제2조 1항.

137) 2011년 8월 3일자 방송통신위원회 보도자료, “애플 및 구글의 위치정보보호 법규 위반행위에 대해 시정요구 및 과태료 부과처분 공표”, 1쪽.

138) 위 자료, 3쪽.

139) 위 자료, 3쪽.

기 위한 기술적 조치의 의무를 위반한 것이다.¹⁴¹⁾

방송통신위원회의 이러한 제재는 지금까지 전례가 없던 최초의 행정처분으로서 위치 정보 수집이라는 새로운 모바일 기술에 대한 행정제재의 선례로서 작용한다.¹⁴²⁾ 이로 인해 유사한 혐의로 애플에 대한 조사를 진행 중인 미국, 프랑스 등은 한국 사례를 일종의 선례로 참고할 가능성이 높아졌다. 영국 언론사 가디언에 따르면 애플이 한국의 방송통신위원회로부터 받은 행정처분은 “다른 정부의 판단에 전례로 남을 수 있다는 점에서 애플에게 매우 불리한 처분”이라고 평가하였다.¹⁴³⁾ 미국과 프랑스뿐만 아니라 현재 독일, 이탈리아, 대만 등도 애플의 불법 위치정보 수집 문제에 대해 위치정보 수집에 대한 이유와 목적에 대하여 진상규명을 요청하고 있다.¹⁴⁴⁾ 이 가운데 독일과 이탈리아 정부는 애플의 행위가 자국민의 사생활 보호 관련 법률에 위배되는지 조사하고 있다.¹⁴⁵⁾

2. 사례 분석

가. 애플에 대한 방송통신위원회의 행정제재

140) 위 자료, 4쪽.

141) 현행 개인정보보호법에 따르면 애플과 구글의 행위는 동법의 위반을 구성한다. 개인정보보호법 제15조 제1항은 정보주체의 동의를 받은 개인정보의 수집 및 이용을 규정하고 있고, 제29조는 개인정보의 안전한 관리를 위한 기술적 조치를 규정하고 있기 때문이다.

142) 한국이 가장 먼저 애플에 대하여 제재를 내릴수 있었던 것은 2005년 위치정보법을 세계 최초로 제정하였기 때문이다.

143) Jemima Kiss, South Korea fines Apple over location data blunder, UK Guardian, 2011 Oct 17, <http://www.guardian.co.uk/technology/pda/2011/aug/03/apple-south-korea-location-data>

144) 김상훈, “위치정보 수집 해명하라” 각국, 애플에 요구 확산, 동아일보 2011년 4월 26일 자, http://news.donga.com/Issue/List_08000000000069/3/08000000000069/20110425/36666395/1

145) 위 기사.

2011년 8월 3일 애플에 대한 방송통신위원회의 행정처분은 위치정보를 수집하는 과정에서 어떠한 기술적 조치가 동의로서 인정될 수 있는지에 대한 구체적이고 세부적인 법률의 필요성을 부각시켰다. 방송통신위원회는 “무선 네트워크 사용”에 체크표시를 해제하여 위치정보 수집에 대한 동의를 철회한 이용자의 위치정보를 자사의 서버로 전송하지 않은 구글에 대하여 위법이 없다고 판단하였다.¹⁴⁶⁾ 즉 종전까지 논란이 되어왔던 위치추적 행위가 모바일서비스의 한 콘텐츠로서 합법성을 인정받은 대신 이용자의 동의가 없는 무단 수집에 대하여만 그 절차적 위법성을 판단한 것이다.

중요한 문제는 서비스 이용자의 입장에서 동의가 이루어졌다고 판단할 수 있는 법적 기준을 마련하고 이를 구체화시키는 것에 있다. 이는 보호법익이 아닌 보호정도의 문제이다. 즉, 개인정보처리자의 기술적 조치가 어느 정도까지 이루어져야 그것을 이용자의 동의로서 인정할 수 있는가에 대하여 현행 법률은 아무런 구체적 방안을 제시하지 못하고 있다. 이와 관련하여 방송통신위원회는 위치정보법의 개선방안을 제시하면서 “위치정보시스템의 정의 및 보호조치 적용범위를 구체화하고, 향후 새로운 서비스의 도입 가능성을 고려해 세부적인 보호조치 내용을 고시 등으로 입법”하겠다고 밝혔다.¹⁴⁷⁾

나. 증권통 판례에서 드러난 모바일 개인정보 보호의 향후 과제

증권통 판례는 모바일 개인정보를 규제하는 법률과 정책의 도입에 있어서 다음과 같은 과제를 제시하고 있다. 첫째, 새로운 모바일 기술에 대한 개념의 정의 및 적용범위를 명확히 하여야 한다. 법원이 정보통신망법 제71조 제1호, 제22조 제1항, 그리고 형법 제30조의 위법을 인정하면서도 벌금 700만원에 불과한 처벌을 부과한 이유는 IMEI나 USIM 일련번호의 수집이 개인정보 인지에 대한 개념이 정립되지 아니한 상태에서 이루어졌기 때문이다.¹⁴⁸⁾ 이처럼 기술 발달로 인해 새롭게 도입되는 모바일 정보가 어떠한 법률에 의하여 보호되고 그 보호의 정도가 어디까지인지에 대하여 정보통신서비스제공

146) 2011년 8월 3일자 방송통신위원회 보도자료, 애플 및 구글의 위치정보보호 법규 위반 행위에 대해 시정요구 및 과태료 부과처분 공표, 47쪽.

147) 위 자료, 8쪽.

148) 2010고단5343.

자 또는 개인정보처리자에게 숙지시키기 위하여는 개념의 정리와 보호법익의 설정이 시급하다. 실제로 통신비밀보호법에 따르면 "단말기 고유번호"라 함은 이동통신사업자와 이용계약이 체결된 개인의 이동전화 단말기에 부여된 전자적 고유번호를 말한다.¹⁴⁹⁾ 그러나 과거 ESN 일련번호와 달리 IMEI는 단말기 번호와 가입자 정보가 분리되어 있으므로, 해당 판결이 나오기 전까지 IMEI의 수집을 개인정보의 수집이라고 단정짓기는 힘든 실정이었다.¹⁵⁰⁾ 다시 말해, 앱서비스 제공자는 서비스 공급에 따른 개인정보의 수집 및 이용에 있어서 어떠한 행위가 위법을 구성하는지에 대하여 확신을 가지지 못한다. 이러한 문제는 비단 국내의 문제만은 아니다. EU의 제29조작업반의 연구에서도 드러나듯이 단말기 고유번호, IP 주소와 같은 새로운 개념의 정보가 EU개인정보보호지침 제2조에서 규정하고 있는 개인정보의 범위에 해당하는지에 대하여 개인정보보호지침은 확실한 답변을 내리지 못하고 있기 때문이다.¹⁵¹⁾ '대리운전' 앱 사건에서 모바일 프로그램 내 악성코드의 탑재 및 배포를 통하여 이루어진 개인정보의 유출은 명백한 위법행위이다. 이와 달리, 증권통 사건은 개인정보의 범위와 그 보호대상의 모호함이 문제가 되었다는 점에서 법적 안정성 확보를 위한 법률 및 정책 보완에 대한 필요성을 부각시켰다.

둘째, 정보통신서비스 제공자 및 개인정보처리자가 모바일 고유의 정보를 어떻게 다루어야 하는지에 대한 구체적이고 통일적인 지침이 제시되어야 한다. 이는 모바일 개인정보에 대한 통일적인 취급방침이 부재하는 상황에서 모바일 보안의 기준이 일률적이지 못하다는 사실에 기인한다. 현재 모바일 보안프로그램을 개발하는 기업들은 각각 다른 보안기술과 보안기준을 적용하고 있다. 동일한 앱에 대하여 A사의 스마트폰 백신은 아무런 문제를 발견하지 못한 반면 B사의 프로그램이 악성 앱이라고 정의한다면 이용자들은 큰 혼란을 겪게 될 것이다.

셋째, 증권통 사례는 모바일 개인정보의 보호가 서비스에 대한 쉽고 간편한 접근성이라는 반대급부를 가지고 있음을 보여주었다. 증권통 앱의 단말기 고유번호 자동추출 프

149) 통신비밀보호법 제2조 제12항.

150) 주민영, 단말기 고유번호 수집하는 안드로이드 앱, 문제 없나, 2010. 08. 29 <http://www.bloter.net/archives/37504>.

151) Opinion 4/2007 on the concept of personal data, 01248/07/EN WP 136, p. 3.

로그인은 해당 서비스의 편리한 이용을 위하여 로그인 절차를 간소화시키기 위한 기술적 조치였다. 법원 역시 양형의 이유에서 ‘피고인들이 개인정보를 수집한 이유가 개인정보를 비정상적인 상황에서 사용하려는데 이유가 있는 것이 아니라 단지 증권통 이용자들의 이용의 편의를 위한 발상에서 시작되어 경위에 참작할 바가 있다’하여 이러한 문제를 직시하였다.¹⁵²⁾ 이는 대리운전 앱에 탑재되어 있던 악성코드가 개인정보를 이용한 광고 즉, 사용자를 기망하여 얻게 되는 부당이득을 목적으로 배포되었다는 사실과 큰 차이를 보인다.

모바일서비스의 가장 큰 장점 가운데 하나는 휴대장비를 이용한 편리하고 신속한 서비스의 접근에 있다. 이처럼 접근성을 높이기 위하여 보다 간편한 서비스 시스템을 구축하는 행위는 개인정보라는 보호법익과 배치될 수 있다. 따라서 새로운 기술의 도입으로부터 개인정보를 최대한 보호하는 동시에 그러한 기술이 가져다주는 여러 가지 편익을 제고할 때 모바일서비스 이용자의 권익은 비로소 실현될 것이다. 이러한 균형의 접점을 찾는 것은 본 연구의 중요한 목적 가운데 하나이다.

다. 적용 법률의 파편화

앞선 사례들에서 애플의 위치추적 위반에는 위치정보법이, 증권통 사건에서는 정보통신망법이 적용되었음을 알 수 있다. 이처럼 스마트폰의 경우 전화라는 점에서 통신관련 법제가 적용될 수 있고, GPS좌표를 이용한 위치정보의 수집이 가능하다는 점에서 위치정보법, 무선랜을 이용한 네트워크가 가능하다는 점에서 정보통신망법의 적용을 받을 수 있다.¹⁵³⁾ 또한 2011년 9월 발효된 개인정보보호법 역시 제6조의 내용에 따라 다른 법률에 대한 일반법으로 그 적용순위가 밀려나면서 모바일 개인정보를 규제하는 법제는 통일적이지 않다는 문제점을 발생시키고 있다.

개인정보보호 담당기관 역시 문제이다. 개인정보보호법의 취지를 살펴볼 때, 카카오톡의 강압적인 동의 획득의 문제는 국가인권위원회가 아닌 개인정보보호위원회의 소관으

152) 2010고단5343.

153) 박인회, 스마트폰과 관련된 법적문제에 관한 소고, 월간 법제, 법제처, 2011년 6월호, 40쪽.

로 보인다. 개인정보보호법 제7조에 근거하여 설립된 개인정보보호위원회는 동법 제8조에 의하여 개인정보 보호와 관련된 정책, 제도 및 법령 개선에 관한 사항을 담당하도록 되어있기 때문이다.¹⁵⁴⁾ 개인정보보호법이 발효된 지 얼마 되지 않았다는 점을 고려한다면 하더라도 문제점은 여전히 존재한다. 정보통신망법 제4조에 따라 방송통신위원회는 이용자의 개인정보보호에 대한 시책을 마련하여야 한다. 그러나 개인정보보호법 제62조에 따라 개인정보 침해에 대한 신고의 접수·처리·상담을 행하는 전문기관은 한국인터넷진흥원이며,¹⁵⁵⁾ 동법 제63조에 근거하여 법률을 위반하는 사항을 발견하거나 혐의가 있음을 파악하는 자문기관은 한국정보화진흥원 또는 한국인터넷진흥원이다.¹⁵⁶⁾ 또한 개인정보보호법 제62조의 신고센터에 접수된 신고의 접수·처리 및 상담과 관련된 사항에 대한 제63조상 자료제출 요구 및 검사에 관한 권한은 동법 시행령 제60조 제3항에 의하여 한국인터넷진흥원에 위탁되고 있다. 이처럼 담당기관이 혼재되어 있는 상황에서 모바일 개인정보보호가 나타내는 모호한 적용범위와 대상은 이용자 또는 정보주체의 혼란을 가중시킬 수밖에 없다. 국가인권위원회, 방송통신위원회, 개인정보보호위원회, 한국인터넷진흥원 등 복수의 행정기관이 각각 개인정보자기결정권, 정보통신망법, 개인정보보호법을 근거로 모바일 개인정보에 관여할 수 있다는 사실은 복잡하고 비효율적인 관할의 단점을 나타내고 있다.

국내 적용법의 파편화와 담당기관의 혼재는 EU의 개인정보보호법제와 비교된다. 한국의 개인정보보호법은 미국의 민간자율형 규제가 아닌 유럽의 통합형 규제 모델을 따르고 있다. 그러나 모바일 개인정보에 대하여 적용되는 법률의 양태를 살펴보면 오히려 사안에 따라 개별법을 적용하는 미국의 그것과 흡사한 모습을 지니고 있다. 여러 행정기관의 혼재 역시 ICO가 개인정보보호의 문제를 총괄적으로 다룰 수 있도록 복수의 법률이 단일한 행정기관에게 그 권한을 위임하는 영국의 입법과 대비된다.¹⁵⁷⁾

154) 개인정보보호법 제8조 1항 2호.

155) 개인정보보호법 시행령 제59조.

156) 개인정보보호법 시행령 제60조 제2항.

157) UK Data Protection Act, Art. 6.

제4절 소 결

설문조사를 통한 이용자 인식도 조사와 사례를 통해 드러난 모바일 환경에서 개인정보 보호의 문제는 다음과 같이 요약될 수 있다.

1) 개인정보의 범위 및 적용대상의 모호성

증권통 사례에서 논란이 된 바와 같이 개별 사례에서는 모바일기기로부터 수집되는 다양한 정보들이 각각 보호대상이 되는 개인정보에 해당하는지 여부가 불분명하여 정보주체는 물론 서비스제공자 역시 혼란을 겪고 있다. 정보주체는 스스로 전혀 인식하지 못하는 사이 자신의 개인정보가 타인에 의해 수집되는 것을 방치하게 되고, 서비스제공자는 자신이 개인정보를 수집한다는 사실을 인지하지 못하여 불법행위를 하게 되는 경우가 발생하였다.

2) 형식적이고 강압적인 동의 획득 절차

개인정보를 수집, 이용하는 모바일 앱의 이용에서 동의 획득 절차가 제대로 준수되지 않거나, 준수된다 하더라도 형식적 절차에 그치거나 정보주체가 실질적 선택권을 가지지 못하는 경우가 많다. 설문조사 결과 과반수 이상의 이용자들이 자신의 개인정보에 대한 통제권을 완전히 행사하지 못한다고 인식하고 있었으며, 실제 사례에서도 동의 획득 절차의 문제가 가장 다양하고 빈번한 것으로 나타났다.

또한 동의획득의 시점 역시 문제가 되었다. 많은 모바일 애플리케이션은 마켓에서 다운로드 및 설치시 개인정보의 수집목적, 범위, 보유기간 등을 사전에 적시하지 않는 것으로 확인되었다. 즉 관련 법률상 규정되어 있는 수집시 동의 획득 의무가 제대로 준수되지 않고 있는 것으로 보인다.

3) 개인정보 취급방침의 취약성과 낮은 접근성

모바일 환경에서 개인정보 취급방침은 이용자로 하여금 개인정보 수집의 목적, 수집되는 개인정보의 항목 등 정보통신서비스 사업자의 개인정보 처리를 구체적으로 확인할 수 있는 유일한 통로이다. 그러나 개인정보 취급방침을 통일적으로 규율하는 법률 또는 정책이 부재하는 현실에서, 사업자에 의하여 공개되는 개인정보 취급방침의 형식, 내용

은 모두 상이하다.

이처럼 상이한 형태로 제공되는 개인정보 취급방침은 대부분 길고 어려운 문장으로 구성되어 있어 이용자로 하여금 취급방침의 내용을 인지하는데 어려움을 가지게 한다. 또한 동의 절차와 상관없는 개인정보 취급방침 공개의 의무는 개인정보의 처리와 상관 없이 공개의 여부만이 법적 의무로서 규정되어 있으므로 이용자의 낮은 접근성을 야기한다.

4) 개인정보의 과도한 수집

개인정보 처리에 대한 동의 획득 절차의 문제와 개인정보 취급방침의 취약성은 개인정보의 과도한 수집을 통하여 직접적인 문제를 일으킨다. 개인정보 처리목적에 대한 일반적인 기준이 없고, 여러 사례에서 드러나듯이 목적에 비하여 과도한 개인정보가 수집되고 있는 것이다. 모바일서비스 환경에서 이러한 문제는 더욱 심각해진다. 작은 휴대형 기기를 이용하여 동의를 획득하고 이에 대한 처리방침의 내용을 별도로 공개하는 현재의 이용실태는 과도한 정보수집에 대한 이용자의 인식을 저해할뿐더러, 사업자로 하여금 과도한 수집 및 이용을 적법하게 만드는 면죄부를 제공하고 있다.

선택적 동의제도가 정착되지 않은 점은 과도한 개인정보의 수집과 직결된다. 현행 법률에서 규정하고 있는 처리목적의 범위를 초과한 개인정보의 수집을 방지하기 위한 선택적 동의제도는 현재 국내 모바일 환경에서 그 목적과 기능을 발휘하지 못하고 있다.

5) 개인정보의 제3자 제공시의 문제

모바일서비스에서 개인정보의 제3자 제공은 더욱 빈번히 일어나게 된다. 각종 메신저와 같이 이용자의 주소록 정보를 수집하여 제공하는 서비스의 경우 이용자가 제공하는 정보는 제3자의 정보가 되며, 일정관리를 위한 캘린더 앱 등을 이용할 때 타인의 개인정보를 입력하거나 혹은 이러한 일정이 공개되는 경우에 개인정보 수집시와 동일한 문제가 발생할 수 있다. 특히 위치기반서비스는 위치정보사업자로부터 위치정보를 제공받아야 가능한 서비스로서 모바일서비스에서 개인정보의 제3자 제공은 더욱 빈번히 일어나므로 예전에 비해 더욱 강화된 보호가 요구된다 할 것이다.

6) 담당기관의 혼재와 적용법의 파편화

2011년 9월 발효된 개인정보보호법은 공공기관을 포함한 민간 개인정보처리자에 대한 통합적이고 일반적인 개인정보보호를 다루고 있다. 이러한 입법의 취지와 기본적 구조는 미국의 자율형 규율체제가 아닌 유럽의 통합형 규율체제를 따르고 있다. 그러나 국내 개인정보보호 체계는 일반법적 지위를 가지는 개인정보보호법과 기존에 제정된 특별법으로서의 정보통신망법, 위치정보법 등이 혼재하고 있다. 또한 각각의 법률이 규정하고 있는 권한감독기관이 모두 다르다는 점은 이용자로 하여금 혼란을 가중시킨다.

이처럼 적용법이 파편화되어 있고, 행정기관 사이의 권한의 배분 문제 또한 명확하지 않다는 점은 영국의 개인정보보호 체계와 극명히 대비되는 문제이다. 영국은 개인정보보호법과 이를 보완하는 E-프라이시법을 순차적으로 제정하고 이에 대한 권한감독기관을 단일화하여 개인정보보호와 피해대처에 대하여 그 책임소재와 적용법률을 명확하게 규정하고 있다.

제4장 현행 법제의 평가 및 개선방안

제3장에서 설문조사를 통해 조사된 이용자 인식과 피해사례를 통해 분석한 모바일서비스 제공시 개인정보보호와 관련한 주요 문제는 개인정보와 개인정보처리자의 범위가 모호하여 혼란을 야기한다는 점, 개인정보 처리에 대한 동의 획득시 절차상의 문제점, 모바일기기에서 개인정보 취급방침에 대한 접근이 용이하지 않고 가독성이 떨어지는 등의 문제, 개별 앱들이 수집하는 개인정보의 범위가 과도하다는 점, 개인정보의 제3자 제공에 대한 통제가 취약하다는 점, 그리고 개인정보보호에 대한 담당기관과 적용 법률이 파편화되어 있다는 점으로 드러났다. 이러한 문제점들은 모바일서비스에서만 나타나는 문제라기보다는 모바일기기라는 매체의 특성에 따라 문제가 더욱 가속화되거나 심화되는 것으로 볼 수 있다. 이러한 대규모 집행결손에 대해서는 법률이 적용되기 위한 실효적 정책의 도입이 요구된다. 또한 경우에 따라 현행법이 모바일 환경의 특성을 반영하지 못하여 관련 문제들을 완벽하게 포섭하지 못하거나, 모바일서비스에서 이루어지는 개인정보의 처리 행태를 반영하지 못하는 경우도 발생하는 것으로 보인다. 이러한 문제의 경우 추가적인 입법이나 법률 개정, 또는 하부정책의 보완이 이루어져야 할 것이다.

본 장에서는 이러한 문제점들에 대해 현행 개인정보보호 법제가 실효성 있는 해결책을 제시하는지를 살피고, 미국, EU, 영국 등 외국의 관련 법제 및 입법동향과의 비교 분석을 통하여 문제를 해결하기 위한 개선안을 모색한다.

제1절 모바일서비스에 적용되는 현행 법체계 개관

2011년 9월 30일 개인정보보호법의 시행 이전 우리나라의 개인정보보호법체계는 공공 부문과 민간부문에 대한 별도의 법률로 구분되어 규율되어 왔다. 공공부문에 대해서는 「공공기관의 개인정보보호에 관한 법률」로서 규제되어 왔으나, 개인정보보호법의 시

행에 따라 동법은 폐지되었고¹⁵⁸⁾ 개인정보보호법이 일반법으로서 적용되고 있으며, 다만 개인정보보호법 시행 이전에 동법을 위반한 행위에 대한 벌칙규정만이 경과적으로 적용되고 있다.¹⁵⁹⁾ 민간부문의 경우 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 ‘정보통신망법’), 「신용정보의 이용 및 보호에 관한 법률」(이하 ‘신용정보법’), 「교육법」, 「보건의료기본법」, 「위치정보의 보호 및 이용 등에 관한 법률」(이하 ‘위치정보법’) 등 개별 법률에 의해 분야별로 규율되고 있다. 신설 개인정보

<표 4-1> 분야별 개인정보에 관한 국내법

	정보통신	금융	의료	교육
소관 법령	정보통신망 이용촉진 및 정보보호등에 관한 법률	신용정보의 이용 및 보호에 관한 법률	보건의료기본법, 의료법	교육기본법, 초·중등 교육법
적용 범위	정보통신서비스 제공자가 이용자 개인 정보 수집 시	신용정보업자들이 개인 신용정보 수집·응용·제공 시	의료인 및 의료기관 종사자가 처리하는 환자기록 및 비밀	교육기관이 학생 및 학부모 개인 정보 취급 시
적용 대상	정보통신서비스 제공자 및 준용사업자	신용정보집중기관 신용정보업자 기타 신용정보 취급 사업자 등	의료인 및 의료기관 종사자	모든 교육기관 및 종사자
수집	민감정보 수집제한 및 필요 최소정보 수집 수집 목적 등 고지 및 사전동의 획득 후 수집	수집시 목적명시 합리적·공리적 수집 신용정보 무관 정보 수집 금지	관련 조항 없음	교육적 목적 제한 및 제3자 제공금지
이용/제공	목적 외 이용 및 동의 없는 제3자 제공 금지	개인신용정보 제공 및 활용 시 동의 획득 의무 상거래 관계 성립·유지 여부 판단 외 제공 금지	의료기록 누설 및 제3자 제공 금지	학교생활기록 및 건강검사 자료 등을 동의없이 제3자 제공 금지(초·중등)

(출처: 개인정보보호 종합지원 포털)

158) 개인정보보호법 부칙 제2조.

159) 개인정보보호법 부칙 제5조 제1항.

호법은 개별 법률에 산재되어 규율되고 있던 것을 통일적으로 규율하기 위하여 제정되어 개인정보 보호에 관한 기본법의 지위를 가지며, 정보통신망법, 위치정보법, 신용정보법 등의 개별법은 개인정보보호법에 대한 특별법으로서의 지위를 가진다. 따라서 개인정보보호법은 공공부문과 민간부문을 포괄하여 모든 개인정보의 처리에 적용되며 동법과 다른 내용의 규정이 있는 경우 정보통신망법 등의 특별법 규정이 적용된다.

1. 개인정보보호법의 주요 규정

개인정보보호법은 “업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등”¹⁶⁰⁾의 개인정보처리자에게 적용된다.

개인정보보호법은 본문 75개 조로 구성되는 9개 장과 부칙 7개 조로 구성된다. 제1장은 총칙으로서 제1조부터 제6조까지로 구성된다. 제2장은 ‘개인정보 보호정책의 수립 등’으로서 제7조부터 제14조까지로 구성된다. 제3장은 ‘개인정보의 처리’로서 제1절과 제2절로 구성된다. 제3장의 제1절은 개인정보의 수집, 이용, 제공 등으로서 제15조부터 제22조까지, 제3장의 제2절은 개인정보의 처리 제한으로서 제23조부터 제28조까지로 구성된다. 특히 제3장의 제1절은 개인정보의 수집, 이용, 제공, 파기에 이르는 각 단계별로 개인정보처리자가 준수하여야 할 처리기준을 구체적으로 규정한다. 제4장은 ‘개인정보의 안전한 관리’로서 제29조부터 제34조까지로 구성된다. 제5장은 ‘정보주체의 권리 보장’으로서 제35조부터 제39조까지로 구성된다. 제6장은 개인정보분쟁조정위원회로서 제40조부터 제50조까지로 구성된다. 제7장은 ‘개인정보 단체소송’으로서 제51조부터 제57조까지로 구성된다. 제8장은 보칙으로서 제58조부터 제69조까지로 구성된다. 제9장은 벌칙으로서 제70조부터 제75조까지로 구성된다. 개인정보보호법상 개인정보처리자의 주요 의무는 다음과 같다.

우선 개인정보의 수집, 이용시 개인정보보호법은 정보주체의 사전 동의가 있는 경우, 법률의 규정에 의해 요구되는 경우, 공공기관이 소관업무를 수행하기 위해 불가피한 경

160) 개인정보보호법 제2조 5호.

우, 정보주체와의 계약 체결 및 이행을 위해 불가피한 경우, 정보주체의 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산상의 이익을 위해 필요하다고 인정되는 경우, 개인정보처리자의 정당한 이익을 달성하기 위해 필요한 경우로서 명백히 정보주체의 권리보다 우선하는 경우에 한해 개인정보의 수집을 허용하고 있다.¹⁶¹⁾ 정보주체의 동의를 받는 경우에는 수집·이용의 목적, 수집하고자 하는 개인정보의 항목, 보유 및 이용기간, 동의를 거부할 권리가 있다는 사실 및 거부에 따른 불이익의 내용을 정보주체에게 알려야 한다. 이와 같은 조건을 충족하여 개인정보를 수집하더라도 목적에 필요한 최소한의 범위에 한정되어야 하며, 처리하는 정보가 최소한의 정보인지 여부에 대한 입증책임은 개인정보처리자가 부담한다.¹⁶²⁾ 또한 개인정보처리자는 필요한 최소한의 정보 외의 개인정보의 수집에 동의가 이루어지지 않았다는 이유로 서비스의 제공을 거부할 수 없다.¹⁶³⁾ 또한 처리하려는 정보가 민감정보나 고유 식별정보인 경우 개인정보처리자는 다른 개인정보의 처리에 대한 동의와 별도의 동의를 받아야 한다.¹⁶⁴⁾

수집한 개인정보를 제3자에게 제공하는 경우 개인정보처리자는 정보주체에게 개인정보를 제공받는 자, 제공받는 자의 이용 목적, 이용 또는 제공하는 개인정보의 항목, 제공받은 자의 보유 및 이용 기간, 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익의 내용을 정보주체에게 알리고 별도의 동의를 받아야 한다.¹⁶⁵⁾ 개인정보의 이용 또는 제공은 동의의 범위 내에서만 이루어져야 하며, 예외적으로 정보주체로부터 별도의 동의를 받은 경우, 다른 법률에 특별한 규정이 있는 경우, 정보주체의 사전 동의를 받을 수 없는 경우로 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산상의 이익을 위하여 필요하다고 인정되는 경우, 통계작성 및 학술연구의 목적으로 개인을 식별할 수 없는 형태로 제공하는 경우 등에 한하여 정보주체 및 제3자의 이익을 부당하게 침해하지 않는 범위 내에서 목적 외 이용 또는 제공을 할 수 있다. 제3자로부터 개인정보를 제공받은 개인정보처리자는 정보주체의 요구가 있는 경우 개인정보의 수집 출처와 처리

161) 개인정보보호법 제15조.

162) 개인정보보호법 제16조 제1항.

163) 개인정보보호법 제16조 제2항.

164) 개인정보보호법 제23, 24조.

165) 개인정보보호법 제17조.

목적 등을 정보주체에게 고지하여야 한다.¹⁶⁶⁾ 위의 동의를 받는 방법에 대해서는 따로 이 규정하고 있다.

개인정보처리자는 자신이 수집, 보유하는 개인정보에 대하여 기술적·관리적·물리적 안전조치를 취할 의무를 지니며,¹⁶⁷⁾ 보유기간의 경과, 개인정보의 처리 목적 달성 등 그 개인정보가 불필요하게 되었을 때에는 지체 없이 그 개인정보를 파기하여야 하며, 이때 개인정보가 복구 또는 재생되지 아니하도록 조치하여야 한다.¹⁶⁸⁾ 또한 개인정보처리자는 개인정보 처리 목적, 처리 및 보유 기간, 제3자 제공에 관한 사항, 업무위탁에 관한 사항, 정보주체의 권리·의무 및 그 행사방법에 관한 사항 등을 포함하는 개인정보 처리방침을 작성하여야 하며, 이를 공개하여야 한다.¹⁶⁹⁾

개인정보보호법에 개인정보 유출 통지 제도가 새로이 도입되었다. 동법 제34조에 따라 개인정보처리자는 개인정보가 유출되었음을 알게 되었을 때에는 지체 없이 해당 정보주체에게 유출된 개인정보의 항목, 유출된 시점과 그 경위, 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 정보, 개인정보처리자의 대응조치 및 피해 구제 절차, 피해 발생시 신고 등을 접수할 수 있는 담당부서 및 연락처를 알리고 피해를 최소화하기 위한 대책을 마련하고 조치를 취하여야 한다.¹⁷⁰⁾

2. 정보통신망법의 주요 규정

정보통신망법의 목적은 정보통신서비스를 이용하는 자의 개인정보를 보호하는 데에 있다.¹⁷¹⁾ 개인정보보호법이 개인정보의 오남용으로부터 사생활의 비밀 등을 보호함을 목적으로 하는 것과 보호법익의 차이가 있다. 그럼에도 정보통신망법의 주된 보호법익은 정보주체의 사생활 보호라고 볼 수 있다.

정보통신망법의 의무주체가 되는 개인정보처리자는 정보통신서비스 제공자가 된다.

166) 개인정보보호법 제20조.

167) 개인정보보호법 제29조.

168) 개인정보보호법 제21조.

169) 개인정보보호법 제30조.

170) 개인정보보호법 제34조.

171) 정보통신망법 제1조.

정보통신서비스 제공자는 「전기통신사업법」 제2조 제8호에 따른 전기통신사업자와, 영리를 목적으로 전기통신역무를 이용하여 정보를 제공하거나 정보제공을 매개하는 자를 의미한다.¹⁷²⁾ 전기통신사업자에는 이동통신사, 인터넷서비스제공자 등의 기간통신사업자, 이러한 기간통신사업자의 통신설비를 이용하여 기간통신역무를 제공하는 별정통신사업자, 인터넷 포털 사이트나 온라인 쇼핑몰과 같이 기간통신사업자의 통신설비를 임차하여 기간통신역무 이외의 전기통신역무를 제공하는 부가통신사업자가 있다. 전기통신역무를 이용하여 영리를 목적으로 정보를 제공하거나 매개하는 자의 범위는 보다 폭넓게 인정된다. 이 때 어떠한 서비스가 유상으로 제공되는지 여부와 관계없이 학술·종교·단체 등 비영리단체가 제공하는 경우를 제외하고 모두 영리성을 인정할 수 있다. 또한 정보를 제공하는 행위에는 정보를 게시·전송·대여·공유하는 등의 일련의 정보 제공행위가 모두 포함되므로 광고를 게재하거나 각종 정보를 제공하는 것이 모두 해당될 수 있으며, 정보제공을 매개하는 것에는 이메일 등과 같이 정보를 제공하려는 자와 제공받으려는 자를 연결시켜 서비스 제공이 가능하도록 하는 모든 행위가 포함된다.¹⁷³⁾ 따라서 모바일서비스의 경우 기본적인 이동통신서비스는 물론, 애플리케이션 마켓과 같은 중개 서비스, 통신기능이 포함된 애플리케이션을 이용한 모든 서비스는 정보통신망법상 정보통신서비스에 해당한다.

정보통신망법에서는 제22조 내지 제31조에서 폭넓은 개인정보보호 규정을 두고 있다. 제22조에서 개인정보 수집시 개인정보의 수집/이용의 목적과 수집하는 개인정보의 항목, 개인정보의 보유 및 이용기간을 고지하고 이용자의 동의를 획득하도록 규정하고 있으며, 제23조에서는 수집제한 정보와 최소수집원칙을 규정하고 있다. 제24조는 수집목적과 다른 이용을 금지하고 있고, 제24조의2는 개인정보 제3자 제공시 동의획득 의무를 규정한다. 제25조는 개인정보취급위탁시의 절차와 책임을 규정하고 있다. 제26조의2에서는 동의획득방법에 대하여 구체적으로 규정하고 있으며, 제27조의2에서는 개인정보 취급방침을 이용자에게 공개할 것을 명시하고 있다. 제28조는 수집된 개인정보를 보호하기 위한 기술적·관리적 조치를 취해야 할 것을 규정하며, 제29조에서는 개인정보의 파기 조건

172) 정보통신망법 제2조 제3호.

173) 방송통신위원회, 정보통신서비스 제공자를 위한 개인정보보호 가이드, (방통위, 2011.1.), p.22.

을 명시한다.

정보통신분야의 경우 정보통신망을 통해 개인정보를 대량으로 처리함으로써 개인정보 침해 가능성이 더욱 높기 때문에 개인정보보호법보다 더욱 강화된 의무가 규정된다. 예컨대, 개인정보 처리 위탁의 경우 정보주체와의 관계에서 개인정보보호법은 위탁업무의 내용과 수탁자를 언제든지 정보주체가 쉽게 확인할 수 있도록 할 것만을 규정하고 있지만¹⁷⁴⁾ 정보통신망법은 한 발 나아가 개인정보 취급 수탁자, 위탁업무의 내용을 이용자에게 알리고 동의를 받을 것을 요구하고 있다.

3. 위치정보법의 주요 규정

위치정보법은 “위치정보의 유출·오용 및 남용으로부터 사생활의 비밀 등을 보호하고 위치정보의 안전한 이용환경을 조성하여 위치정보의 이용을 활성화함으로써 국민생활의 향상과 공공복리의 증진에 이바지함”을 목적으로 한다.¹⁷⁵⁾ 동 법의 수범대상은 크게 위치정보사업자와 위치기반서비스사업자로 나뉜다. 위치정보사업자는 위치정보를 수집하여 위치기반서비스사업자에게 제공하는 사업자를 의미하며, 위치기반서비스사업자는 위치정보를 이용한 서비스(위치기반서비스)를 제공하는 사업자를 의미한다.¹⁷⁶⁾ 위치정보사업은 방송통신위원회의 허가대상이 되며, 위치기반서비스사업은 방송통신위원회에 신고 대상이 된다. 허가 또는 신고시 위치정보사업자나 위치기반서비스사업자는 자신이 제공하고자 하는 위치정보의 수집, 이용 및 제공에 관한 요금 및 조건 등을 이용약관으로 정하여 방송통신위원회에 신고해야 하며, 방송통신위원회는 동 약관이 개인 위치정보의 보호, 공정경쟁 또는 공공이익을 침해할 우려가 있다고 판단되는 경우에는 위치정보사업자 등에게 이용약관의 변경을 명할 수 있다.¹⁷⁷⁾

위치정보사업자는 제15조에 따라 위치정보의 수집, 이용, 제공시 개인 또는 이동성 있는 물건의 소유자에게 동의를 얻을 의무와 위치정보의 보호를 위한 기술적·관리적 조치

174) 개인정보보호법 제26조.

175) 위치정보법 제1조.

176) 위치정보보호법 제2조 6호, 7호.

177) 위치정보법 제12조.

를 취할 의무가 있다. 나아가 개인위치정보를 수집하는 경우는 위치정보사업자의 상호, 주소, 전화번호 그 밖의 연락처, 개인위치정보주체의 권리와 그 행사방법, 위치기반서비스사업자에게 제공하고자 하는 서비스의 내용, 위치정보 수집사실 확인자료의 보유근거 및 보유기간 등을 약관에 명시하여 동 약관에 대한 동의를 받아야 한다.¹⁷⁸⁾ 위치기반서비스사업자는 개인위치정보를 이용하여 서비스를 제공하고자 하는 경우 위치기반서비스사업자의 상호, 주소, 전화번호 그 밖의 연락처, 개인위치정보주체의 권리와 그 행사방법, 제공하고자 하는 위치기반서비스의 내용, 위치정보 이용·제공사실 확인자료의 보유근거 및 보유기간 등을 이용약관에 명시하여 개인위치정보주체에게 동의를 얻어야 하며, 개인위치정보를 개인위치정보주체가 지정하는 제3자에게 제공하는 서비스를 하고자 하는 경우에는 동일한 내용을 이용약관에 명시한 후 제공받는 자 및 제공목적은 개인위치정보주체에게 고지하고 동의를 얻어야 한다.¹⁷⁹⁾ 위치기반서비스사업자는 개인위치정보의 동의를 받았다는 사실과 개인위치정보의 범위, 기간을 갖추어 위치정보사업자에게 개인위치정보의 제공을 요청할 수 있다.¹⁸⁰⁾ 개인정보보호법이 개인정보를 제3자에게 제공받는 경우 정보주체의 요구가 있을 때에 한해 수집 출처, 처리 목적을 정보주체에게 고지할 의무를 부과하는 데 비해 위치정보를 제공받는 위치기반서비스사업자는 보다 강력한 의무를 부담한다.

178) 위치정보법 제18조.

179) 위치정보법 제19조.

180) 위치정보법 시행령 제25조.

제2절 개인정보의 범위와 적용대상의 불명확성

1. 개인정보의 범위

가. 관련법상 보호범위의 차이

개인정보보호법을 비롯해 정보통신망법 등 특별법은 개인정보에 대해 각기 다른 정의를 내리고 있다. 따라서 특정 정보가 개인정보에 해당하는지 여부는 개별 법률로 상이하게 나타날 수 있다. 개인정보보호법과 정보통신망법 등 개별법은 위반에 대하여 벌금과 자유형 등 형벌을 부과할 수 있다는 점에서 죄형법정주의 원칙에 따라 구성요건이 명확해야 할 필요가 있다. 그러나 예컨대 “증권통” 사건의 예에서 보이듯 특정 정보가 각 법률상의 보호범위에 포함되는지 여부는 사안에 따라 개별적으로 파악될 수밖에 없다. 동 사건에서 문제가 된 것은 IMEI 번호였는데, 피고인은 이것이 개인정보가 아니라 정보통신망법 제27조의2에서 규정하는 “인터넷 접속정보파일”에 불과하다는 주장을 하였으나, 재판부는 이들이 “특정 개인의 소유로 귀속되기 전까지는 기기나 특정 카드에 부여된 고유번호로서 그 자체로는 당해 개인을 알아볼 수 있는 정보라 보기는 어렵다”고 하더라도 이들은 휴대폰을 특정 개인이 소유하게 되는 순간부터 휴대폰 가입자 정보와 쉽게 결합하여 개인을 식별할 수 있게 되는 개인정보가 된다며 이러한 주장을 배척하였다.¹⁸¹⁾ 그러나 개인과 직접 연관되어 판매되는 USIM 카드의 번호와는 달리 기기 자체의 고유번호인 IMEI 번호의 경우, USIM 카드의 교체만으로 손쉽게 다른 사람에 의한 이용이 가능하다는 점에서 개인과 직접적으로 연결된다고 단정짓기는 어렵다. 신기술의 도입은 서비스제공자들로 하여금 더욱 다양한 종류와 범위의 정보를 수집하는 것을 가능하게 하고 있어 새로이 등장하는 수집 가능한 정보들이 각각 개인정보에 해당하는지 여부는 점점 불분명해진다.

개인정보보호법과 정보통신망법에서 개인정보는 각각 “살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는

181) 서울중앙지법 판결 2010고단5343.

<표 4-2> 법규별 개인정보의 정의

	개인정보보호법	정보통신망법	위치정보법
용어	개인정보	개인정보	개인위치정보
정의	<ul style="list-style-type: none"> • 살아 있는 개인에 관한 정보 • 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보 (해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다)	<ul style="list-style-type: none"> • 생존하는 개인에 관한 정보 • 성명·주민등록번호 등에 의하여 특정 개인을 알아볼 수 있는 정보 • 부호·문자·음성·영상 및 영상 등의 정보 (해당 정보만으로는 특정 개인을 알아볼 수 없어도 다른 정보와 쉽게 결합하여 알아볼 수 있는 경우에는 그 정보를 포함한다)	<ul style="list-style-type: none"> • 이동성이 있는 물건 또는 개인이 특정한 시간에 존재하거나 존재하였던 장소에 관한 정보로서 • 전기통신설비 및 전기통신회선설비를 이용하여 수집된 것 중 • 특정 개인의 위치정보 (위치정보만으로는 특정 개인의 위치를 알 수 없는 경우에도 다른 정보와 용이하게 결합하여 특정 개인의 위치를 알 수 있는 것을 포함한다)

것을 포함한다)” 및 “생존하는 개인에 관한 정보로서 성명·주민등록번호 등에 의하여 특정 개인을 알아볼 수 있는 부호·문자·음성·영상 및 영상 등의 정보(해당 정보만으로는 특정 개인을 알아볼 수 없어도 다른 정보와 쉽게 결합하여 알아볼 수 있는 경우에는 그 정보를 포함한다)”로 정의된다. 이밖에 신용정보법에서는 신용정보를 “특정 신용정보주체를 식별할 수 있는 정보”로, 위치정보법은 “특정 개인의 위치정보(위치정보만으로는 특정 개인의 위치를 알 수 없는 경우에도 다른 정보와 용이하게 결합하여 특정 개인의 위치를 알 수 있는 것을 포함한다)”를 개인위치정보로 정의하고 있다. 이들 규정에서 공통적으로 발견되는 요소는 개인에 관한 정보라는 점, 특정 개인을 식별할 수 있는 정보라는 점이다. 나아가 개인정보보호법과 정보통신망법에서는 살아 있는 개인에 관한 정보일 것을 추가적으로 규정하고 있다.

구체적으로 각 법상의 보호대상이 되는 개인정보를 개인정보보호법상의 개인정보와

비교하면 다음과 같은 차이가 있다.

1) 개인정보보호법과 정보통신망법

개인정보보호법과 정보통신망법에서 개인정보의 정의는 동일하다고 볼 수 있다. 정보통신망법은 “부호·문자·음성·음향 및 영상 등의 정보”라는 표현을 사용하지만 이는 예시적인 것으로 개인정보보호법과 범위의 차이는 없다.

위 법들에서 개인정보는 첫째, “정보”이며, 둘째, “살아있는 개인”에 관한 정보이고, 셋째, 살아있는 개인에 “관한” 정보이며, 넷째, 개인을 “알아볼 수 있는” 정보이다. 또한 해당 정보만으로는 특정 개인을 알아볼 수 없더라도 ‘다른 정보와 쉽게 결합하여 알아볼 수 있는 것’을 포함한다.

우선 개인정보는 “정보”이다. 개인정보보호법은 ‘정보’의 종류나 형태를 한정하지 않으므로 문자, 음성, 음향, 영상, 부호 등 다양한 형식의 정보가 그 적용 대상이 된다. 또한, 정보가 저장되는 매체의 종류나 형태도 한정되지 않아서, 회원가입신청서나 행정서식지 등의 종이문서상의 정보, 컴퓨터에 저장된 정보, CCTV에 찍힌 영상정보 등도 정보가 된다. 국가정보화기본법은 정보를 ‘특정 목적을 위하여 광(光) 또는 전자적 방식으로 처리되어 부호, 문자, 음성, 음향 및 영상 등으로 표현된 모든 종류의 자료 또는 지식’이라고 정의한다.¹⁸²⁾

둘째, “살아있는 개인”에 관한 정보로, 정보주체가 사망한 경우 그에 관한 정보는 개인정보가 되지 않는다. 즉 개인정보보호법의 보호법익은 정보주체의 인격권으로서의 프라이버시이므로, 사자(死者)에 대해서는 적용되지 않는다. 또한 실종선고 등 관계 법령에 의해 사망한 것으로 간주되는 자에 관한 정보 역시 개인정보가 되지 않는다.¹⁸³⁾ EU개인정보보호지침의 경우 개인정보를 “식별되거나 식별가능한 자연인에 관련된 정보”라고 정의하며, 이 때 자연인은 생존하고 있는 자만을 의미하지 않으므로 사자(死者)를 식별할 수 있는 정보 역시 포함하여 우리 법보다 넓은 범위를 규정하고 있다. 그

182) 국가정보화기본법 제3조 제1호. 동 법은 국가정보화의 기본 방향과 관련 정책의 수립·추진에 필요한 사항을 규정한다.

183) 방송통신위원회, 『정보통신서비스 제공자를 위한 개인정보보호 가이드』 (방통위, 2011.1.), p.14.

외 캐나다와 뉴질랜드의 입법례에서는 명시적으로 죽은 자에 대한 정보 역시 개인정보에 해당한다고 규정하는 경우도 있다.¹⁸⁴⁾

사망한 자는 인격권을 가지지 않으므로 개인정보자기결정권의 주체 역시 되지 못한다고 보는 것이 논리적이다. 주지하듯 개인정보보호법의 목적은 정보 자체를 보호하는 것이 아니라 개인의 기본권으로서 프라이버시를 보호하는 데 있기 때문이다. 또한 개인정보 수집/이용에 대한 동의 획득 등의 절차는 사망한 자에 대해서는 현실적으로 적용이 불가능하다. 그러나 개인정보로서 수집한 항목이 정보주체의 사망으로 인해 개인정보의 지위를 상실하고, 따라서 개인정보보호에 대한 법의 적용이 되지 않는 것은 현실적으로 문제가 될 수 있다. 예컨대 생전에 자신의 모바일기기에 앱을 설치하여 모바일서비스를 이용하던 자가 사망할 경우, 그에 대한 정보는 그의 사망 시점으로부터 개인정보로서 보호되지 못하여 개인정보처리자가 이용, 보유, 제3자 제공 등을 함에 있어 아무런 제약을 받지 않게 될 수 있다. 개인의 사망으로 자동적으로 해당 서비스에서 탈퇴하거나 개인정보 수집/이용에 관한 동의가 철회되는 것은 아니기 때문이다. 다만, 사망한 자에 관한 정보라도 해당 정보가 생존하는 유족의 프라이버시를 침해할 수 있는 경우, 해당 정보는 그 유족의 개인정보로서 보호될 여지는 있다.¹⁸⁵⁾ 그러나 사자(死者)에 관한 정보라도 여전히 개인정보처리자의 입장에서는 재산적 가치를 지닌다고 볼 수 있을 뿐 아니라 우리 법제에서 사자의 인격권이 전혀 보호받지 못하는 것은 아니다. 예컨대 형법 제308조는 사자에 대한 명예훼손죄를 인정하고 있다. 따라서 “개인정보의 수집·유출·이용·남용으로부터 사생활의 비밀 등을 보호함으로써 국민의 권리와 이익을 증진하고, 나아가 개인의 존엄과 가치를 구현”하기 위한 개인정보보호법의 목적상 제한적으로 사

184) 뉴질랜드의 ‘Privacy Act 1993’ 제2조 제1항은 ‘personal information’을 ‘information about an identifiable individual’라고 정의하면서 ‘information relating to a death that is maintained by the Registrar-General pursuant to the Births, Deaths, Marriages, and Relationships Registration Act 1995, or any former Act’을 포함한다고 규정한다. 캐나다의 ‘Personal Information Protection and Electronic Documents Act’ 제2조 제1항은 ‘personal information’을 ‘information about an identifiable individual’이라고 정의하면서, ‘the name, title or business address or telephone number of an employee of an organization’을 포함하지 않는다고 규정한다.

185) 방송통신위원회, 정보통신서비스 제공자를 위한 개인정보보호 가이드, p.14.

자(死者)에 대한 정보 역시 개인정보보호법의 보호범위에 포섭시키는 것이 입법론적으로 필요할 것이다. 이 때 적용가능한 규정은 이미 수집된 개인정보의 이용, 보유, 파기에 관한 규정들이 될 것이다.

셋째, 개인정보는 개인에 “관한” 정보이다. 개인정보보호법과 정보통신망법 등 현행 법은 구체적, 세부적 기준이나 요건을 규정하고 있지 않으므로 특정 개인과 관련이 있는 정보는 모두 개인에 관한 정보로 볼 수 있다.¹⁸⁶⁾ 관련성 여부는 사실문제로 사안에 따라 결정된다.¹⁸⁷⁾ EU개인정보보호지침이나 영국 개인정보보호법 역시 개인정보를 개인에 ‘관한’(relating to) 정보로 정의를 내리는데, 이에 대해 EU개인정보지침에 따라 설치된 제29조작업반 (Article 29 Working Party)은 양육권에 관한 재판에서 본인인 어린이가 제출한 자신의 가족에 관한 그림이 개인정보에 해당한다는 의견을 제시하였다.¹⁸⁸⁾ 그 그림이 어린이의 심경과 가족 구성원들에 대한 느낌에 관한 정보를 제공하기 때문에 개인정보가 된다는 것이다. 영국 항소법원은 *Durant v. Financial Services Authority* 사건에서 항소인의 이의제기 등으로 생성된 문서에 대하여 해당 문서가 Durant에 관련된 문서가 아니라고 판단한 바 있다. 즉, 항소인은 관련성을 광의로 해석하여 개인의 성명을 참조하여 데이터베이스를 검색한 결과 나올 수 있는 ‘어떤 데이터’ (any data)도 포함한다고 주장한 반면, 반대 측은 영어사전에 수록된 ‘관련성’ (relate to)의 두 가지 의미 중에서 ‘개인과 대체로 직접 연결됨을 의미하는’ (implying ... a more or less direct connection with an individual) 의미에서 보다 제한적인 개념을 주장하였다. 항소법원은 이를 제한적으로 해석하여 정보주체의 열람권은 자신의 프라이버시를 침해하지 않도록 하는 것이므로 정보주체의 이름을 참조하여 컴퓨터 내용을 검색하여 문서가 검색된 사실 만으로 이들 문서가 정보주체에 관련되는 개인정보가 되는 것은 아니라고 판단하였다.¹⁸⁹⁾ 영국 정보보호위원회는 동 사건 결정에 대하여 이전에 대부분의 전문가들이 생각한 것보다 더 좁게 개인정보를 해석한 것으로 이해된다고 밝혔다.¹⁹⁰⁾

186) Ibid. p.15.

187) ICO Legal Guidance, supra note , p. 11.

188) ARTICLE 29 DATA PROTECTION WORKING PARTY, *Opinion 4/2007 on the concept of personal data* 8 (01248/07/EN, WP136).

189) Lloyd, supra note , p. 45.

190) Information Commissioner’s Office, Data Protection Technical Guidance:

넷째, 개인정보보호법상 개인정보는 ‘알아볼 수 있는’ 정보를 의미하고, ‘해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것’을 포함한다.¹⁹¹⁾ 개인정보 보호에 있어서 개인의 식별은 그 개인을 다른 개인들로부터 구별하는 것을 의미한다. 개인을 식별하게 하는 수단은 성명, 주민등록번호, 영상 등 다양하며, 개인정보보호법은 개인을 식별하는 수단에 제한을 두지 않기 때문에 개인정보는 전자적으로 처리되는 개인정보는 물론 수기문서도 포함한다.¹⁹²⁾ 또한 공공기관은 물론 비영리단체 등이 처리하는 개인정보도 포함된다.¹⁹³⁾ 따라서 개인정보보호법에 따라 보호되는 개인정보의 범위는 광범위하다. 또한 개인정보보호법은 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 개인정보에 포함하도록 규정하고 있어, 서로 다른 데이터베이스상에서 각각 식별이 불가능한 정보라도 두 데이터베이스가 결합한 정보로부터 식별될 수 있으면 해당 정보는 개인정보가 된다.¹⁹⁴⁾ 또한 ‘다른 정보’를 개인정보처리자가 보유하는 정보로 제한하지 않는다. 다만 ‘쉽게 결합하여’ 알아볼 수 있어야 하므로, 그 결합을 통한 식별에 소요되는 시간과 비용이 합리적으로 용인될 수 있어야 할 것이다. 따라서, ‘쉽게 결합하여’의 판단은 개인정보를 처리하는 개인정보처리자와 처리되는 개인정보의 성격 등에 따라 다를 수 있다. 이는 영국 개인정보보호법이 ‘다른 정보’를 개인정보처리자(data controller)¹⁹⁵⁾가 보유하거나 보유하게 될 것 같은(likely to come into the possession) 정보로 제한하는 것과 비교된다.

위를 바탕으로 살펴보면 개인정보보호법상 개인정보의 정의는 다소 구체적이지 못한데, 이는 동 법이 개인정보의 보호에 있어 일반적으로 적용되는 단일법의 특성을 가지기 때문이다. 그러나 개인정보보호법이 위반에 대한 제재 수단으로 형벌을 규정하고 있

Determining what is personal data p. 1 (2007. 8. 21.)

191) 개인정보보호법 제2조 제1호..

192) 국회 행정안전위원장, 개인정보보호법안 (대안), 2면.

193) 국회 행정안전위원장, 개인정보보호법안 (대안), 2면.

194) Peter Carey, *supra* note , p. 18.

195) 국내 개인정보보호법의 개인정보처리자는 영국 개인정보보호법 Section1(1)의 정보관리자(data controller)와 대비되는 개념이다. 동조는 또한 정보처리자(data processor)의 개념을 정의하고 있는데, 이는 정보관리자를 대신하여 개인정보를 처리하는 자로서 정보관리자에게 개인정보의 처리를 위탁받은 제3자가 이에 해당한다. 용어에 따른 혼란을 방지하기 위하여 영국법의 정보관리자를 개인정보처리자로 통일하여 서술한다.

다는 점에서 형벌이 적용되는 규정들은 형사특별법적 성격을 가진다. 이는 개인정보보호법보다 강력한 처벌규정을 두고 있는 정보통신망법의 경우에도 마찬가지이다.(개인정보보호법제상 형벌을 부과하는 규정은 <표4-3>, 과태료를 부과하는 규정은 <표 4-4> 참조) 따라서 구성요건에 대한 불명확성은 죄형법정주의상 명확성의 원칙에 위반되는지에 대한 논란이 제기될 수 있다. 즉, 범죄의 구성요건이 불명확하면 국민의 자유와 권리를 보장할 수 없으므로 죄형법정주의에 위배되는데,¹⁹⁶⁾ 우리 법원은 죄형법정주의를 설명하면서 범죄 구성요건에 대한 판단기준을 “통상의 판단능력을 가진 사람의 의미 이해 가능성”,¹⁹⁷⁾ “사물의 변별능력을 제대로 갖춘 일반인의 이해와 판단”¹⁹⁸⁾으로 보고 있다. 따라서 어떠한 유형의 정보가 개인정보에 해당하는지가 업계 전문가의 입장에서 모호하다면 전문적 지식을 갖추지 않은 일반인의 입장에서는 더욱 판단이 어려울 수 있다.

그러나 개념의 다양성 자체가 즉시 명확성원칙의 위반을 구성하는 것은 아니다. 입법자가 모든 개별 사건의 내용을 예견하여 이를 법률로서 규정하는 것은 불가능하기 때문에 사법심사에 일정한 재량을 인정하지 않으면 안되며, 다만 법관의 자의적 판단에 의하여 범죄 여부가 결정될 수 있는 정도에 이르지 않도록 해야 하는 것이다. 따라서 법률에서는 해석의 여지가 있는 다의적 개념들이 사용되며, 이러한 개념들에는 해당 여부를 분명하게 결정할 수 없는 중립적 대상이 하나라도 존재함으로써 다의성을 갖게 되는 ‘모호개념’, 현재는 모호성이 없지만 장래에 그렇게 될 수 있는 가능성이 있는 ‘잠재적 모호개념’, 높은 단계의 모호성을 가진 개념으로서 가치충족을 필요로 하는 ‘가치개념’, 직접 관찰에 의하여 확인하는 것이 불가능하여 그 존재를 추정할 수 있는 관찰 가능한 간접적 판단자료를 수집하여 우회적으로 추론할 수밖에 없는 ‘성향개념’ 등이 있다.¹⁹⁹⁾ 개인정보의 정의상 “다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다”는 대목에서 “쉽게”, “알아볼 수 있는”과 개념은 형법학상 잠재적 모호개념에 해당한다. 증권통 사건에서 피고인이 수집한 IMEI 번호가 통신사의 가입자 개인

196) 헌재 1995. 9. 28. 93헌바50.

197) 헌재 1992. 9. 25. 89헌가104.

198) 대법원 2002. 7. 26. 2002도1855.

199) 배중대, 형법총론(제8전정판), 홍문사, 2007, p.88-89.

정보 데이터베이스에 포함되어 있다 할지라도 피고인의 입장에서는 그러한 사실을 알기 어려웠다는 점, 합법적 방법으로 통신사 데이터베이스에 접근할 수 있는 방법이 없다는 점 등에서 해당 정보가 쉽게 결합될 수 있는 정보로서 개인정보에 해당하는지 여부는 예측하기도 어려웠다고 볼 수 있다. 그러나 개인정보보호법에 일반형법의 판단 기준이 그대로 적용된다고 단정짓기는 어렵다. 즉, 개인정보보호법은 전문법이며, 따라서 그 의무주체가 되는 업무를 목적으로 개인정보를 처리하는 개인정보처리자에게는 일반인에 비하여 높은 수준의 주의의무가 요구된다. 상장기업의 경우 상법 개정에 따라 도입된 준법지원인²⁰⁰⁾이 역할을 할 것으로 기대된다.

기술의 발전으로 수집 가능한 정보가 확대되면서 각각의 정보가 개인정보에 해당하는지 여부가 모호한 것은 필연적이다. 오히려 기술 발전 속도가 매우 빨라 수집될 수 있는 정보의 유형은 구체적으로 예측이 불가능하며, 정보주체의 보호에 대한 기대와 입법 목적을 충족하기 위한 유연성이 요구된다 할 것이다. 다만 표현상의 모호성으로 인해 발생할 수 있는 혼란을 예방하기 위해 어떠한 유형의 정보가 개인정보에 해당하는지에 대한 산업계와 담당기관 차원의 가이드라인이 계속적으로 보충되어야 할 것이다. 또한 명확성 원칙에 대한 논란을 피하기 위해서는 이러한 지침이 반드시 법률의 형식을 취할 필요는 없더라도 구체적이고 개별적으로 한정된 사항에 관해 법률로부터 위임을 받아 제정된 명령의 지위를 갖추는 것이 입법론적으로 요구된다.²⁰¹⁾

200) 개정 상법 제542조의 13.

201) 헌재 1995. 9. 28. 93헌바50.

<표 4-3> 관련법상 개인정보보호 관련 형벌 규정

개 인 정 보 보 호 법	<p>제71조(벌칙) 다음 각 호의 어느 하나에 해당하는 자는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다.</p> <ol style="list-style-type: none"> 1. 제17조제1항제2호에 해당하지 아니함에도 같은 항 제1호를 위반하여 정보주체의 동의를 받지 아니하고 개인정보를 제3자에게 제공한 자 및 그 사정을 알고 개인정보를 제공받은 자 2. 제18조제1항·제2항, 제19조, 제26조제5항 또는 제27조제3항을 위반하여 개인정보를 이용하거나 제3자에게 제공한 자 및 그 사정을 알면서도 영리 또는 부정한 목적으로 개인정보를 제공받은 자 3. 제23조를 위반하여 민감정보를 처리한 자 4. 제24조제1항을 위반하여 고유식별정보를 처리한 자 5. 제59조제2호를 위반하여 업무상 알게 된 개인정보를 누설하거나 권한 없이 다른 사람이 이용하도록 제공한 자 및 그 사정을 알면서도 영리 또는 부정한 목적으로 개인정보를 제공받은 자 6. 제59조제3호를 위반하여 다른 사람의 개인정보를 훼손, 멸실, 변경, 위조 또는 유출한 자 <p>제72조(벌칙) 다음 각 호의 어느 하나에 해당하는 자는 3년 이하의 징역 또는 3천만원 이하의 벌금에 처한다.</p> <ol style="list-style-type: none"> 1. 제25조제5항을 위반하여 영상정보처리기기의 설치 목적과 다른 목적으로 영상정보처리기기를 임의로 조작하거나 다른 곳을 비추는 자 또는 녹음기능을 사용한 자 2. 제59조제1호를 위반하여 거짓이나 그 밖의 부정한 수단이나 방법으로 개인정보를 취득하거나 개인정보 처리에 관한 동의를 받는 행위를 한 자 및 그 사정을 알면서도 영리 또는 부정한 목적으로 개인정보를 제공받은 자 3. 제60조를 위반하여 직무상 알게 된 비밀을 누설하거나 직무상 목적 외에 이용한 자 <p>제73조(벌칙) 다음 각 호의 어느 하나에 해당하는 자는 2년 이하의 징역 또는 1천만원 이하의 벌금에 처한다.</p> <ol style="list-style-type: none"> 1. 제24조제3항, 제25조제6항 또는 제29조를 위반하여 안전성 확보에 필요한 조치를 하지 아니하여 개인정보를 분실·도난·유출·변조 또는 훼손당한 자 2. 제36조제2항을 위반하여 정정·삭제 등 필요한 조치를 하지 아니하고 개인정보를 계속 이용하거나 이를 제3자에게 제공한 자
---------------------------------	---

	<p>3. 제37조제2항을 위반하여 개인정보의 처리를 정지하지 아니하고 계속 이용하거나 제3자에게 제공한 자</p> <p>제74조(양벌규정) ① 법인의 대표자나 법인 또는 개인의 대리인, 사용인, 그 밖의 종업원이 그 법인 또는 개인의 업무에 관하여 제70조에 해당하는 위반행위를 하면 그 행위자를 벌하는 외에 그 법인 또는 개인을 7천만원 이하의 벌금에 처한다. 다만, 법인 또는 개인이 그 위반행위를 방지하기 위하여 해당 업무에 관하여 상당한 주의와 감독을 게을리하지 아니한 경우에는 그러하지 아니하다.</p> <p>② 법인의 대표자나 법인 또는 개인의 대리인, 사용인, 그 밖의 종업원이 그 법인 또는 개인의 업무에 관하여 제71조부터 제73조까지의 어느 하나에 해당하는 위반행위를 하면 그 행위자를 벌하는 외에 그 법인 또는 개인에게도 해당 조문의 벌금형을 과(科)한다. 다만, 법인 또는 개인이 그 위반행위를 방지하기 위하여 해당 업무에 관하여 상당한 주의와 감독을 게을리하지 아니한 경우에는 그러하지 아니하다.</p>
정 보 통 신 망 법	<p>제71조(벌칙) 다음 각 호의 어느 하나에 해당하는 자는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다.</p> <ol style="list-style-type: none"> 1. 제22조제1항(제67조에 따라 준용되는 경우를 포함한다)을 위반하여 이용자의 동의를 받지 아니하고 개인정보를 수집한 자 2. 제23조제1항(제67조에 따라 준용되는 경우를 포함한다)을 위반하여 이용자의 동의를 받지 아니하고 개인의 권리·이익이나 사생활을 뚜렷하게 침해할 우려가 있는 개인정보를 수집한 자 3. 제24조, 제24조의2제1항 및 제2항 또는 제26조제3항(제67조에 따라 준용되는 경우를 포함한다)을 위반하여 개인정보를 이용하거나 제3자에게 제공한 자 및 그 사정을 알면서도 영리 또는 부정한 목적으로 개인정보를 제공받은 자 4. 제25조제1항(제67조에 따라 준용되는 경우를 포함한다)을 위반하여 이용자의 동의를 받지 아니하고 개인정보 취급위탁을 한 자 5. 제28조의2제1항(제67조에 따라 준용되는 경우를 포함한다)을 위반하여 이용자의 개인정보를 훼손·침해 또는 누설한 자 6. 제28조의2제2항을 위반하여 그 개인정보가 누설된 사정을 알면서도 영리 또는 부정한 목적으로 개인정보를 제공받은 자 7. 제30조제5항(제30조제7항, 제31조제3항 및 제67조에 따라 준용되는 경우를 포함한다)을 위반하여 필요한 조치를 하지 아니하고 개인정보를 제공하거나 이용한 자 8. 제31조제1항(제67조에 따라 준용되는 경우를 포함한다)을 위반하여 법정대리인의 동의를 받지 아니하고 만 14세 미만인 아동의 개인정보

	<p>보를 수집한 자</p> <p>제72조(벌칙) ① 다음 각 호의 어느 하나에 해당하는 자는 3년 이하의 징역 또는 3천만원 이하의 벌금에 처한다.</p> <p>2. 제49조의2제1항을 위반하여 다른 사람의 개인정보를 수집한 자</p> <p>제73조(벌칙) 다음 각 호의 어느 하나에 해당하는 자는 2년 이하의 징역 또는 1천만원 이하의 벌금에 처한다.</p> <p>1. 제28조제1항제2호부터 제5호까지(제67조에 따라 준용되는 경우를 포함한다)의 규정에 따른 기술적·관리적 조치를 하지 아니하여 이용자의 개인정보를 분실·도난·누출·변조 또는 훼손한 자</p>
<p>위 치 정 보 법</p>	<p>제39조(벌칙) 다음 각호의 1에 해당하는 자는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다.</p> <p>1. 제5조제1항의 규정을 위반하여 허가를 받지 아니하고 위치정보사업을 하는 자 또는 속임수 그 밖의 부정한 방법으로 허가를 받은 자</p> <p>2. 제17조의 규정을 위반하여 개인위치정보를 누설·변조·훼손 또는 공개한 자</p> <p>3. 제18조제1항·제2항 또는 제19조제1항·제2항·제4항의 규정을 위반하여 개인위치정보주체의 동의를 얻지 아니하거나 동意的 범위를 넘어 개인위치정보를 수집·이용 또는 제공한 자 및 그 정을 알고 영리 또는 부정한 목적으로 개인위치정보를 제공받은 자</p> <p>4. 제21조의 규정을 위반하여 이용약관에 명시하거나 고지한 범위를 넘어 개인위치정보를 이용하거나 제3자에게 제공한 자</p> <p>5. 제29조제6항의 규정을 위반하여 개인위치정보를 긴급구조 외의 목적에 사용한 자</p> <p>제40조(벌칙) 다음 각호의 1에 해당하는 자는 3년 이하의 징역 또는 3천만원 이하의 벌금에 처한다. <개정 2007.12.21></p> <p>1. 제5조제7항의 규정을 위반하여 변경허가를 받지 아니하거나 변경신고를 하지 아니하고 위치정보사업을 하는 자 또는 속임수 그 밖의 부정한 방법으로 변경허가를 받거나 변경신고를 한 자</p> <p>2. 제9조제1항의 규정을 위반하여 신고를 하지 아니하고 위치기반서비스사업을 하는 자 또는 속임수 그 밖의 부정한 방법으로 신고한 자</p> <p>3. 제13조제1항의 규정에 의한 사업폐지명령을 위반한 자</p> <p>4. 제15조제1항의 규정을 위반하여 개인의 동의를 얻지 아니하고 당해 개인의 위치정보를 수집·이용 또는 제공한 자</p>

	<p>5. 제15조제2항의 규정을 위반하여 타인의 정보통신기기를 복제하거나 정보를 도용하는 등의 방법으로 위치정보사업자들을 속여 타인의 개인위치정보를 제공받은 자</p> <p>제41조(벌칙) 다음 각호의 1에 해당하는 자는 1년 이하의 징역 또는 2천만원 이하의 벌금에 처한다.</p> <ol style="list-style-type: none"> 1. 제8조제1항·제2항, 제11조제1항·제2항, 제23조 또는 제24조제4항의 규정을 위반하여 개인위치정보를 파기하지 아니한 자 2. 제9조제3항의 규정을 위반하여 변경신고를 하지 아니하고 위치기반서비스사업을 하는 자 또는 속임수 그 밖의 부정한 방법으로 변경신고를 한 자 3. 제13조제1항의 규정에 의한 사업의 정지명령을 위반한 자 4. 제16조제1항의 규정을 위반하여 기술적·관리적 조치를 하지 아니하거나 제16조제2항의 규정을 위반하여 위치정보 수집·이용·제공사실 확인자료가 위치정보시스템에 자동으로 기록·보존되도록 하지 아니한 자 5. 제29조제3항의 규정을 위반하여 긴급구조기관의 요청을 거부하거나 제29조제5항의 규정을 위반하여 경보발송을 거부한 자
--	---

<표 4-4> 관련법상 개인정보보호 관련 행정벌(과태료) 규정

개인정보보호법	<p>제75조(과태료) ① 다음 각 호의 어느 하나에 해당하는 자에게는 5천만원 이하의 과태료를 부과한다.</p> <ol style="list-style-type: none"> 1. 제15조제1항을 위반하여 개인정보를 수집한 자 2. 제22조제5항을 위반하여 법정대리인의 동의를 받지 아니한 자 3. 제25조제2항을 위반하여 영상정보처리기기를 설치·운영한 자 <p>② 다음 각 호의 어느 하나에 해당하는 자에게는 3천만원 이하의 과태료를 부과한다.</p> <ol style="list-style-type: none"> 1. 제15조제2항, 제17조제2항, 제18조제3항 또는 제26조제3항을 위반하여 정보주체에게 알려야 할 사항을 알리지 아니한 자 2. 제16조제2항 또는 제22조제4항을 위반하여 재화 또는 서비스의 제공을 거부한 자 3. 제20조제1항을 위반하여 정보주체에게 같은 항 각 호의 사실을 알리지 아니한 자 4. 제21조제1항을 위반하여 개인정보를 파기하지 아니한 자
---------	--

	<p>5. 제24조제2항을 위반하여 정보주체가 주민등록번호를 사용하지 아니할 수 있는 방법을 제공하지 아니한 자</p> <p>6. 제24조제3항, 제25조제6항 또는 제29조를 위반하여 안전성 확보에 필요한 조치를 하지 아니한 자</p> <p>7. 제25조제1항을 위반하여 영상정보처리기기를 설치·운영한 자</p> <p>8. 제34조제1항을 위반하여 정보주체에게 같은 항 각 호의 사실을 알리지 아니한 자</p> <p>9. 제34조제3항을 위반하여 조치 결과를 신고하지 아니한 자</p> <p>10. 제35조제3항을 위반하여 열람을 제한하거나 거절한 자</p> <p>11. 제36조제2항을 위반하여 정정·삭제 등 필요한 조치를 하지 아니한 자</p> <p>12. 제37조제4항을 위반하여 처리가 정지된 개인정보에 대하여 파기 등 필요한 조치를 하지 아니한 자</p> <p>13. 제64조제1항에 따른 시정명령에 따르지 아니한 자</p> <p>③ 다음 각 호의 어느 하나에 해당하는 자에게는 1천만원 이하의 과태료를 부과한다.</p> <p>1. 제21조제3항을 위반하여 개인정보를 분리하여 저장·관리하지 아니한 자</p> <p>2. 제22조제1항부터 제3항까지의 규정을 위반하여 동의를 받은 자</p> <p>3. 제25조제4항을 위반하여 안내판 설치 등 필요한 조치를 하지 아니한 자</p> <p>4. 제26조제1항을 위반하여 업무 위탁 시 같은 항 각 호의 내용이 포함된 문서에 의하지 아니한 자</p> <p>5. 제26조제2항을 위반하여 위탁하는 업무의 내용과 수탁자를 공개하지 아니한 자</p> <p>6. 제27조제1항 또는 제2항을 위반하여 정보주체에게 개인정보의 이전 사실을 알리지 아니한 자</p> <p>7. 제30조제1항 또는 제2항을 위반하여 개인정보 처리방침을 정하지 아니하거나 이를 공개하지 아니한 자</p> <p>8. 제31조제1항을 위반하여 개인정보 보호책임자를 지정하지 아니한 자</p> <p>9. 제35조제3항·제4항, 제36조제2항·제4항 또는 제37조제3항을 위반하여 정보주체에게 알려야 할 사항을 알리지 아니한 자</p> <p>10. 제63조제1항에 따른 관계 물품·서류 등 자료를 제출하지 아니하거나 거짓으로 제출한 자</p> <p>11. 제63조제2항에 따른 출입·검사를 거부·방해 또는 기피한 자</p>
--	--

	<p>④ 제1항부터 제3항까지의 규정에 따른 과태료는 대통령령으로 정하는 바에 따라 행정안전부장관과 관계 중앙행정기관의 장이 부과·징수한다. 이 경우 관계 중앙행정기관의 장은 소관 분야의 개인정보처리자에게 과태료를 부과·징수한다.</p>
<p>정 보 통 신 망 법</p>	<p>제76조(과태료) ① 다음 각 호의 어느 하나에 해당하는 자와 제7호부터 제11호까지의 경우에 해당하는 행위를 하도록 한 자에게는 3천만원 이하의 과태료를 부과한다. <개정 2011.3.29></p> <ol style="list-style-type: none"> 1. 제23조제2항(제67조에 따라 준용되는 경우를 포함한다)을 위반하여 서비스의 제공을 거부한 자 2. 제23조의2를 위반하여 필요한 조치를 하지 아니한 자 3. 제28조제1항제1호 및 제6호(제67조에 따라 준용되는 경우를 포함한다)에 따른 기술적·관리적 조치를 하지 아니한 자 4. 제29조 본문(제67조에 따라 준용되는 경우를 포함한다)을 위반하여 개인정보를 파기하지 아니한 자 5. 제30조제3항·제4항 및 제6항(제30조제7항, 제31조제3항 및 제67조에 따라 준용되는 경우를 포함한다)을 위반하여 필요한 조치를 하지 아니한 자 6. 제44조의5제2항에 따른 방송통신위원회의 명령을 이행하지 아니한 자 7. 제50조제1항부터 제3항까지의 규정을 위반하여 영리 목적의 광고성 정보를 전송한 자 8. 제50조제4항 또는 제5항을 위반하여 광고성 정보를 전송할 때 밝히야 하는 사항을 밝히지 아니하거나 거짓으로 밝힌 자 9. 제50조제7항을 위반하여 비용을 수신자에게 부담하도록 한 자 10. 제50조의5를 위반하여 이용자의 동의를 받지 아니하고 프로그램을 설치한 자 11. 제50조의7제1항을 위반하여 인터넷 홈페이지에 영리목적의 광고성 정보를 게시한 자 12. 제71조부터 제74조까지, 제1호부터 제11호까지 및 제2항의 위반행위를 하여 제64조제4항에 따른 방송통신위원회의 시정조치 명령을 이행하지 아니한 자 <p>② 다음 각 호의 어느 하나에 해당하는 자에게는 2천만원 이하의 과태료를 부과한다.</p> <ol style="list-style-type: none"> 1. 제25조제2항(제67조에 따라 준용되는 경우를 포함한다)을 위반하여 이용자에게 개인정보 취급위탁에 관한 사항을 공개하지 아니하거나 알리지 아니한 자

	<p>2. 제26조제1항 및 제2항(제67조에 따라 준용되는 경우를 포함한다)을 위반하여 이용자에게 개인정보의 이전사실을 알리지 아니한 자</p> <p>3. 제27조제1항(제67조에 따라 준용되는 경우를 포함한다)을 위반하여 개인정보 관리책임자를 지정하지 아니한 자</p> <p>4. 제27조의2제1항(제67조에 따라 준용되는 경우를 포함한다)을 위반하여 개인정보 취급방침을 공개하지 아니한 자</p> <p>③ 다음 각 호의 어느 하나에 해당하는 자에게는 1천만원 이하의 과태료를 부과한다. <개정 2009.4.22, 2011.4.5></p> <p>1. 제20조제2항을 위반하여 전자문서를 보관하지 아니한 자</p> <p>2. 제21조를 위반하여 전자문서를 공개한 자</p> <p>2의2. 제23조의3제1항을 위반하여 본인확인기관의 지정을 받지 아니하고 본인확인업무를 한 자</p> <p>2의3. 제23조의3제2항에 따른 본인확인업무를 휴지 또는 같은 조 제3항에 따른 본인확인업무를 폐지 사실을 이용자에게 통보하지 아니하거나 방송통신위원회에 신고하지 아니한 자</p> <p>2의4. 제23조의4제1항에 따른 본인확인업무를 정지 및 지정취소 처분에도 불구하고 본인확인업무를 계속한 자</p> <p>2의5. 제24조의2제3항(제67조에 따라 준용되는 경우를 포함한다)을 위반하여 제공 또는 취급위탁에 대한 동의를 받을 때 개인정보의 수집·이용에 대한 동의와 구분하여 받지 아니하거나 이에 동의하지 아니한 이유로 서비스 제공을 거부한 자</p>
<p>위 치 정 보 법</p>	<p>제43조(과태료) ① 다음 각호의 1에 해당하는 자는 2천만원 이하의 과태료에 처한다.</p> <p>1. 제5조제4항의 규정에 의한 허가조건을 위반한 자</p> <p>2. 제7조제1항의 규정을 위반하여 인가를 받지 아니하고 사업을 양수하거나 합병·분할한 자</p> <p>3. 제8조제1항 또는 제2항의 규정을 위반하여 승인을 얻지 아니하고 사업의 전부 또는 일부를 휴지하거나 폐지한 자</p> <p>4. 제20조제1항의 규정을 위반하여 개인위치정보의 제공을 거절한 자</p> <p>5. 제24조제2항의 규정을 위반하여 일시적인 중지 요구를 거절 또는 기술적 수단을 갖추지 아니한 자</p> <p>② 다음 각호의 1에 해당하는 자는 1천만원 이하의 과태료에 처한다.</p> <p>1. 제10조제1항의 규정을 위반하여 사업의 양수, 상속 또는 합병·분할의 신고를 하지 아니한 자</p> <p>2. 제11조제1항 또는 제2항의 규정을 위반하여 사업의 전부 또는 일부의 휴지·폐지를 신고하지 아니한 자</p>

	<p>3. 제12조제1항의 규정을 위반하여 이용약관의 신고 또는 변경신고를 하지 아니하거나 제12조제2항의 규정에 의한 이용약관 변경명령을 위반한 자</p> <p>4. 제15조제1항의 규정을 위반하여 소유자의 동의를 얻지 아니하고 이동성이 있는 물건의 위치정보를 수집·이용 또는 제공하거나 제15조제3항의 규정을 위반하여 위치정보 수집장치가 부착된 사실을 고지하지 아니한 자</p> <p>5. 제18조제1항 또는 제19조제1항의 규정을 위반하여 이용약관명시를무를 다하지 아니한 자</p> <p>6. 제18조제3항의 규정을 위반하여 개인위치정보를 수집한 자</p> <p>7. 제19조제2항 또는 제3항의 규정을 위반하여 고지 또는 통보를 하지 아니한 자</p> <p>8. 제22조의 규정을 위반하여 사업의 양도등의 통지를 하지 아니한 자</p> <p>9. 제24조제3항의 규정을 위반하여 열람, 고지 또는 정정요구를 거절한 자</p> <p>10. 제25조제1항의 규정을 위반하여 법정대리인의 동의를 얻지 아니하고 개인위치정보를 수집·이용 또는 제공한 자</p> <p>11. 제29조제1항의 규정에 따른 긴급구조요청을 허위로 한 자</p> <p>12. 제29조제4항의 규정을 위반하여 개인위치정보의 제공사실을 통보하지 아니한 자</p> <p>③제32조의 규정을 위반하여 통계자료를 제출하지 아니한 자는 500만원 이하의 과태료에 처한다.</p> <p>④제1항, 제2항제1호 내지 제10호, 동항제12호 및 제3항의 규정에 의한 과태료는 대통령이 정하는 바에 따라 방송통신위원회가 부과·징수한다. <개정 2008.2.29></p> <p>⑤제4항의 규정에 의한 과태료 처분에 불복이 있는 자는 그 처분의 고지를 받은 날부터 30일 이내에 방송통신위원회에 이의를 제기할 수 있다. <개정 2008.2.29></p> <p>⑥제4항의 규정에 의하여 과태료 처분을 받은 자가 제5항의 규정에 의하여 이의를 제기한 때에는 방송통신위원회는 지체없이 관할법원에 그 사실을 통보하여야 하며, 그 통보를 받은 관할법원은 비송사건절차법에 따른 과태료의 재판을 한다. <개정 2008.2.29></p> <p>⑦제5항의 규정에 의한 기간 이내에 이의를 제기하지 아니하고 과태료를 납부하지 아니한 때에는 국세체납처분의 예에 따라 이를 징수한다.</p> <p>⑧제2항제11호의 규정에 따른 과태료는 대통령이 정하는 바에 따라</p>
--	---

	소방본부장 또는 소방서장이 부과·징수한다.
	⑨제5항 내지 제7항의 규정은 제8항의 규정에 의한 과태료 처분에 이를 준용한다. 이 경우 "방송통신위원회"와 "국세채납처분의 예"는 각각 "소방본부장 또는 소방서장"과 "지방세채납처분의 예"로 본다.

나. 위치정보와 개인위치정보

우리 위치정보법은 “위치정보”와 “개인위치정보”를 구분하고 있다. 위치정보는 “이동성이 있는 물건 또는 개인이 특정한 시간에 존재하거나 존재하였던 장소에 관한 정보로서 「전기통신사업법」 제2조 제2호 및 제3호에 따른 전기통신설비 및 전기통신 회선설비를 이용하여 수집된 것”²⁰²⁾으로 정의된다. 이 때 전기통신은 “유선·무선·광선 또는 그 밖의 전자적 방식으로 부호·문언·음향 또는 영상을 송신하거나 수신하는 것”²⁰³⁾을 모두 포함하며 GPS에 의한 수집과 기지국 기반의 수집 등 현재 모바일기기의 위치를 수집하는 모든 방법을 포섭한다. 예컨대 RFID 기능을 가진 IC칩을 내장하고 있어 교통카드 기능 등을 할 수 있는 모바일기기의 경우 이론적으로 위치추적이 가능하다. 개인위치정보는 이 중에서“특정 개인의 위치정보”²⁰⁴⁾를 의미한다. 모바일서비스에 이용되는 위치정보에는 단순 위치정보와 개인위치정보가 혼재되어 있다. 대표적인 예로, 대중교통 검색서비스를 제공하는 “Seoul Bus” 앱의 경우, 이용자의 모바일기기 위치를 기반으로 이용자 주변의 버스정류소에 도착하는 버스의 현재위치와 도착예정시간 등을 알려주는데, 이 때 이용자의 위치정보는 개인위치정보에 해당하고 버스의 위치정보는 개인식별력을 갖추지 않은 단순 위치정보에 해당한다. 지하철공사에서 제공하는 지하철 도착시간 안내 서비스의 경우에도 전동차의 위치정보는 단순 위치정보에 불과하나, 개인이 소지한 모바일기기의 위치정보는 개인위치정보에 해당한다. 따라서 모바일서비스와 관련해 개인위치정보는 GPS나 기지국을 통해 파악한 단말기의 위치정보가 해당될 수 있다.

위치정보법이 개인정보로서 보호하고자 하는 것은 개인위치정보에 한정되며, 이에 대

202) 위치정보법 제2조 제1호.

203) 전기통신사업법 제2조 제1호.

204) 위치정보법 제2조 제2호.

해서는 단순 위치정보보다 더욱 높은 수준의 의무를 위치정보사업자 또는 위치기반서비스사업자(이하 ‘위치정보사업자 등’)에게 부과하고 있다는 점에서 단순 위치정보와 개인위치정보의 구별의 실익이 있다. 예를 들어 위치정보사업자 등이 사업을 폐지하는 경우에는 보유하는 위치정보를 모두 파기하여야 할 의무를 지는 반면, 사업을 휴지하는 경우에는 휴지의 사실을 개인위치정보주체에게 알리고 보유하고 있는 개인위치정보를 파기하여야 한다.²⁰⁵⁾ 또한 위치정보의 수집·이용·제공을 위해서는 개인 또는 소유자의 동의가 있어야 할 것만을 요구하는데 비하여, 개인위치정보의 경우에는 수집시 구체적으로 위치정보사업자의 상호, 주소, 전화번호 그 밖의 연락처, 개인위치정보주체 및 법정대리인의 권리와 그 행사방법, 위치정보사업자가 위치기반서비스사업자에게 제공하고자 하는 서비스의 내용, 위치정보 수집사실 확인자료의 보유근거 및 보유기간, 그 밖에 개인위치정보의 보호를 위하여 필요한 사항으로서 대통령령이 정하는 사항을 모두 위치정보사업자의 이용약관에 명시하여 동의를 받을 것을 추가적으로 규정하고 있다.²⁰⁶⁾ 또한, 이용·제공시에는 위치기반서비스사업자의 상호, 주소, 전화번호 그 밖의 연락처, 개인위치정보주체 및 법정대리인의 권리와 그 행사방법, 위치기반서비스사업자가 제공하고자 하는 위치기반서비스의 내용, 위치정보 이용·제공사실 확인자료의 보유근거 및 보유기간, 그 밖에 개인위치정보의 보호를 위하여 필요한 사항을 위치기반서비스 이용약관에 명시하여 동의를 받을 것을 규정하고 있다.²⁰⁷⁾ 또한, 위치기반서비스사업자가 개인위치정보를 개인위치정보주체가 지정하는 제3자에게 제공하는 서비스를 하고자 하는 경우에는 위와 같은 내용을 이용약관에 명시한 후 제공받는 자 및 제공목적은 개인위치정보주체에게 고지하고 동의를 얻어야 하며, 이에 따라 개인위치정보를 제공할 때에는 매회 개인위치정보주체에게 제공받는 자, 제공일시 및 제공목적은 즉시 통보하여야 할 것을 규정하고 있다.²⁰⁸⁾ 사업의 양도 등의 통지의무나 수집목적 달성시 파기 의무 역시 개인위치정보에 대해서만 규정되어 있다.²⁰⁹⁾

스마트폰을 비롯한 모바일기기의 위치정보가 개인위치정보에 해당하는지에 대하여 과

205) 위치정보법 제8조, 제11조.

206) 위치정보법 제15조, 제18조.

207) 위치정보법 제19조.

208) 위치정보법 제19조.

209) 위치정보법 제22조, 제23조.

거 우리나라 감독당국은 일관되게 피쳐폰을 포함하여 모든 개인이동통신기기의 위치정보를 개인위치정보로 간주해온 것으로 보인다. 2007년 이동통신사의 제3자에 대한 휴대폰 위치정보 무단 제공을 정보통신부가 묵인하였다는 보도²¹⁰⁾에 대해 당시 정통부는 해명자료를 통해 이동통신사는 위치정보법에 따라 위치정보 제공시 이용자에게 위치정보 조회사실을 즉시 통보할 의무가 있음에도 이를 위반하였다고 밝힌 바 있다.²¹¹⁾ 이 때 정통부가 적용된다고 한 법규정은 위치정보법 제19조 제3항으로서, 동 조는 개인위치정보의 제3자 제공에 관한 규정으로, 정통부의 판단은 이동전화의 위치정보는 개인위치정보에 해당함을 전제로 하고 있다. 또한 2010년 말 방송통신위원회가 프라이버시 문제를 포함해 모바일기기의 보안위협에 대응하기 위한 중장기 계획으로 발간한 “스마트 모바일 시큐리티 종합계획”에서도 이용자의 자기위치정보 통제권 강화를 위한 ‘개인위치정보 자기제어시스템 구축’을 과제로 선정하고 있는 등 모바일기기의 위치정보 문제를 개인정보보호의 문제로 다루고 있다는 점에서 위와 동일한 입장으로 해석할 수 있을 것이다.

그러나 2011년 방송통신위원회의 애플과 구글에 대한 위치정보법 위반행위에 대한 조사 과정을 살펴보면 기술의 발전에 따라 이러한 입장을 수정할 필요성이 제기되었다. 모바일기기로부터 수집된 모든 위치정보가 개인위치정보에 해당하지 않을 수 있다는 점이 확인되었기 때문이다. 동 조사에서 당사자들의 위치정보 수집에 대하여 개인위치정보의 수집에 대한 제18조를 적용하지 아니하고 위치정보 일반에 적용되는 제15조를 적용하여 과거와 상충된 입장을 보였는데, 이는 애플의 해명과 방통위의 조사 결과 이 사안에서 수집된 정보는 개인을 식별할 수 없는 단순 위치정보에 해당한다는 사실이 입증되었기 때문이다. 즉, 애플이 아이폰으로부터 전송받아 수집하는 정보는 개별 아이폰 내에 자신의 위치를 기록한 위치정보 캐쉬 파일인데, 동 파일에는 개인을 식별할 수 있는 요소가 존재하지 않았다.²¹²⁾ 이미 익명화처리가 된 상태에서 전송된 것이기 때문에 수

210) YTN, 2007. 2. 4. 보도, “이통3사, ‘위치추적’ 통보 무시 불법영업”; 경향신문, 2007. 2.

5. 보도, “이통사 위치추적 ‘불법장사’ 정통부선 알고도 묵인”.

211) 정보통신부 해명자료(2007. 2. 5)

212) 방송통신위원회 보도자료, “방통위, 애플 및 구글의 위치정보보호 법규 위반행위에 대해 시정요구 및 과태료 부과”, 2011. 8. 3. 참조.

집후 익명화처리를 한 경우와는 명백히 구분된다. 다만, 개별 기기를 식별함이 없이 “주변 AP 위치를 기록함으로써 개별 아이폰 기기의 GPS 위치파악 시간을 단축하기 위해 동 정보를 활용하였다”는 스티브 잡스의 해명은 논리적으로 납득하기 어려운 점이 있다. 만약 위 캐쉬파일에 IMEI 번호 등 기기고유번호가 포함되어 있고 해당 식별번호와 개인을 연결짓고 있는 데이터베이스가 존재한다면 위 캐쉬파일은 개인위치정보에 해당한다. 정보통신망법상 개인정보에 대한 판단에서와 같이 우리 법원은 해당 데이터베이스에 대한 접근의 용이성은 전혀 문제삼지 않고 단지 결합이 쉽게 이루어질 수 있는 지만을 판단하기 때문에²¹³⁾ 이 때 애플이 국내 이동사가 보유한 고객 데이터베이스를 획득할 수 있었는지 여부는 문제되지 않는다. 결론적으로 모바일기기로부터 수집될 수 있는 위치정보는 일률적으로 개인위치정보 및 개인정보에 해당한다고 단정지을 수 없으며, 향후 개별 사안별로 식별가능성 여부를 검토하여야 할 것이다.

2. 개인정보보호법제의 인적·장소적 적용 범위

모바일기기가 갖는 가장 큰 특징 중 하나는 이동성으로, 이는 서비스제공자나 이용자(정보주체)의 위치에 무관하게 서비스를 이용할 수 있다는 데 있다. 따라서 서비스제공자나 이용자가 해외에 있는 경우, 해외에서 이루어진 개인정보 처리에 대하여 우리 법제를 적용할 수 있을 것인지가 문제된다. 특히 모바일서비스의 경우 애플 앱스토어나 안드로이드 마켓과 같은 중개업자는 해외에 서버를 두고 해당 서버에 국내 이용자가 접속하여 이를 이용하는 경우가 많다. 또 국내에서 이용되는 앱 중에는 국내의 개발자가 아닌 해외 개발자가 판매하는 애플리케이션도 많다. 애플이나 구글의 위치정보 수집에 대해 논란이 되었던 경우와 같이 하드웨어 제작자나 운영체제 제공자 역시 문제될 수 있다.

애플이나 구글과 같이 국내에 상업적 실체를 두고 있는 경우에는 국내법을 통한 규제가 어떤 식으로든 가능하다고 할 것이나, 특히 개별 앱개발자의 경우에는 규제가 어렵다. 이들 앱개발자들은 국내에서의 서비스 제공을 예정하고 있지 않으며, 또한 외국의

213) 서울중앙지법, 2011. 2. 23, 판결 2010고단5343.

개인정보보호법제를 일일이 확인하여 반영한다는 것 역시 사실상 불가능하다. 예를 들어 “Endomondo sports tracker” 앱의 경우, 전세계적으로 100만건 이상의 다운로드를 기록하고 있으며²¹⁴⁾ 국내에서도 레저스포츠 활동시 널리 이용되는 앱이다. 이를 제공하는 앱개발자는 덴마크에 소재한 기업이다. 동 애플리케이션은 이메일주소, facebook 계정을 통해 이용자를 식별하고 이용자의 몸무게, 심박수 등의 생체정보, facebook 계정을 활용한 친구관계 정보 등을 수집하고, 이용자가 등산, 런닝, 산책, 자전거 등 이동성 레저활동시 이동거리와 위치 등을 GPS 정보를 이용해 수집하고 기록, 분석, 저장하고 이를 이용자의 facebook과 연동시켜주는 기능을 한다. 이 앱의 설치, 이용시 접하게 되는 이용약관에서는 EU개인정보보호지침을 반영한 덴마크 개인정보보호법²¹⁵⁾에 따른 수집동의 절차를 취하고 있다. 그런데 이러한 동의 절차가 국내법과 상충될 가능성이 있다는 점, 그리고 국내에서 위치기반서비스를 제공하기 위해서는 위치정보법상 등록된 사업자여야 한다는 점 등 서비스제공자의 개인정보 수집, 이용이 국내법에 위반되는 경우 이를 규제하기 어렵다.

1) 형사사법공조 절차의 활용과 한계

개인정보보호법과 정보통신망법은 위반에 대한 처벌 수단으로 형벌과 과태료를 규정하고 있다. 형벌이 부과되는 규정의 경우, 즉 위반행위가 범죄를 구성하는 경우에는 관할권 등에 있어 형법의 기본원칙이 적용된다. 우리 형법은 속지주의와 속인주의를 모두 취하고 있다. 국내에서는 개인정보처리자의 국적을 불문하고 속지주의에 의해 적용이 가능하다. 또한 우리 형법은 내국인의 국외범에 대해서도 처벌을 하고 있으며, 국내 서비스제공자가 관련법규의 적용을 회피하기 위하여 해외에 서버를 두는 경우에도 법리상 처벌을 하는 데에 문제가 없다. 해외에서 외국인의 위반행위가 우리 국민에 대한 범죄를 구성하는 경우에도 형법 제6조에 따라 법률의 적용이 가능하며, 이러한 경우 형사사법공조 절차를 활용할 수 있을 것이다.

그러나 형사사법공조를 통해 해외의 서비스제공자의 문제를 처리하는 것은 매우 제한

214) 2011. 10. 30. 안드로이드 마켓 기준.

215) Danish Act on Processing of Personal Data (Lov om Behandling af Personoplysninger)

적이다. 우선 형법 제6조에 따라 외국에서의 외국인에 의한 범죄에 대해 국내법을 적용하기 위해서는 해당 행위가 행위지의 법률에 의해 범죄를 구성해야 하는데, 일부 개인정보보호의 선진국을 제외하고는 체계적인 개인정보보호 법제를 갖추지 않았거나 혹은 침해행위를 범죄화하지 않는 경우가 대다수이다. 즉, 비교적 새로운 법분야인 개인정보 보호에 있어 국가간 규범의 수렴이 이루어지지 않았기 때문에 법률이 일치하지 않을 가능성이 높기 때문에 형사사법공조절차가 가동되기 위한 쌍방가벌성(dual criminality) 조건이 충족되지 않아 절차가 적용되기 어렵다. 뿐만 아니라 기본적으로 모바일서비스 제공자는 적어도 자신이 영업을 하는 국가의 국내법은 준수하려는 노력을 하기 때문에 영업지국가에서는 범죄를 구성할 여지가 매우 적다. 게다가 이와 같은 절차는 개인정보보호법 등에서 범죄로 규정하는 일부 행위에 대해서만 검토될 수 있다는 점에서 실효성이 떨어진다고 할 것이다.

그럼에도 불구하고 국경을 초월하는 사이버공간의 특성과 한 번 침해되면 그 회복이 사실상 불가능한 개인정보침해사고의 특성상 APEC 국경간 프라이버시 집행협정(Cross-border Privacy Enforcement Arrangement: CPEA)과 같은 지역협정이나 양자협정 등을 통하여 개인정보 보호를 위한 외국과의 공조체제를 구축해나가는 것이 바람직할 것이다.²¹⁶⁾

216) 2010년 7월 공식 발표한 APEC CPEA는 국제적 전자상거래의 활성화를 위해서는 정부간, 사업자간 협력체제의 구축이 필요함을 천명한 1998년 “전자상거래를 위한 행동 계획”(1998 Blueprint for Action on Electronic Commerce)을 바탕으로, 이를 위해서는 개인정보의 국경간 이동에 대한 소비자들의 신뢰를 구축할 필요가 있다는 데 대하여 회원국들이 공감대를 형성하면서 개인정보보호법제의 집행을 위한 지역적 협력체제의 구축을 목적으로 하고 있다. 구체적 목표로 i) APEC 회원국 개인정보보호기관 사이의 정보공유의 활성화, ii) 개인정보보호법제의 집행에 있어 당국간에 효과적인 국경간 협력체제를 증진하기 위한 체제 구축, iii) APEC 영역 외의 국가의 개인정보보호 당국과의 정보공유, 조사 및 집행을 위한 협력 증진을 제시하고 있다. 2011년 11월 현재 호주 정보보호위원회(The Office of the Australian Information Commissioner), 뉴질랜드 정보보호위원회(The New Zealand Office of the Privacy Commissioner), 미국 연방거래위원회(The United States Federal Trade Commission), 홍콩 개인정보보호위원회(The Office of the Privacy Commissioner for Personal Data, Hong Kong, China), 캐나다 정보보호위원회(The Office of the Privacy Commissioner of Canada)가 참여하고 있다. (<http://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Com>)

2) 개인정보보호법의 역외적용 가능성

2009년 방송통신위원회가 Youtube에 대하여 일평균 10만명 이상의 이용자를 보유하는 정보통신서비스제공자가 게시판을 설치·운영하려면 본인확인조치를 하도록 한 정보통신망법 제44조의 5를 근거로 본인확인절차 도입을 요청하였던 사례에서 구글코리아는 이를 거부하고 다만 유튜브의 국가설정을 한국으로 하는 경우에는 동영상 및 댓글 업로드를 못하도록 조치하였을 뿐이다. 이러한 조치에 대해 방통위는 시정명령이 내려지기 전에 자발적으로 조치를 취하였으므로 행정조치의 대상이 되지 않는다는 입장을 밝히고, 나아가 정보통신망법은 국내에서 서비스하는 기업을 대상으로 하는 규제조항인 만큼 동 사안에 적용되지 않는다는 입장을 밝힌 바 있다.²¹⁷⁾ 나아가 2010년에는 유튜브를 아예 본인확인제 대상에서 제외하였는데, 그 이유를 국내법을 적용하기 위해서는 국내 사업자 등록을 해야 하며, 유튜브는 별도의 법인 없이 구글코리아에 의해 운영이 지원되는 것 뿐이므로 정보통신망법의 적용 대상이 되지 않는다고 설명하였다. 따라서 이후 유튜브에 비실명으로 콘텐츠와 댓글을 올리는 것은 본인확인제의 위반이 되지 않는다고 하였다.²¹⁸⁾ 그러나 이와 같은 방통위의 입장에 대해서는 명확한 기준 없이 국내사업자를 차별하는 것이라는 비판이 제기되었으며, 법률을 자의적으로 해석하는 오류를 범하였다는 비판이 제기된다.²¹⁹⁾ 이 사건은 직접적으로 정보통신사업자의 개인정보보호 문제를 언급하지는 아니하였으나, 외국에 기반을 둔 사업자에 대하여 정보통신망법의 적용 자체를 부정하였기 때문에 이러한 입장에서는 개인정보보호 관련 규정의 위반이 있더라도 우리 정부는 아무런 규제 조치를 취할 수 없게 된다.

결국 해외사업자의 국내법 위반행위로부터 우리 국민의 권익을 보호하기 위해서는 해당 사업자에게 우리 법률을 직접적으로 집행할 수 있는 방안이 모색되어야 할 것이다. 이는 효과이론(effects doctrine)²²⁰⁾을 바탕으로 관할권을 확대하는, 이른바 국내법의 역

merce-Steering-Group/Cross-border-Privacy-Enforcement-Arrangement.aspx 참조).

217) 아이뉴스, “방통위, 유튜브 행정조치 “안 하기로””, 2009. 4. 10. 보도.

218) 한겨레신문, “인터넷실명제 유튜브 제외 ‘역차별’ 논란”, 2010. 4. 7. 보도.

219) *Ibid*

220) 효과이론이란 외국인의 외국에서의 행위의 결과가 국내에 영향을 미치는 경우, 동 행위에 대하여 국내법의 관할권을 인정하기 위한 이론이다.

외적용을 통해 가능할 것이다. 형법 제6조에 나타나는 제한적인 객관적 영토주의의 입장과는 달리 효과이론에 의할 경우 행위지에서의 위법 여부와 관계없이 국내법이 적용될 수 있기 때문이다.²²¹⁾ 외국인 또는 외국 기업에 대한 국내법의 역외적용 문제는 공정거래법, 독점규제법, 증권거래법, 부정경쟁방지법과 같은 경제법 분야와 저작권법 등 지식재산권법 분야, 소비자보호법, 근로기준법, 사회보장법 등 인권, 노동, 환경 분야에서 꾸준히 시도되어 왔다.²²²⁾

국내법의 역외적용에 대한 국가들의 입장은 미국, EU와 같이 관례와 법률에 의거해 적극적으로 인정하는 경우와 영국처럼 자국내의 자국민에 대해서는 외국의 어떠한 법률도 적용되지 않음을 명시적으로 선언하여 부정하는 경우, 그리고 법률상 입장이 불분명한 경우로 나뉠 수 있다.²²³⁾ 적극적으로 인정하는 국가들의 경우 외국에서 행해진 외국인의 행위가 국내에 일정한 영향을 미치거나 결과를 발생시켰을 경우 이러한 효과를 근거로 하여 역외관할을 인정하고 있는데, 법리 구성에 있어서는 국가에 따라 약간의 차이를 보인다.

미국은 1945년 이래 거래 당사자의 행위가 자국 영토 내에 효과를 미치며, 그러한 의도가 있다면 관할권을 가진다고 하는 효과이론의 입장을 취하고 있다. 그러나 이러한 미국의 강경한 입장은 증거확보, 배상제도 등으로 인해 다른 국가들의 반발을 일으켜 영국과 같이 이를 명시적으로 부정하는 대항입법을 하거나 외교적으로 항의를 제기하는 등 문제가 발생하였다.²²⁴⁾ 이에 따라 연방항소법원은 *Timberlane* 사건²²⁵⁾에서 관할 행사 여부를 판단하기 위한 이익형량이론을 채택하였다.²²⁶⁾ EU의 경우 미국이 주장하는

221) 김민서, 한국 경쟁법의 역외적용과 국제법적 평가, 국제법학회논총, 제51권 제3호(통권 제106호), 2006. 12., pp.181-183 참조.

222) James Crawford, *The Creation of States in International Law*(Oxford, Clarendon Press, 1979), pp.81-82.

223) 노영돈, 국내경제법의 역외적용과 국가관할권의 충돌에 관한 연구-경쟁법을 중심으로, 국제법학회논총, 제47권 제1호(통권 제92호), 2002. 4., p.57.; 소병천, 국내법의 역외적용에 관한 미국의 관행, 국제법학회논총, 제49권 제3호(통권 제100호), 2004. 12., p.

224) Malcolm Shaw, *International Law*, Cambridge University Press, 2008, pp.689-690.

225) *Timberlane Lumber Co v. Bank of America*, 549 F.2d 597(9th Circuit 1976), *on appeal following remand*, 749 F.2d 1378(9th Circuit 1979).

226) 박노형, "다국적기업의 거래상의 지위남용 행위에 대한 연구", 공정거래위원회(1997),

효과이론보다 제한적인 의미에서의 효과이론을 확립하고 있으며, 자신의 영토와의 실질적 연관성을 관할권 행사의 근거로 하고 있다. 이는 EU 역내에 자회사가 있는 경우 역외의 모기업에 대하여 통제가능성을 근거로 책임을 인정하는 경제적 단일체 이론으로서 출발하였다. 이후 유럽사법법원은 담합행위가 어디에서 이루어졌는지의 여부와 무관하게 그러한 담합의 결과가 실행되는 장소에 따라 관할권이 적용된다고 하는 이른바 ‘이행이론’을 확립하여 적용하고 있다.²²⁷⁾

우리나라의 경우 경쟁법 분야에서 역외관할을 적극적으로 인정한다. 예를 들어, 2002년 최초로 공정거래위원회가 외국 기업들이 외국에서 행한 가격담합에 대하여 우리나라의 「독점규제 및 공정거래에 관한 법률」(이하 ‘공정거래법’)을 역외적용하여 해당 기업들에게 시정명령과 과징금을 부과하는 결정을 내린 바 있다. 일부 기업은 그 취소를 구하는 행정소송을 제기하였는데, 동 사건에서 대법원은 공정거래법의 적용대상은 ‘제조업, 서비스업, 기타 사업을 행하는 자’로 규정하고 있을 뿐 내국사업자로 한정하고 있지 않다는 점과 외국에서의 부당행위가 국내시장에 영향을 미치는 경우 공정거래법의 목적을 달성하기 위해서는 적용대상이 될 필요성이 있으므로 공정거래위원회의 처분은 정당하다고 판시하였다.²²⁸⁾ 동 사건을 계기로 우리 공정거래법에는 이와 같은 내용과 국제협력에 관한 내용을 명문화하였다.²²⁹⁾ 다만, 이러한 입장의 바탕이 미국식의 효과이론과 이익형량이론에 있는 것인지 유럽사법법원의 이행이론 및 경제적단일체이론

p.25. 동 사건에서 항소법원은 반독점법의 역외적용에 대해 미국의 해외통상에 대한 실제의 또는 의도된 일정한 효과가 존재할 것이 요구되며, 효과가 원고에게 인식할 수 있는 손해를 주기에 충분히 크다는 것이 입증될 것, 그리고 외국의 이익에 비하여 미국의 이익이 충분히 큰 것인지에 대한 여부가 검토되어야 한다고 하였다. 이에 따라 ① 외국의 법 또는 정책과 충돌의 정도, ② 당사자들의 국적, 소재지 및 주된 영업장소, ③ 각 국가의 판결의 집행 기대의 정도, ④ 외국에 비교하여 미국에 대한 효과의 상대적 중요성, ⑤ 미국 통상에 영향 또는 해를 주려는 의도의 존재, ⑥ 그러한 효과의 예견가능성, ⑦ 해외의 활동에 비교하여 미국에 대한 활동의 상대적 중요성이 고려되어야 한다고 판시하였다.; M. Shaw, *supra* note .

227) 박노형, *supra* note 227. pp. 23-37 참조.

228) 대법원 2006. 3. 24. 선고, 2004두11275 판결.

229) 2004년 개정으로 신설된 공정거래법 제2조의 2는 다음과 같다.

“이 법은 국외에서 이루어진 행위라도 국내시장에 영향을 미치는 경우에는 적용한다.”

에 있는 것인지는 명확하지 않다.²³⁰⁾ 공정거래법의 규정은 매우 원칙적인 효과이론을 반영하고 있으나, 위 사례의 경우 외국에서의 담합행위가 국내에서 이행됨으로써 영향을 미친 것에 대해 제재를 가한 것으로서 이행이론에 근거를 둔 것으로 해석할 수 있을 것이다.²³¹⁾

개인정보보호법 역시 정보주체의 기본권을 보호함을 목적으로 하고 있다는 점에서 공정거래법의 경우와 같이 효과이론에 의한 관할권 확장을 시도할 수 있을 것이다. 이를 위해 공정거래법 제2조의 2와 유사한 규정을 추가하여 국내법에 관할권 확장에 대한 근거규정을 마련하는 것이 바람직하다. 다만, 명문규정 없이도 역외적용을 인정한 공정거래위원회와 법원의 입장에서 드러났듯이 규정의 존재는 법률의 역외적용을 위해 반드시 필요한 것은 아니며, 선언적 역할을 하는 것에 불과하다.²³²⁾ 또한 국제법의 영토주권원칙에 따라 영토 밖으로 관할권을 확장하는 것은 매우 제한적인 예외에 해당하며, 국내법 규정이 국제적인 관할권 충돌의 문제를 해소하는 것은 아니다. 그러나 국내법의 역외적용에 관한 문제는 집행상의 실효성 문제를 떠나 국내법원에 의해 판단이 내려진다. 개인정보보호 분야에서는 공정거래위원회가 적극적으로 국내법의 역외적용을 시도하였던 것과는 다른 방향의 정책 입장이 전개되고 있는 점에서 향후 사법부에 의한 판단이 청구될 경우 법원의 판단은 예측이 어렵다고 볼 수 있다. 이를 명확히 하기 위한 입법관할을 확대하기 위한 명시적 규정의 창설이 요구된다.²³³⁾

다만 역외적용의 실효성은 집행관할이 실질적으로 행사될 수 있는지에 따라 결정되며, 이는 국제적 다자 또는 양자 조약을 통한 국제협력에 의해서만 실현될 수 있다. 이러한 협력체제의 구축을 위해서는 적어도 양자간 규제 자체에 대하여 보편적 공감대가 형성되어야 하며, 보편적 타당성이 결여된 법률의 역외적용에 대해서는 국제사회로부터 지지를 얻기 힘들다.²³⁴⁾ 집행력을 확보하지 못하면 결과적으로 국내 정보통신사업자 등

230) 김민서, *supra* note ??? p.180.

231) *Ibid* pp.187-188.

232) 김민서, *supra* note , pp.179-180.

233) 국경 개념이 없는 사이버영역에서 개인정보보호는 단일 국가의 영토주권의 제한적 접근이 현실적이지 않을 것이다.

234) 윤중서, “인터넷 산업에 대한 법적 규제 및 활성화 방안”, 저스티스 통권 제121호 (2010. 12.), pp.743-744.

개인정보처리자는 외국의 개인정보처리자에 비해 역차별을 받게 될 수 있으며, 이는 법률이 일반적 평등원칙에 위배되는 결과를 초래할 수 있다는 비판이 제기된다.²³⁵⁾ 따라서 관할권 확대의 실효성을 확보하기 위한 국가간 공조체제 구축을 위한 노력 역시 뒤따라야 할 것이다.

235) 금주환, “일반적 평등원칙의 해석과 적용”, 법조 49권 12호(2000), p.161; 윤중서, 위 논문, p.744에서 재인용.

제3절 동의 획득 절차 — 적법하고 정당한 동의의 획득

이용자의 인식도 조사 및 국가인권위원회의 권고는 현재 통신서비스 제공자에 의하여 제시되는 개인정보 처리에 대한 동의의 획득이 적법하고 정당하게 다루어지고 있는지에 대하여 문제를 제기한다. 이용자의 동의는 모바일 개인정보 보호의 핵심적 내용이다. 이는 동의가 통신서비스 제공자 및 개인정보처리자의 개인정보 처리를 적법하게 만드는 구성요건에 해당하기 때문이다. 정보통신망법은 제22조 내지 제25조에서 개인정보의 수집·이용, 개인정보 처리의 제한, 제3자에 대한 개인정보의 제공, 개인정보 처리의 위탁에 관하여 정보통신서비스 제공자로 하여금 이용자의 동의를 획득할 것을 명시하고 있다. 또한 제26조에 따른 별도의 조항을 통하여 동의의 획득 방식을 규정하고 있다. 개인정보보호법 역시 제15조, 제17조 내지 제19조, 제23조, 제24조 등에서 개인정보의 수집·이용, 개인정보의 제3자 제공, 개인정보의 이용·제공 제한, 제3자의 개인정보 이용·제공 제한, 민감정보의 처리 제한, 고유식별번호의 처리 제한에 대한 정보처리의 적법성 여부를 정보주체의 동의에 근거하여 판단하고 있다. 이러한 원칙이 있음에도 불구하고 모바일 환경에서 동의 획득에 대한 문제점이 꾸준히 제기되고 있는 이유를 관련법의 분석을 통해 살펴보면 다음과 같다.

1. 동의 방식의 개선

가. 국내 동의 획득 절차의 문제

정보통신망법 제22조 제1항에 따라 정보통신서비스 제공자는 이용자의 개인정보를 이용하려고 수집하는 경우에 개인정보의 수집·이용 목적, 수집하는 개인정보의 항목, 개인정보의 보유·이용 기간을 이용자에게 ‘알리고 동의를 받아야 한다.’²³⁶⁾ 또한 개인정보보호법 역시 제15조 제2항 및 제22조 제1항에서 개인정보 수집을 위한 정보주체의 동의를 얻기 위하여, 개인정보의 수집·이용 목적, 수집하려는 개인정보의 항목, 개인정보

236) 정보통신망법 제22조 1항.

보의 보유 및 이용 기간, 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용을 정보주체가 이를 명확하게 인지할 수 있도록 ‘알리고 각각 동의를 받아야 한다’고 규정하고 있다.

현행법에서 명시하고 있는 ‘알리고 동의를 받아야 한다’는 문구는 ‘통지 및 동의’를 의미하는 것이 아니라 ‘통지 후 동의’로 해석된다. 또한 동의는 ‘이용자로부터 반대의 입장을 듣지 않는 한 간주’되는 행위가 아니라 이용자로부터의 적극적 행위로서 이루어져야 한다.²³⁷⁾

<표 4-5> 동의 획득 과정에서 제시되어야 하는 필수적 항목

정보통신망법 제22조 1항	개인정보보호법 제15조 2항
<ul style="list-style-type: none"> - 개인정보의 수집·이용 목적 - 수집하려는 개인정보의 항목 - 개인정보의 보유 및 이용 기간 	<ul style="list-style-type: none"> - 개인정보의 수집·이용 목적 - 수집하려는 개인정보의 항목 - 개인정보의 보유 및 이용 기간 - 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용

이용자의 동의를 얻기 위해서는 개인정보 처리에 대한 필수적 항목이 반드시 통지되어야 한다. <표 4-5>에서 나타나는 바와 같이 정보통신망법과 개인정보보호법은 동의를 얻기 위하여 알려야 하는 필수적 항목을 명시함에 있어 차이를 보인다. 개인정보보호법 제6조에 따르면 정보통신망법은 개인정보보호법에 대하여 특별법으로서의 지위를 가지게 된다.²³⁸⁾ 따라서 모바일서비스 분야를 개별적으로 규율하는 정보통신망법 제22조 제1항에 따라 정보통신서비스 제공자가 알려야 하는 필수적 항목은 개인정보의 수집·이용 목적, 수집하는 개인정보의 항목, 개인정보의 보유·이용 기간으로서 개인정보보호법의 경우보다 제한적이다.

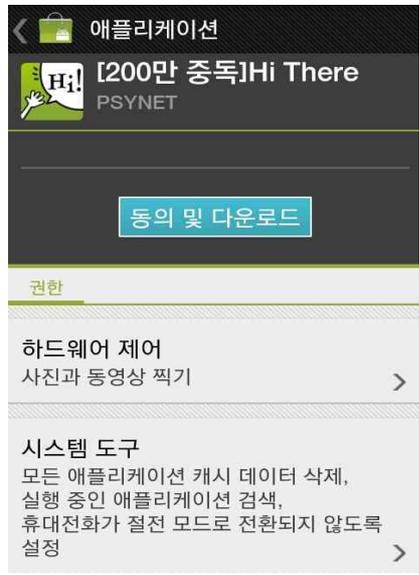
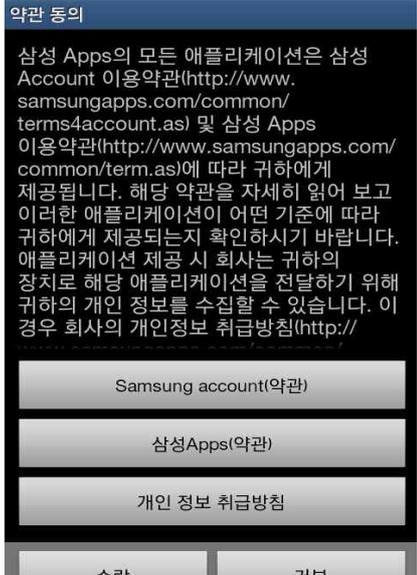
237) EU 개인정보보호지침 제2조는 동의에 대하여 ‘the data subject signifies his agreement’라는 정의 규정을 통하여 이러한 입장을 취하고 있다. 자세한 내용은 Peter Carey, supra note 3, p. 66. 참조.

238) 개인정보보호법 제6조.

1) 개별 정보통신서비스의 상이한 동의 획득 절차

현재 모바일 정보통신서비스 제공자가 제시하고 있는 동의 획득 절차는 OS시스템, 이동통신서비스사, 모바일앱 제공자 마다 모두 다르다. 다음은 인기 모바일앱 프로그램 "Hi there"²³⁹⁾와 삼성 모바일 앱 프로그램이 제시하는 동의 획득 절차이다.

<표 4-6> 모바일 앱에서의 동의 획득 절차의 비교

Hi There 동의 획득 절차	삼성 모바일 앱 동의 획득 절차
 <p>애플리케이션 [200만 중독]Hi There PSYNET</p> <p>동의 및 다운로드</p> <p>권한</p> <p>하드웨어 제어 사진과 동영상 찍기 ></p> <p>시스템 도구 모든 애플리케이션 캐시 데이터 삭제, 실행 중인 애플리케이션 검색, 휴대전화가 절전 모드로 전환되지 않도록 설정 ></p>	 <p>약관 동의</p> <p>삼성 Apps의 모든 애플리케이션은 삼성 Account 이용약관(http://www.samsungapps.com/common/terms4account.as) 및 삼성 Apps 이용약관(http://www.samsungapps.com/common/term.as)에 따라 귀하에게 제공됩니다. 해당 약관을 자세히 읽어 보고 이러한 애플리케이션이 어떤 기준에 따라 귀하에게 제공되는지 확인하시기 바랍니다. 애플리케이션 제공 시 회사는 귀하의 장치로 해당 애플리케이션을 전달하기 위해 귀하의 개인 정보를 수집할 수 있습니다. 이 경우 회사의 개인정보 취급방침(http://www.samsung.com/privacy)을 읽어 주시기 바랍니다.</p> <p>Samsung account(약관)</p> <p>삼성Apps(약관)</p> <p>개인 정보 취급방침</p> <p>수락 거부</p>

<표 4-6>에서 안드로이드 기반체제를 통한 Hi There의 동의 획득 절차에는 하드웨어 제어와 시스템 도구에 대한 정보가 제공되며, 이밖에도 다운로드받기 전 프로그램의 화면에는 전화통화, 위치, 요금이 부과되는 서비스, 저장, 네트워크 통신에 대한 소개가 제공되고 있다. 그러나 이러한 정보들은 개인정보의 수집·이용 목적, 수집하려는 개인정보의 항목, 개인정보의 보유 및 이용 기간 등의 항목과는 거리가 멀다. 정작 필수적 항

239) 앱머썬 2011년 11월 기준 인기 다운로드 모바일 앱 8위.

목들은 이용자가 다운로드받고 난 후에서야 별도의 동의절차를 통하여 제시되고 있다. 이처럼 안드로이드 기반 체계에서 대부분의 모바일 앱 프로그램은 다운로드받기 전 '동의 및 다운로드'절차와, 다운로드받은 후 필수적 항목이 제시되는 개인정보 동의 획득 절차를 구분하고 있다는 문제가 있다. 이용자가 모바일 프로그램을 다운로드받기 전에 접하게 되는 '동의 및 다운로드' 화면에서 개인정보의 수집·이용 목적, 수집하는 개인정보의 항목, 개인정보의 보유·이용 기간이 사전에 알려지고 있지 않다면 이는 적법한 동의라고 보기 어렵기 때문이다.

삼성전자의 스마트폰에 기본적으로 탑재되어 있는 삼성 Apps 역시 안드로이드 체계를 기반으로 하고 있다. 삼성 Apps에서 제공되는 모바일 프로그램을 다운로드받고 이용하기 위해서 이용자는 Samsung account(약관)과 삼성 Apps(약관), 그리고 개인정보 취급방침을 모두 클릭하여 그 내용을 읽어야만 한다. 각각의 내용을 읽지 않는 경우 '수락' 버튼이 활성화되지 않기 때문이다. 정보통신망법 제27조의2 2항에 따라 개인정보 취급방침에서 공개되는 항목은 동법 제22조 1항의 필수적 항목을 포함하고 있다. 이에 따라 삼성 Apps는 약관과 개인정보 취급방침을 제시하는 방법을 통하여 필수적 항목을 제시하고 있다.

이처럼 필수적 항목을 모바일 프로그램을 다운로드받은 후 제시하는 방법과 개인정보 취급방침을 통하여 간접적으로 제시하는 방법이 정보통신망법 제22조 1항의 준수에 해당하는지는 논란의 여지가 있다. 또한 안드로이드의 '마켓'과 달리, 아이폰 '앱 스토어'는 이용자가 모바일 앱 프로그램을 다운로드받기 이전에 어떠한 사전 동의 절차도 제시하지 않고 있다. 이처럼 모바일 운영체제, 스마트폰 제조사, 그리고 개별 모바일 서비스 프로그램에 따라 개인정보 처리에 대한 동의의 방식과 절차가 상이하다는 점은 이용자를 혼란스럽게 만든다.

2) 온라인 특성을 활용한 적법한 사전 동의의 부재

오프라인과 달리 온라인을 통한 개인정보의 처리는 수집을 비롯한 처리방식이 수월하다는 단점을 가지고 있는 반면, 이용자에 대한 높은 접근성을 통해 언제 어디서나 이용자에게 통보가 가능하다는 장점도 가지고 있다. 따라서 무선랜을 이용한 모바일 환경에

서 온라인 웹 브라우저를 이용한 쉽고 빠른 동의 획득 절차는 매우 유효하게 적용될 수 있으며 이러한 방식을 통하여 이용자의 개인정보자기결정권은 용이하게 확보될 수 있다.

그러나, 모바일서비스를 다운로드받을 때 이루어지는 동의가 불안전함에도 불구하고, 광고업체를 비롯한 제3자 제공에 대한 개인정보 처리(이전)에 대한 통보는 <설문 19>에서 나타나듯이 제대로 이루어지고 있지 않다. 무선랜의 특성을 활용한 통보, 동의의 반복적인 획득, 재동의 획득이 기술적으로 가능함에도 불구하고 이러한 개인정보의 처리는 개인정보 취급방침에 언급되어 있다는 이유로 적법성을 가지게 된다. 국내 정보통신망법과 개인정보보호법의 경우, 동의를 받아야 한다는 원칙만을 규정하고 있기 때문에 온라인을 활용한 개인정보 처리의 통보 및 동의는 하위 법령에 따라 세부적으로 입법되어야 하지만 이를 구체적으로 다루는 규정은 아직 존재하지 않는다.

나. 개인정보 동의 절차에 대한 외국의 사례

1) 영국

이용자의 동의를 확보하는 방법으로 영국 ICO(Information Commissioner's Office)의 온라인 홈페이지는 특정 웹주소에 접속하기 전에 화면을 통하여 다음과 같은 개인정보의 처리를 통보하고 있다.

<그림 4-1> 영국 ICO 홈페이지의 개인정보처리 동의화면



출처: 영국 ICO 홈페이지(www.ico.gov.uk)

위 그림에서 다루어지고 있는 쿠키 수집에 대한 동의절차는 2011년 5월에 발효된 EU ‘프라이버시와 전자통신관련 규정’(The Privacy and Electronic Communications (EC Directive) (Amendment) Regulation 2011)의 내용을 반영한 것이다. 동 규정이 온라인 쿠키를 개인정보 범위에 포함시킴에 따라, 정보처리자는 이용자의 로그기록을 수집하는 행위에 앞서서 사전 동의를 얻어야 한다.²⁴⁰⁾ 이에 따라 정보통신서비스 제공자는 <그림 4-3>과 같은 방법으로 이용자가 특정 웹사이트에 접속하기 이전에 쿠키 수집에 대한 동의를 획득한다. 즉, 온라인의 기술적 특성을 이용하여 개인정보를 수집할 때마다 반복적으로 동의를 획득하는 것이다.

2) 미국

미국 연방거래위원회(Federal Trade Commission)는 2010년 보고서에서 이용자의 의사가 어떠한 방식을 통하여 확보되어야 하는지 다루면서 ‘선 동의 후 거부’ 방식에 대한 반대 입장을 명확하게 표명하였다.²⁴¹⁾

특히 FTC는 선택적 동의의 시점과 관련하여 ‘이용자가 개인정보 처리에 대한 동의를 결정하는 시점과 동일한 시점에서 선택적 동의가 이루어져야만 한다(choice mechanism at a time and in a context in which the consumer is making a decision about his or her data)’고 하여 ‘선 동의 후 거부’ 방식을 부정하였다.²⁴²⁾ 또한 모바일서비스에서 개인정보의 제3자 제공과 관련하여 FTC는 제3자가 개인정보를 수집하기 이전에 ‘통보 및 선택 방식’(notice-and-choice mechanism)²⁴³⁾에 의하여 이용자의 사전 동의를 확보해야 한다고 언급하면서 제3자 제공에 대한 언급이 개인정보 취급방침에 포함되어 있다는 사실만으로 이러한 동의 없는 개인정보의 처리가 적법하게 될 수 없다

240) The Privacy and Electronic Communications Regulation 2011, Regulation 6(2)(b), 6(3)(a).

241) Federal Trade Commission, Protecting Consumer Privacy in an Era of Rapid Change, 2011, available at <http://ftc.gov/os/2010/12/101201privacyreport.pdf>.

242) *Ibid* at 58.

243) 해당 보고서의 선택(choice)이라는 용어는 이용자의 동의에 대한 의사결정으로 해석된다.

는 의견을 제시하였다.²⁴⁴⁾ 이는 현재 모바일 개인정보 취급방침에 적시된 내용이 무차별적인 개인정보 수집의 근거로 활용되는 것을 경계하기 위한 목적이다. 또한 FTC는 이용자가 모바일앱서비스를 다운로드받는 경우, 광고자 등 제3자 제공에 대한 해당 앱서비스의 개인정보 처리방식을 이용자가 인식하고 이에 대한 의사결정이 가능하도록 제도의 개선이 필요하다고 언급하고 있다.²⁴⁵⁾

민간자율형 규제를 채택하고 있는 미국은 개인정보 취급방침(Privacy Policy)의 정비를 통하여 동의 절차의 제공 방식을 통일시키려는 노력을 하고 있다.²⁴⁶⁾ 2011년 10월 미국의 모바일 마케팅협회(Mobile Marketing Association)가 제시한 가이드라인은 최근 논란이 되고 있는 모바일앱의 개인정보 취급방침을 통일시키려고 시도하고 있다.²⁴⁷⁾ 동 가이드라인은 모바일앱 개발자에게 처리의 목적, 수집되고 처리되는 개인정보의 항목, 개인정보 보유기간을 포함한 항목들을 이용자에게 제시하도록 권고하고 있다.

특히 동의와 관련하여 가이드라인은 개인정보 처리에 대한 항목을 모두 공개한 후에 ‘당신의 동의’(Your Consent)라는 항목이 의미하는 바가 무엇인지를 설명하도록 제안하고 있다.²⁴⁸⁾ 이러한 가이드라인의 권고는 서비스 제공자가 사전에 ‘동의’가 무엇을 의미하는지, ‘처리’(processing)는 무엇을 의미하는지를 이용자에게 상세히 알리고 나서 동의를 받아야만 한다는 사실을 부각시키고 있다.²⁴⁹⁾ 동 가이드라인에 따르면 모바일앱 제공자에게 동의라 함은 이용자가 제공한 개인정보(User Provided Information)와 자동수집정보(Automatically Collection Information)에 대한 처리의 동의를 의미하며, 처리라 함은 수집, 저장, 삭제, 이용, 결합을 포함하는 행위이다. 특히 미국 외에 거주하는 이용자의 정보는 미국의 사생활보호 기준에 따라 미국으로 이전되어 처리된다.²⁵⁰⁾

244) Federal Trade Commission, Protecting Consumer Privacy in an Era of Rapid Change, 2011, p. 58-59. available at <http://ftc.gov/os/2010/12/101201privacyreport.pdf>

245) *Ibid*, p. 59.

246) 이는 개인정보 처리에 대한 동의와 개인정보 취급방침을 별도의 규정을 통하여 규율하고 있는 국내법 체계와 대비된다.

247) Mobile Application Privacy Policy Framework, October 2011, the MMA Privacy & Advocay Commitee.

248) *Ibid*, at 8.

249) *Ibid*

다. 적법한 사전 동의의 확보

모바일 환경에서 필수적 항목이 이용자에게 사전에 통보되지 않고 있는 현실은 우선적으로 해결되어야 할 문제이다. 이는 크게 법률의 입법 및 개정을 통하거나 정책을 통한 동의 절차의 실효성 확보를 통하여 해결될 수 있다.

입법 및 개정을 통한 해결 방안은 동의 획득 과정의 필수적 항목에 대한 사전 동의를 법적 강제로서 확보하는 방법이다. 정보통신망법은 개인정보에 대한 수집 동의와 개인정보 취급방침을 연계하여 다루고 있지 않다. 동법 제27조의2는 개인정보 처리에 대한 전체적인 내용을 이용자가 이해할 수 있도록 공개해야 한다는 규정으므로 동의 획득과는 별도의 의무를 부여하고 있다. 그러나 제22조 1항의 동의 획득 과정에서 다루어지는 필수적 항목은 개인정보의 수집·이용 목적, 수집하는 개인정보의 항목, 개인정보의 보유·이용 기간으로서 이는 개인정보 취급방침에서도 반드시 다루어져야만 하는 항목이다.²⁵¹⁾ 따라서 미국과 같이 필수적 항목과 개인정보 취급방침을 별도로 구분하지 않고, 필수적 항목을 포함한 개인정보 취급방침을 사전에 공개하는 의무를 부과함으로써 사전 동의의 획득을 효율적으로 확보할 수 있다.

미국 모바일협회가 제시한 가이드라인과 같이 적법한 사전 동의는 실효적인 정책을 통하여 확보될 수 있다. 방송통신위원회 등 감독기관은 가이드라인을 채택하고 이를 이용한 정보통신서비스 제공자에 대한 교육을 통하여 개별 모바일 프로그램 간의 각기 다른 동의 절차를 통일시키기 위한 노력을 하는 것이다. 특히, 가이드라인에는 사전 동의의 중요성에 대한 기본원칙과 함께, 모바일서비스 제공자가 통일적인 동의 획득 방법을 제시할 수 있도록 구체적이고 세부적인 제시방법이 담겨져야만 한다.

250) *Ibid*

251) 정보통신망법 제27조의2 2항

<표 4-7> 동의 획득 필수적 항목의 개정안

정보통신망법 제22조 1항	개인정보보호법 제15조 2항
- 개인정보의 수집·이용 목적	- 개인정보의 수집·이용 목적
- 수집하려는 개인정보의 항목	- 수집하려는 개인정보의 항목
- 개인정보의 보유 및 이용 기간	- 개인정보의 보유 및 이용 기간
- 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용 (삽입)	- 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용

정보통신망법 제22조 1항과 개인정보보호법 제15조 2항 간의 불일치 또한 문제가 된다. 앞서 <표4-7>에서 나타난 바와 같이 정보통신망법과 달리 개인정보보호법 제15조 2항 4호는 ‘동의 획득 과정에 있어서 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용’을 동의의 필수적 항목으로 규정하고 있다. 동의를 거부할 권리가 있다는 사실과 불이익의 내용을 적시하는 행위가 정보통신망법이 규율하는 정보통신서비스 분야에서 특별히 배제되어야 하는 특별한 사정이 없다면, 이를 정보통신망법 제22조 1항의 필수적 항목에 포함시킬 필요성이 있다. 또한 정보통신망법 제22조 제1항의 내용을 삭제하여 필수적 항목에 대한 규정을 개인정보보호법의 일반 규정의 적용을 받게 하는 방안도 고려될 수 있다.

적극적 동의에 대한 사전 확보는 영국 사례에서와 같이 온라인의 특성을 활용하여 이루어질 수 있다. 정보통신망법 제22조 2항 1호는 ‘정보통신서비스의 제공에 관한 계약을 이행하기 위하여 필요한 개인정보로서 경제적·기술적인 사유로 통상적인 동의를 받는 것이 뚜렷하게 곤란한 경우’에 한하여 사업자로 하여금 이용자의 동의 없는 개인정보 수집을 예외적으로 허용하고 있다. 그러나 다른 매체와 달리 무선랜을 통하여 언제든지 인터넷에 접속할 수 있다는 모바일서비스의 특징은 기술적 사유에 근거한 예외조항의 적용을 어렵게 만든다는 점에서 개인정보 보호를 더욱 강화시키는 근거를 제공한다.

2. 선택적 동의제도의 효율적 확보

선택적 동의는 정보통신망법 제24조의2 3항과 개인정보보호법 제16조 2항, 제18조 2항 1호, 그리고 제22조 2항 내지 4항에 명시되어 있다. 예컨대, 개인정보처리자는 정보주체 또는 제3자의 이익을 부당하게 침해할 우려가 있는 경우를 제외하고는 정보주체의 동의를 통하여 ‘목적 외 용도’로 개인정보를 이용하거나 제3자에게 제공이 가능하다.²⁵²⁾

선택적 동의는 과도한 개인정보의 수집을 방지하기 위한 규정이다. 과도한 개인정보 수집에 대하여, 정보통신망법 제23조 2항은 정보통신서비스 제공자로 하여금 정보통신서비스의 제공을 위하여 필요한 최소한의 정보를 수집할 것을 규정할 뿐, 필요한 최소한의 정보에 대한 기준에 대하여는 언급을 하고 있지 않다. 이와 달리, 개인정보보호법은 제16조 1항에서 ‘개인정보를 수집하는 경우에는 그 목적에 필요한 최소한의 개인정보를 수집해야 한다’라고 명시하고 있다. 따라서 과도한 개인정보의 수집이란 동법 제3조 1항에서 명시하고 있는 개인정보 처리 목적의 범위를 초과하는 개인정보의 수집이다. 따라서 어떠한 개인정보의 수집이 과도한지를 판단하기 위해서는 먼저 개인정보 처리 목적의 범위에 대한 명확한 기준이 제시되어야 한다.

가. ‘적법한’ 처리 목적의 확립

모바일 환경에서 처리 목적에 ‘비하여’ 과도하게 개인정보를 처리하는 행위와, 처리 목적의 범위 내에서 개인정보를 수집하고 이용하되 그 처리 목적 자체를 광범위하게 설정하는 행위 사이에는 큰 차이가 있다. 처리 목적의 범위를 초과한 개인정보의 처리는 현행법의 규율을 받지만 처리 목적 자체를 어떻게 정하는지에 대하여는 관련 규정이 존재하지 않는다. 예컨대, 정보통신망법 제23조 제2항과 개인정보보호법 제16조 제1항은 필요한 목적의 최소한의 범위 내에서 개인정보를 수집할 것을 규정하고 있다. 또한 개인정보보호법 제3조 제1항은 개인정보처리자로 하여금 개인정보의 처리 목적을 명확하게 하고 그 목적에 필요한 범위 내에서 최소한의 개인정보만을 적법하고 정당하게 수집해야함을 명시하고 있다.

252) 개인정보보호법 제18조 2항 1호.

그러나 개인정보보호법 제3조 1항의 ‘명확한’ 목적이라는 요건 이외에 처리 목적 자체가 어떠한 요건을 가져야만 하는지, 처리 목적을 어떻게 정해야 하는지에 대한 원칙을 명시한 규정은 존재하지 않는다. 이에 따라, 모바일서비스 제공자가 개인정보의 처리 목적 자체를 서비스의 주된 기능에 국한시키지 않고, 애초부터 처리 목적을 지나치게 넓혀 개인정보를 수집하고 이용한다 하더라도 이는 적법한 개인정보의 처리로 간주될 가능성이 있다.

1) EU 및 영국의 개인정보 보호원칙

국내 개인정보보호법 제3조 1항에 명시된 ‘처리’목적은 EU개인정보보호지침과 영국 개인정보보호법에서 다루고 있는 ‘수집’목적과 대비된다.²⁵³⁾ EU개인정보보호지침은 개인정보의 수집 목적이 ‘구체적이고(specified) 명확하며(explicit) 정당하여야(legitimate) 한다’고 명시하고 있다.²⁵⁴⁾ 영국의 정보보호 제2원칙 역시 이러한 수집 목적에 대한 원칙을 규정하고 있다. 이에 따르면 개인정보는 하나 이상의 특정되고 적법한(lawful) 목적으로만 수집이 가능하며 그 목적에 부합하지 않는 방법으로 개인정보를 처리하는 것은 금지된다.²⁵⁵⁾ 이상의 규정들과 국내법 규정을 비교하여 표로 나타내면 다음과 같다.

253) 영국 개인정보보호법 정보보호원칙 제2원칙은 적법한 ‘수집’ 목적과 이에 부합하는 개인정보의 ‘처리’를 규정하여 개인정보의 수집원칙을 규정하고 있다. 반면 국내 개인정보보호법 제3조 1항은 ‘수집’이 아닌 ‘처리’ 목적에 따라 적법하고 정당한 개인정보의 ‘수집’을 규정하고 있다. 영국 개인정보보호법이 적법한 ‘수집’ 목적에 따라 개인정보의 적합한 ‘처리’를 규정하는 것과 달리, 개인정보보호법은 명확한 ‘처리’ 목적에 따른 적법하고 정당한 ‘수집’을 규정하고 있는 것이다. 즉, 국내 개인정보보호법 제3조 1항은 영국 개인정보보호법 정보보호 제2원칙과 비교하여 ‘수집’과 ‘처리’의 위치가 바뀌어져 규정되어 있다.

254) EU 개인정보보호지침 Article6(b). 이들 법의 ‘정당한’(legitimate)은 우리나라 개인정보보호법 제3조 1항의 ‘정당한’과 다르다. 개인정보보호법 제3조 1항에서의 ‘정당한’ 개인정보의 수집은 EU 및 영국법 규정의 ‘fair’를 의미하는 것으로 이해되어야 하기 때문이다.

255) 영국개인정보보호법 부칙1 제1장 제2조.

<표 4-8> 개인정보 처리 목적과 수집 목적의 요건

국내법	정보통신망법	제24조 정보통신서비스 제공자는 제22조 및 제23조제1항 단서에 따라 수집한 개인정보를 이용자로부터 동의 받은 목적이나 제22조제2항 각 호에서 정한 목적과 다른 목적으로 이용하여서는 아니 된다.
	개인정보보호법	제3조 (개인정보 보호 원칙) ① 개인정보처리자는 개인정보의 처리 목적을 명확하게 하여야 하고 그 목적에 필요한 범위에서 최소한의 개인정보만을 적법하고 정당하게 수집하여야 한다. ② 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 적법하게 개인정보를 처리하여야 하며, 그 목적 외의 용도로 활용하여서는 아니 된다.
		제16조 (개인정보의 수집 제한) 개인정보처리자는 제15조제1항 각호의 어느 하나에 해당하여 개인정보를 수집하는 경우에는 그 목적에 필요한 최소한의 개인정보를 수집하여야 한다. 이 경우 최소한의 개인정보 수집이라는 입증책임은 개인정보처리자가 부담한다.
EU 개인정보 보호지침	Article 6 1. Member States shall provide that personal data must be: (b) <u>collected for specified, explicit and legitimate purposes</u> and not further <u>processed</u> in a way incompatible with those purposes. (회원국은 개인정보가 다음 각호에 따를 것을 규정하여야 한다. (b) 특정되고, 명확하고, 정당한 목적으로 수집하고 이러한 목적과 부합되지 않는 방법으로 처리되지 아니할 것)	
영국 개인정보 보호법	Schedule 1 Part 1 2. Personal data shall be <u>obtained</u> only for <u>one or more specified and lawful purpose</u> , and shall not be further <u>processed</u> in any manner incompatible with that purpose or those purposes. (개인정보는 하나 이상의 특정되고 적법한 목적으로만 수집되어야 하며 그 목적에 부합하지 않는 방법으로 처리되어서는 아니 된다.)	

<표 4-8>에서 나타나는 바와 같이 정보통신망법과 개인정보보호법은 목적 외의 용도, 목적에 필요한 범위를 벗어난 처리를 금지하면서 정작 그 처리 목적에 대해서는 아무런 요건을 규정하고 있지 않다. 개인정보보호법 제3조 1항이 처리 목적이 명확성을 가져야

함을 규정하고 있을 뿐이다. 반면 영국의 개인정보보호법은 개인정보의 수집 목적이 적법(lawful)해야 한다는 원칙을 규정하고, 수집되는 개인정보가 이러한 적법한 목적에 부합하여 처리되어야 함을 명시하고 있다.²⁵⁶⁾

2) 처리 목적에 대한 원칙 수립의 필요성

모바일 앱 프로그램의 경우, 개별 프로그램마다 가지고 있는 서비스의 기능과 아이디어가 다양하기 때문에 감독기관이 제공자가 제시하는 처리 목적이 서비스의 주된 기능에 반드시 필요한 것인지를 판단하기란 매우 어렵다. 정보통신서비스 제공자는 이러한 점을 악용하여 자신의 원하는 개인정보를 제한 없이 수집하고 이용할 수 있다. 처리하고자 하는 개인정보의 항목들을 우선적으로 정하고 해당 항목을 모두 포섭하는 처리 목적을 차후에 추가적으로 마련하면 되기 때문이다.

이러한 문제점을 최대한 방지하기 위하여 개인정보 처리 목적에 대한 원칙을 확립해야 한다. 실제로 영국 개인정보보호법 제6조에 근거하여 설립된 정보보호법정(Information Tribunal)은 다양하고 복잡한 형태로 나타나는 개인정보 피해사례들을 세부 조항이 아닌 원칙조항에 근거하여 판단하고 있다.²⁵⁷⁾ 1997년 영국 *British Gas* 사건²⁵⁸⁾에서 개인정보보호위원(Data Protection Registrar)²⁵⁹⁾은 *British Gas*가 제시한 제3자의 수금대행(third party debt collection)을 위한 개인정보 수집 목적이 개인정보보호 제2원칙에 위반되었다고 주장하였고, *British Gas*는 항변하지 않고 해당 행위를 중지한 바 있다.²⁶⁰⁾ 즉, 제3자 수금대행이라는 수집 목적 자체가 법률의 위반을 구성하였다고 주장한 것이다. 영국은 이처럼 수집 목적과 수집 항목 사이의 비례성 문제를 떠나 개인정보 수집 목적만을 가지고 개인정보보호의 위반여부를 판단하고 있다. 이를 반영하여, 국내 개

256) 영국 개인정보보호법, Schedule 1, Part 1, 2.

257) 이와 관련한 사례들은 아래의 문헌 참조. Peter Carey, *Data Protection A Practical Guide to UK and EU Law* 3ed, Oxford University Press 2009, pp. 73-78.

258) *British Gas Trading Ltd. v. Data Prot. Reg.*, <1997/98> 1 Info. T.L.R. 393, available at http://www.informationtribunal.gov.uk/DBFiles/Decision/i162/british_gas.pdf.

259) 이는 현재 영국 개인정보보호법상 개인정보보호위원(Information Commissioner)에 해당한다.

260) Peter Carey, *Data Protection A Practical Guide to UK and EU Law* 3ed, Oxford University Press 2009, p. 49.

인정보보호법 제3조 1항 역시 처리 목적에 대한 원칙을 통하여 광범위한 처리 목적에 따른 과도한 개인정보의 수집을 방지할 필요가 있다. 이에 따라 제3조 1항의 ‘명확한’에 대하여 ‘적법한’ 처리 목적의 요건이 추가적으로 개정되는 것이 바람직하다.

나. ‘정당한’ 개인정보 수집 원칙의 적용

1) 국가인권위원회 권고를 통한 카카오톡의 문제점

2011년 10월 28일 국가인권위원회는 카카오톡의 강제적이고 고압적인 개인정보 수집 행위가 헌법재판소를 통하여 인정된 개인정보자기결정권을 침해하고 정보통신망법에 대한 위반의 소지가 있다고 밝히고 방송통신위원회에 철저한 조사와 그에 따른 적절한 조치를 취할 것을 권고하였다.²⁶¹⁾ 동 권고는 선택적 동의 제도의 필요성을 다시 한 번 부각시켰다. 국가인권위원회는 카카오톡이 ‘선 동의 후 거부방식’을 적용하여 서비스 제공에 필요한 개인정보 처리 목적의 범위를 초과하는 개인정보를 과도하게 수집하였는데, 동의를 획득 후 ‘옵트아웃’(opt-out) 방식을 적용하여 개인정보자기결정권을 침해할 소지를 야기하였다고 밝힌 바 있다.²⁶²⁾

국가인권위원회의 권고에서 주목할 점은 동 위원회가 ‘옵트인’(opt-in)과 ‘옵트아웃’(opt-out)의 차이를 구별하고 있다는 점이다. 두 방식의 차이에 대하여 현행법에서는 아무런 구별을 하고 있지 않다. 옵트인 방식에서 정보주체는 자신이 원하는 개인정보의 처리를 선택하여 지정할 수 있고, 정보처리자는 정보주체가 동의한 항목에 대해서만 처리가 가능하다. 반면, 옵트아웃 방식에서는 개인정보처리자가 원하는 항목에 대하여 기본적인 처리를 하되 정보주체가 이에 대한 동의를 거부하는 경우에 한하여 그에 대한 처리가 금지된다. 정보주체가 아무런 의사표시를 하지 않는 경우, 목적의 범위를 초과하는 개인정보의 처리는 옵트아웃 방식에서는 허용되는 반면, 옵트인 방식에서는 허용되지 않는다. 이러한 측면에서 옵트인 방식은 옵트아웃 방식에 비하여 정보주체의 권익을 더욱 엄격하게 보호할 수 있다.

261) 국가인권위원회 보도자료, “인권위, 기업의 강제적 개인정보 수집 관련 일체 점검 및 가이드라인 제정 권고”, 1쪽.

262) 위 보도자료, 2-3쪽.

그러나, 옵트인이 아니라 옵트아웃이기 때문에 개인정보보호에 문제가 있다는 국가인권위원회의 권고는 자칫 모든 선택적 동의의 방식이 옵트아웃이 아닌 옵트인이 되어야 한다는 잘못된 논리로 발전할 가능성이 있다.²⁶³⁾ 현행법에서 두 방식을 구별하는 명시적 조항이 존재하지 않는다. 또한 두 가지 방식은 의사결정의 방식이지 시간적 순서를 따지지 않는다. 옵트인이 사전 동의와 동일한 개념이 아니며, 옵트아웃 역시 ‘선 동의 후 거부’와는 구별되는 개념이다. 개인정보 처리에 대한 사전 동의 획득 절차에서 옵트아웃 방식이 적용될 수 있고, 실제로 적용되는 사례가 많기 때문이다.

국가인권위원회가 언급한 ‘선 동의 후 거부 방식’이라는 표현에서 알 수 있듯이, 정작 문제가 되는 것은 동의를 획득하는 과정에서 부가항목에 대한 동의의 기회가 주어지지 않았다는 데 있다. 즉, 수집 목적의 범위를 초과하는 개인정보에 대하여 ‘사후에’ 거부의 의사표시를 받았다는 점에서 카카오톡 사례는 선택적 동의의 문제와 함께 포괄적인 사전 동의의 문제를 가지고 있는 것이다. 이와 관련하여 미국 FTC는 서비스 제공에 반드시 필요한 개인정보 수집에 대하여, 동의 획득의 시점과 선택적 동의의 시점이 동일하여야 한다는 견해를 밝힌 바 있다.²⁶⁴⁾ 현행법상 이용자가 개인정보자기결정권을 확보함에 있어서 개인정보 처리에 대한 사전 동의 절차는 거의 모든 부분을 차지한다. 이에 따라 부가항목에 대한 추가적인 개인정보 수집의 동의는 필수항목에 대한 개인정보 수집의 동의와 함께 개인정보 처리 이전에 이용자로부터 사전 확보되는 것이 바람직하다.

2) 영국 British Gas 사건: 공정한 개인정보의 처리

영국의 정보보호원칙 제1원칙은 개인정보 처리가 적법한(lawful) 동시에 공정(fair)할 것을 규정하고 있다.²⁶⁵⁾ 카카오톡의 사례는 영국 개인정보보호법의 ‘공정한’(fair) 개인정보 처리의 중요성을 다루었던 영국 British Gas 사건과 유사하다. 동 사건에서 개인

263) 위 보도자료, 2쪽.

264) Federal Trade Commission, Protecting Consumer Privacy in an Era of Rapid Change, 2011, p. 58.

265) 영국 개인정보보호법 Schedule 1, Part 1, 1.

정보처리자인 가스회사는 개인정보 처리에 대한 동의를 얻었던 기존 고객에게 전단지
통하여 추가된 개인정보 처리에 대한 내용을 통보하면서, 부가항목에 대한 수집을 원하
지 않는 고객에게 전단지상 동의 거부란에 표시한 후 이를 회사에 별도로 발송할 것을
요구하였다.²⁶⁶⁾ 법원은 이에 대하여 이미 개인정보 처리에 동의한 정보주체가 서비스에
필요한 최소한의 개인정보가 아닌 광고의 거부를 위하여 별도의 절차를 거쳐야 하는 것
은 ‘불공정한’(unfair) 개인정보 처리에 해당한다고 판시하였다.²⁶⁷⁾ 즉, 서비스의 주된
목적은 벗어나는 개인정보의 수집을 거부함에 있어서 정보주체에게 별도의 의사표시를
사후에 요구하는 동의 획득 방식은 영국 개인정보보호법상 ‘공정하지’(fair) 못하다는
것이다.

이처럼 적법성과는 별도로 ‘공정성’(fairness)이라는 요건을 개인정보보호의 기본원
칙으로 규정함에 따라 영국 개인정보보호법은 개인정보처리자의 행위가 법률의 요건을
충족하여 적법하더라도, 정보주체에게 과도한 의무를 부담하거나 일방적이고 강압적으
로 개인정보를 처리하는 경우 ‘공정성’(fairness)이라는 원칙조항에 근거하여 해당 행
위를 규제할 수 있다.²⁶⁸⁾

3) 선택적 동의 방식의 정착을 위한 정당성 원칙의 적용

선택적 동의의 방식은 정보통신망법과 개인정보보호법에 모두 규정되어 있으나 그
실효성이 확보되어 있지 않다. 옵트인이 올바른지 옵트아웃이 올바른지에 대한 논의는
개별 사례에 따라 다르게 적용되어야 한다. 이러한 선택적 동의의 국내 정착을 위해서
는 영국의 개인정보보호법에 자리잡고 있는 ‘공정성’(fairness)의 원칙이 국내법에서도
적극 적용되어야 한다.

정보통신망법에는 개인정보 처리에 대한 원칙조항이 존재하지 않는다. 이는 동 법이
이용자의 개인정보 보호만을 규율하는 것이 아니라 ‘기술개발의 추진’, ‘기술관련
정보의 관리 및 보급’과 같은 정보통신망의 이용촉진 전반의 내용도 규율하는 전문법

266) British Gas Trading Ltd. V. Data Protection Registrar <1998> Info. T.L.R. 393, at 415-16.

267) British Gas Trading Ltd. V. Data Protection Registrar <1998> Info. T.L.R. 393, at 415-16.

268) Peter Carey, supra note 3, p. 57-58.

이기 때문이다.²⁶⁹⁾ 정보통신망법이 구체적인 적용대상과 범위를 가지고 있는 전문법인 반면, 개인정보보호법은 개인정보에 대한 모든 사항을 통합하여 규율하는 일반법이다. 개인정보보호법은 제3조에서 개인정보보호의 기본원칙을 규정하고 있으며, 동조 제1항은 개인정보처리자로 하여금 ‘적법’하고 ‘정당’하게 개인정보를 수집할 것을 규정하고 있다.²⁷⁰⁾

<표 4-9> 영국 개인정보보호법 개인정보 처리원칙과
국내 개인정보보호법 개인정보 수집원칙의 비교

UK Data Protection Act Schedule 1, Part1, 1	Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless (a) at least one of the conditions in Schedule 2 is met, and (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.
국내 개인정보보호법 제3조 제1항	개인정보처리자는 개인정보의 처리 목적을 명확하게 하여야 하고 그 목적에 필요한 범위에서 최소한 개인정보를 적법 하고 정당 하게 수집하여야 한다.

<표 4-9>에서 나타나는 바와 같이, 영국법은 적법하고(lawful) ‘공정한’(fair) 개인정보 처리를 원칙으로 하여 두 가지 요건의 충족을 모두 요구하고 있다. 이에 비추어 볼 때, 국내법의 ‘정당한’ 개인정보의 수집은 ‘공정한’(fair)의 개념으로 해석되어야 할 것이다.

예컨대, 영국 *British Gas* 사건처럼 부가항목에 대한 ‘선 동의 후 거부’방식을 적용한 카카오톡의 사례는 적법하지만 ‘정당’하지 못한 개인정보의 수집이 될 수 있다.

269) 정보통신망법 제2절.

270) 여기에서도 마찬가지로 우리나라와 영국의 개인정보보호법은 ‘처리’와 ‘수집’의 위치가 바뀌어져 있다. 영국 개인정보보호법 부칙 1장 정보보호원칙 제1원칙은 적법하고 공정한 ‘처리’를 규정하고 있는 반면, 국내 개인정보보호법 제3조 1항은 적법하고 정당한 ‘수집’을 규정하고 있다.

동의 획득 절차에서 필수적 항목을 제시하여 동의를 획득하고,²⁷¹⁾ 사후에 옵트아웃 방식을 통하여 부가적인 개인정보의 처리를 이용자가 거부할 수 있도록 한다면 이에 대한 현행법의 위반은 발견되지 않는다.²⁷²⁾ 그러나, 각각의 법률요건을 충족하여 적법한 수집이 된다 하더라도 이용자에게 선택하여 동의할 수 있는 기회를 사전에 부여하지 않는다면 이는 ‘정당한’ 수집이라고 보기가 어렵다. 따라서 영국법의 ‘공정한’(fair) 개인정보 처리 원칙과 같이, 정보통신서비스 제공자의 경우 적법하나 정당하지 못한 개인정보의 수집을 규율하기 위하여 개인정보보호법 제3조 제1항의 ‘정당한’ 개인정보의 수집 원칙은 ‘적법한’ 개인정보의 수집 원칙에 상응하는 개인정보 수집 원칙으로써 적극적으로 적용되어야만 한다.

271) 정보통신망법 제22조 1항, 개인정보보호법 제15조 1항.

272) 정보통신망법 제23조2항, 개인정보보호법 제22조 4항.

제4절 개인정보파일 등록 및 개인정보 영향평가 대상의 확대

개인정보가 무단으로 또는 과도하게 수집되더라도 실제 유출사고가 발생하기 전까지는 개인정보가 수집되었다는 사실을 이용자 또는 수사기관이 인지하기 매우 어렵다. 실제로 개인정보와 관련해 대중적으로 널리 알려진 사건들은 국내외를 막론하고 정보 유출, 누출, 누설²⁷³⁾이 발생한 후의 문제였으며, 개인정보의 수집 단계에서 관련한 사건은 극소수에 불과하다. 국내의 경우 증권통 사건은 다른 사건을 수사하던 중 검찰이 자체적으로 인지하여 수사를 개시한 경우였고, 구글 스트리트뷰에 대한 조사의 경우도 국제적인 쟁점이 되면서 조사가 개시된 바 있다. 또한 개인정보 유출 또는 누설의 경우 한번 유출된 개인정보는 회수하기가 사실상 불가능한 경우가 많으며, 실질적인 피해 발생 여부와 관계 없이 그 사실 자체만으로도 개인정보자기결정권을 침해하여 개인정보를 제3자가 알게 되거나 이를 도용 또는 악용할지도 모를 위험에 노출되었다는 것만으로 정보주체의 정신적 고통이 인정된다.²⁷⁴⁾

273) 정보통신망법상 “누출”은 개인정보가 정보통신서비스제공자 및 이용자의 개인정보 관리·통제권의 범위를 벗어나 당해 개인정보를 모르는 제3자가 그 내용을 알 수 있는 상태에 이르는 것을 의미하며, 침해, 누설, 도용의 경우처럼 당해 개인정보를 모르는 제3자가 현실적으로 그 내용을 알게 되었다거나 적어도 이와 동일시할 수 있는 정도의 구체적이고 현실적인 고도의 위험이 발생할 것 또는 당해 개인정보를 모르는 제3자에게 그 내용을 알릴 것 또는 이를 도용할 것까지 요구하는 것은 아니다.(서울중앙지법 2009. 11. 6. 판결 2008가합75268, 2009가합91281 병합) 개인정보보호법상에는 “누출”의 개념은 존재하지 않으며, “유출”과 “누설”만을 구분할 뿐이다. 정보통신망법상에는 “누출”과 “유출”의 용어가 혼재되어 사용되고 있다. 이에 비해 “누설”은 정보통신망법 제 28조의 2, 개인정보보호법 제59, 60조의 취지에 비추어볼 때 업무담당자의 고의가 포함 된, 보다 협소한 개념으로 볼 수 있다. 법원은 과거 「공공기관의 개인정보보호에 관한 법률」 위반 사건에서 경찰공무원인 피고인이 당사자의 동의 없이 업무상 알게 된 통화내역을 고소장에 첨부하여 제출한 것은 고의적 행위로서 개인정보 누설에 해당한다고 판시한 바 있다.(서울중앙지법 2008. 6. 12. 선고 2008노1198, 대법원 2008.10.23. 선고 2008도5526)

274) 서울중앙지법 2007. 2. 8. 선고 2006가합33062. 실질적 피해가 발생하였는지의 여부와 관계 없이 개인을 식별할 수 있는 정보가 유출(누출)되었다면 해당 개인정보의 정보주체에게 정신적 고통으로 인한 손해배상청구권을 인정하는 것이 우리 법원의 일관된 입

따라서 개인정보보호의 문제에 있어서는 개인정보의 무단수집이나 제3자에 대한 불법적 제공, 기술적·관리적 보호조치의 이행 등에 대해 담당기관의 감독을 통해 사전에 예방하기 위한 수단을 강화하는 것이 요구된다. 현행법의 제도상에서는 개인정보파일 등록 의무대상과 개인정보 영향평가 대상을 확대 적용하는 방안이 검토될 수 있다.

1. 개인정보파일 등록의 의무

모바일서비스 제공자가 개인정보파일 등록의 의무와 개인정보 영향평가의 필수적 대상에서 제외된다는 사실은 많은 문제점을 나타낸다. 개인정보보호법 제32조에 따르면 공공기관은 운용하는 개인정보파일의 명칭, 운영 근거 및 목적, 기록되는 개인정보의 항목, 개인정보의 처리방법, 개인정보의 보유기간 등을 행정안전부에 등록하여야만 한다.²⁷⁵⁾ 즉, 개인정보보호법에서 공공기관은 정보처리자 가운데서도 별도의 의무를 지니는 특별한 관리의 대상이 되는 것이다.

반면 영국 개인정보보호법에 따르면 개인정보처리자는 국내 개인정보보호법의 개인정보파일에 해당하는 '등록 가능한 사항'(the registrable particulars)²⁷⁶⁾과 정보보호원칙 제7원칙²⁷⁷⁾을 따르기 위해 취해야 할 조치에 대한 전반적인 설명을 정보보호위원회에

장이다. 또한 실제로 제3자에 의해 해당 정보의 열람이 이루어졌는지 여부와 관계없이 언제든지 열람될 수 있는 상태에 놓이는 것만으로 유출(누출)이 발생한 것으로 본다. (서울중앙지법 2010. 9. 16. 선고 2008가합90021; 서울중앙지법 2009. 11. 6. 판결 2008가합75268, 2009가합91281(병합))

275) 개인정보보호법 제32조

276) 영국 개인정보보호법 제16조. 이에 따르면 등록 가능한 사항은 개인정보처리자의 이름과 주소, 개인정보처리자에 의해 또는 그를 대신해서 처리되고 있거나 처리되어야 하는 개인정보, 개인정보와 관련된 정보주체의 범주에 관한 설명, 데이터가 처리되고 있는 또는 처리되어야 하는 목적에 대한 설명, 개인정보처리자가 데이터를 공개하고자 의도하거나 의도할 수 있는 수령자나 수령자들에 대한 설명, 개인정보처리자가 데이터를 직접, 간접적으로 전송하거나 또는 전송할 의도가 있거나 희망하는 유럽경제지역 밖의 국가나 지역의 이름이나 설명, 개인정보처리자가 공공당국인 경우 그러한 사실에 대한 진술 등이 존재한다.

277) 영국 개인정보보호법 부칙 1, 제1장, 7. 이에 따르면 개인정보처리자는 권한 없는 또는 불법적인 개인정보의 처리와, 사고로 인한 개인정보의 손실이나 파괴, 손상에 대해

통보(notification)하고 있다.²⁷⁸⁾ 정보보호위원회는 개인정보처리자의 이러한 통보를 등록부(register)에 등재하여야 한다.²⁷⁹⁾ 정보처리자의 통보 의무와 관련하여, 영국 개인정보보호법 제18조 1항의 ‘등록부에 포함되기를 원하는 개인정보처리자’(data controller who wishes to be included in the register)라는 문구는 통보에 대한 법적 강제를 규정하고 있지 않은 것처럼 보인다. 그러나 동법 제17조 1항은 통보를 통한 등록부 등재가 이루어지지 않은 개인정보처리자로 하여금 개인정보의 처리를 금지하고 있으므로 사실상 모든 개인정보처리자는 정보보호위원회에 ‘등록 가능한 사항’을 통보하여야만 개인정보의 처리가 가능하다. 즉, 국내 개인정보보호법이 공공기관에 한하여 개인정보파일을 등록 및 공개하도록 규정한 반면, 영국의 개인정보보호법은 모든 개인정보처리자로 하여금 ‘등록 가능한 사항’을 통보하여 이러한 사항이 등록부에 등록되도록 규정하고 있다.

2. 개인정보 영향평가

개인정보보호법 제33조의 개인정보 영향평가에 따라 공공기관의 장은 정보주체의 개인정보 침해가 우려되는 경우에 그 위험요인의 분석과 개선 사항의 도출을 위하여 평가를 실시하여야 한다.²⁸⁰⁾ 개인정보 영향평가는 영국 개인정보보호법 제22조에 근거한 개인정보 예비평가(preliminary assessment)와 대비된다. 영국법에 따른 예비평가 또한 정보주체에게 중대한 손해 또는 심각한 고통을 초래할 가능성이 있거나²⁸¹⁾, 그 외에 정보주체의 권리와 자유를 심각하게 해칠 가능성이 있는 경우²⁸²⁾ 정보보호위원회는 이에 대한 평가를 실시하여야 한다.

그러나 국내 영향평가와 영국의 예비평가는 실효성 측면에서 많은 차이를 보인다. 개인정보 영향평가와 관련하여 관련주체의 현황을 살펴보면 다음과 같다.

여 적절한 기술적, 구조적 조치를 취해야 한다.

278) 영국 개인정보보호법 제18조(2).

279) 영국 개인정보보호법 제19조(1).

280) 개인정보보호법 제22조 제1항.

281) 영국 개인정보보호법 제22조(1)(a).

282) 영국 개인정보보호법 제22조(1)(b).

<표 4-10> 개인정보 영향평가 관련주체

대상 (영향평가 관련 주체)	고시의 주요 내용
행정안전부	영향평가기관의 지정 및 지정 취소
대상기관 (공공기관)	개인정보 영향평가 수행의 제반사항 (영향평가 기준, 절차, 방법)
개인정보 보호 관련 업체	평가기관 자격획득을 위한 제반 신청 사항 (영향평가기관 수행실적·수행인력·설비 등 증빙 및 확보, 평가기관 지정 신청)
평가기관	개인정보 영향평가 수행의 준수사항 (영향평가 기준·절차·방법, 보호대책 등 준수)
전문기관 (한국정보화진흥원)	평가기관 지정신청 접수 및 신고사항의 접수 사항

출처: 개인정보 영향평가에 관한 고시 및 해설서²⁸³⁾

<표 4-10>에서 나타나는 바와 같이 공공기관은 개인정보 영향평가의 대상기관이다. 실질적인 평가를 하는 평가기관은 행정안전부에 의하여 별도로 지정되도록 되어 있고, 평가기관 지정신청 접수 및 신고사항의 접수 사항은 한국정보화진흥원에서 담당하고 있다.

반면, 영국 개인정보보호법은 위에서 열거된 모든 업무를 정보보호위원회가 담당하도록 규정하고 있다.²⁸⁴⁾ 다시 말해, 영국법의 예비평가와 관련된 주체는 평가를 받는 정보처리자와 평가를 하는 정보보호위원회 둘 뿐이다. 이러한 차이는 행정의 효율성으로 직결된다. 개인정보 영향평가란 개인정보의 처리로 인하여 발생 가능한 정보주체의 권리 훼손을 방지하는 데 목적이 있다. 이러한 평가가 제대로 시행되기 위한 필수적 요건은 감독기관의 전문화된 역량이다. 그러나 복수의 담당기관이 권한을 위임받아 각자의 역할을 담당하도록 규정하고 있는 개인정보보호법의 규정은 전문화된 감독기관을 구성하는데 지장을 초래할 수 있다.

283) 개인정보 영향평가와 관련한 고시 및 해설서, 행정안전부 개인정보보호과, 2011, 2쪽.

284) 정보보호위원회는 평가기관이므로 행정안전부가 가지는 평가기관의 지정 업무 권한을 가지지 않는다.

평가의 대상이 공공기관에 한정되어 있다는 점도 문제이다. 영국 정보보호위원회는 개인정보처리자가 ‘등록 가능한 사항’을 통보하는 경우, 관련된 처리가 ‘평가 가능한 처리’(assessable processing)인지에 대한 여부를 판단하고,²⁸⁵⁾ 만약 평가 가능한 처리에 해당하면 그러한 처리가 영국 개인정보보호법 규정에 합치될 수 있는지에 대하여 평가하고 있다.²⁸⁶⁾ 이때, ‘평가 가능한 처리’란 정보주체에게 중대한 손해 또는 심각한 고통을 초래할 가능성²⁸⁷⁾, 그 외에 정보주체의 권리와 자유를 심각히 해칠 가능성이 명시적으로 설명된 처리를 의미한다.²⁸⁸⁾ 즉, 영국의 경우 모든 개인정보처리자가 자신이 처리하는 개인정보에 대한 제반 사항을 정보보호위원회에게 통보하면, 동 위원회는 이에 대한 예비평가를 하고 위반사항이 있는 경우 이에 대한 규제를 독자적으로 시행할 수 있는 것이다.²⁸⁹⁾

반면 개인정보보호법은 제32조에 따라 개인정보파일을 등록해야만 하는 의무를 공공기관에 한정하고 있다. 또한 동법 제33조 8항은 공공기관을 제외한 민간 개인정보처리자에게 영향평가에 대한 적극적인 참여를 유도하고 있을 뿐, 이를 의무사항으로 규정하고 있지 않다. 이러한 선언적 규정은 현실에서 실효성을 가지기가 어렵다.

3. 개인정보파일 등록 및 영향평가를 통한 모바일 개인정보의 보호

모바일 환경에서 이러한 문제점은 더욱 심각해질 수밖에 없다. 모바일기기의 이용이 급증함에 따라 모바일서비스를 이용하는 이용자의 수 또한 급증하였기 때문이다. 국내 안드로이드 마켓 최다 이용 모바일앱 현황에 따르면 카카오톡, GO런처EX, 폰꾸미기와 같은 프로그램은 안드로이드 마켓에서만 각각 천만 건, 5백만 건, 백만 건에 달하는 다운로드 수를 기록하고 있다.²⁹⁰⁾

285) 영국 개인정보보호법 제22조(2)(a).

286) 영국 개인정보보호법 제22조(2)(b).

287) 영국 개인정보보호법 제22조(1)(a).

288) 영국 개인정보보호법 제22조(1)(b).

289) Peter Carey, *Data Protection A Practical Guide to UK and EU Law* 3ed, Oxford University Press 2009, pp. 40-41.

290) 앱머썬 2011년 11월 2일 최종검색.

개인정보보호법시행령 제35조에 따라 개인정보영향평가의 대상이 되는 공공기관은 1) 5만 명 이상의 민감정보 또는 고유식별정보의 처리가 수반되는 개인정보파일, 2) 공공기관 내부 또는 외부에서 다른 개인정보파일과 연계 결과 50만 명 이상의 정보주체에 관한 개인정보가 포함되는 개인정보파일, 그리고 3) 100만 명 이상의 정보주체에 관한 개인정보파일을 구축·운용하고 있는 공공기관이다.²⁹¹⁾ 즉, 100만 명 이상의 개인정보를 처리하는 공공기관은 개인정보파일을 등록하고 개인정보 영향평가를 받아야 하는 반면, 100만 명이 넘는 개인정보를 처리하고 있는 상당수의 모바일서비스 제공자는 개인정보 파일에 대한 등록의무를 지니지 않고, 개인정보 영향평가의 의무적 대상에서도 배제되는 것이다.

구(舊) 「공공기관의 개인정보보호에 관한 법률」이 개인정보보호법의 제정과 함께 폐지되었음을 고려할 때, 개인정보보호법의 입법취지는 민간부문과 공공부문을 가리지 않는 통합적 규율을 통하여 개인정보에 대한 보호범위를 넓히는 데 있다. 따라서 수많은 개인정보를 처리하는 모바일서비스 제공자가 개인정보 영향평가의 대상에서 제외된다는 사실은 개인정보보호법의 입법 취지에 어긋난다. 이러한 맥락에서 현행 개인정보보호법은 영국법과 마찬가지로 개인정보파일 등록 및 개인정보영향평가의 대상을 모바일서비스 제공자를 포함한 민간 개인정보처리자로 확장하는 것이 바람직하다. 또한 개인정보 영향평가의 관련 주체를 축소하여 감독기관의 전문성을 제고할 필요성이 있다.

291) 개인정보보호법 시행령 제35조.

제5절 모바일서비스에 특화된 개인정보 취급방침의 정비

모바일 개인정보 취급방침은 자신의 개인정보가 어떻게 처리되는지, 언제 누구에게 어느 범위까지 처리되는지에 대하여 이용자가 한눈에 알아보고 수시로 확인 및 변경이 가능하도록 접근성이 제고되어야 한다. 이에 따라 현행법의 규정을 살펴보고, 개인정보 취급방침의 접근성과 실효성을 확보하기 위한 정책의 개선안을 살펴본다.

1. 정보통신망법의 문제점

정보통신망법 제27조의2 제1항은 정보통신서비스 제공자로 하여금 개인정보 취급방침을 정하여 이용자가 언제든지 쉽게 확인할 수 있도록 공개하여야 함을 규정하고 있다. 또한 개인정보보호법 제30조 제2항 역시 정보처리자가 개인정보 처리방침을 수립하거나 변경하는 경우 정보주체가 쉽게 확인할 수 있도록 그 내용을 공개하여야 함을 명시하고 있다. 이러한 공개의 방법은 대통령령에 의하여 규정되고 있으며 그 상세한 내용은 다음과 같다.

<표 4-11> 개인정보 취급(처리)방침의 공개 방법

정보통신망법시행령 제14조 제1항	개인정보보호법시행령 제34조 제2항
<p>법 제27조의2 제1항에 따라 정보통신서비스 제공자등은 개인정보의 수집 장소와 매체 등을 고려하여 다음 각 호 중 어느 하나 이상의 방법으로 개인정보 취급방침을 공개하되, 그 명칭을 '개인정보 취급방침'이라고 표시하여야 한다.</p> <ol style="list-style-type: none"> 1. 인터넷 홈페이지의 첫 화면 또는 첫 화면과의 연결화면을 통하여 법 제27조의2 제2항 각 호의 사항을 이용자가 볼 수 있도록 하는 방법. 이 경우 정보통신서비스 제공자등은 글자 크기, 색상 등을 활용하여 이용자가 개인정보 취급방침을 쉽게 확인할 수 있도록 표시하여야 한다. 2. 점포·사무소 안의 보기 쉬운 장소에 써 붙이거나 비치하여 열람하도록 하는 방법 3. 동일한 제호로 연 2회 이상 계속적으로 발행하여 이용자에게 배포하는 간행물·소식지·홍보지·청구서 등에 지속적으로 게재하는 방법 	<p>개인정보처리자는 법 제30조 제2항에 따라 개인정보 처리방침을 수립하거나 변경하는 경우에는 인터넷 홈페이지의 첫 화면 또는 첫 화면과의 연결화면을 통하여 공개하여야 하며, 인터넷 홈페이지를 통해 공개할 수 없는 경우 다음 각 호의 어느 하나 이상의 방법으로 개인정보 처리방침을 공개하여야 한다.</p> <ol style="list-style-type: none"> 1. 관보에 게재하는 방법 2. 동일한 제호로 연 2회 이상 계속적으로 발행하여 이용자에게 배포하는 간행물·소식지·홍보지·청구서 등에 지속적으로 게재하는 방법 3. 재화 또는 용역을 제공하기 위한 이용계약서 등에 게재하여 배포하는 방법

<표 4-11>에서 알 수 있듯이 정보통신망법시행령 제14조 1항에 따라 정보통신서비스 제공자는 개인정보 취급방침을 1호 내지 3호의 사항 가운데 선택적으로 제시할 수 있다. 반면 개인정보보호법시행령 제34조 2항은 인터넷 홈페이지를 통한 공개가 가능한 경우 이에 대한 우선적 공개를 의무화하고, 인터넷 홈페이지를 통한 공개가 불가능한 경우 1호 내지 3호의 방법을 통하여 처리방침을 공개하도록 하고 있다.

정보통신망법시행령은 이처럼 개인정보 취급방침의 공개 방법을 선택적으로 규정함에 따라 인터넷 브라우저 혹은 인터넷 연결을 통한 취급방침의 공개를 의무화하고 있지 않다. 이는 모바일서비스 제공자로 하여금 정보통신망법시행령 제14조 1항 2호 내지 3호에 명시된 방법을 통하여 모바일 인터넷 웹 브라우저를 통한 개인정보 취급방침의 공

개를 회피할 수 있는 가능성을 열어두고 있는 셈이다. 개인정보보호법을 적용하는 경우 이러한 문제를 방지할 수 있으나, 개인정보보호법 제6조에 따라 개인정보보호법은 정보통신망법의 특별한 규정이 없는 경우에만 적용이 되는 일반법의 지위를 가진다. 따라서 모바일서비스의 개인정보 취급방침의 공개에 대하여 개인정보보호법은 적용될 여지가 없다.²⁹²⁾

2. 개인정보 취급방침에 대한 이용자 접근성 확보

정보통신망법시행령에 따라 정보통신서비스 제공자가 인터넷 브라우저를 통하여 개인정보 취급방침을 공개할 경우, 글자 크기, 색상 등을 활용하여 이용자가 이를 한눈에 쉽게 확인할 수 있도록 표시하여야 한다.²⁹³⁾ 그러나 앞서 설문조사에서 살펴본 바와 같이 모바일 화면을 통하여 제시되는 개인정보 취급방침은 이러한 요건을 충족시키지 못하고 있다.²⁹⁴⁾

가. 개인정보 취급방침의 통일

통일된 방식으로 개인정보 취급방침을 이용자에게 제시하는 것은 중요한 문제이다. 각기 다른 개인정보 취급방침의 내용과 형식은 이용자로 하여금 이에 대한 이해를 더욱 어렵게 만들기 때문이다. 통일적이지 못한 개인정보 취급방침은 모바일서비스 제공자에게도 불리하게 작용한다. 악의를 가지고 개인정보보호를 위반하는 개인정보처리자는 드물기 때문이다. 정작 개인정보처리자가 안고 있는 가장 큰 고민은 자신의 개인정보 처리행위가 합법적 행위인지에 대한 법적 확신이 서지 않는다는 데 있다. 이러한 관점에서, 모바일앱 개발자를 대상으로 개인정보 취급방침에 대한 통일적인 제시방법을 유도하고 있는 미국 모바일 마케팅 협회(Mobile Marketing Association, 이하 MMA)의 개인정보 취급방침 가이드라인은 참고할 가치가 있다.²⁹⁵⁾

292) 개인정보보호법 제6조.

293) 정보통신망법 시행령 제14조 1항 1호.

294) 본문 53-56쪽 참조.

295) Mobile Application Privacy Policy Framework, MMA Privacy & Advocacy Committee, October 2011.

미국 MMA가 제시한 가이드라인은 모바일 앱 개발자가 이용자에게 제공하는 개인정보 취급방침에 대하여 구체적이고 통일적인 예시를 제시하고 있다. 동 가이드라인은 개인정보 수집항목, 이용자의 위치정보, 제3자에 대한 개인정보 제공 등 개인정보 취급방침에 제시되어야하는 항목들을 각각에 대한 모범예시를 통하여 제공하고 있다.²⁹⁶⁾ 이러한 모범예시를 개별 앱 개발자가 적용하는 경우, 각각의 개인정보 취급방침은 통일된 문체와 형식을 통하여 이용자에게 친숙한 방식으로 제공될 수 있다.

<표 4-12> 미국 MMA의 개인정보 취급방침 가이드라인의 예 (위치정보수집 부분)

Does the Application collect precise real time location information of the device?	
<IF No>	This Application does not collect precise information about the location of your mobile device.
<IF Yes>	This application does collect precise information about the location of your device. <INSERT A GENERAL DESCRIPTION OF HOW THIS IS DONE IN A WAY THAT IS CLEAR TO AN AVERAGE CONSUMER.> We use your location information to Provide requested location services, and <INSERT A LIST OF OTHER USES (E.G., TO ALLOW TAGGING, OR TO CHECK-IN) AND IF APPLICABLE, DESCRIBE THE CIRCUMSTANCES WHERE PRECISE LOCATION DATA IS SHARED WITH THIRD PARTIES FOR THEIR INDEPENDENT USE.>

출처: Mobile Application Privacy Policy Framework²⁹⁷⁾

<표 4-12>는 위치정보 항목에 대한 MMA의 가이드라인이다. 동 표에서 나타나는 바와 같이 동 가이드라인은 개인정보 취급방침에서 기본적으로 다루어지는 문구를 제시할 뿐만 아니라, 개별 프로그램에 따라 다르게 제시되는 항목이 삽입되는 자리 또한 세부적

296) *Ibid*, at 3-4.

297) Mobile Application Privacy Policy Framework, MMA Privacy & Advocacy Committee, October 2011. p. 4.

으로 지정하고 있다. 이에 따라 개별 서비스 프로그램에 따라 달라질 수 있는 서비스의 기능 및 기술적 특성과 상관없이, 모바일 개인정보 취급방침의 형식과 내용은 통일된 방식으로 이용자에게 공개될 수 있다.

설문조사에서 드러난 바와 같이, 대다수의 국내 이용자들 역시 이처럼 개인정보 취급 방침을 통일적으로 규율하는 가이드라인이 마련되길 바라고 있다.²⁹⁸⁾ 개별 서비스마다 다르게 제공되는 개인정보 취급방침의 형식이 통일되어 제공된다면, 이용자는 하나의 전달 방식에 익숙해질 수 있다. 이에 따라 이용자는 각각의 모바일서비스가 처리하는 개인정보 처리사항의 내용을 쉽게 이해할 수 있게 된다.

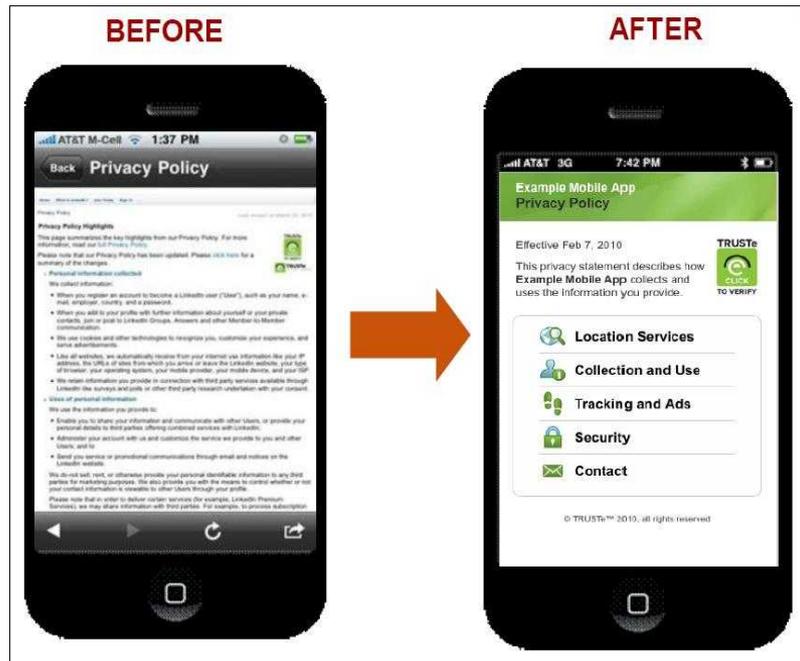
나. 까다롭고 복잡한 공개방식의 간소화

<설문 13>에서 나타난 바와 같이 전문적이고 기술적인 용어, 길고 복잡한 문체를 통한 개인정보 취급방침의 공개방식은 간소화될 필요성이 있다. 이와 관련하여 미국 연방거래위원회(Federal Trade Commission)는 개인정보 취급방침에서 제시되는 ‘길고 이해하기 어려운’(long and incomprehensible) 개인정보 취급방침이 이용자로 하여금 정작 중요한 개인정보 처리의 내용을 파악하는데 막대한 부담을 부여하고 있다고 언급한 바 있다.²⁹⁹⁾

298) 본문 69-70쪽 참조.

299) Federal Trade Commission, Protecting Consumer Privacy in an Era of Rapid Change, 2011, pp. 26-27.

<그림 4-2> 미국 TRUSTe에서 제공하는 모바일 개인정보취급 도안



출처: Harris Interactive³⁰⁰⁾

<그림 4-4>는 개인정보 취급방침의 접근성을 높이기 위한 도안의 예이다. 미국 TRUSTe는 모바일서비스 제공자의 개별적인 개인정보 취급방침을 이해하기 쉽고 간소화된 자사의 도안을 통하여 이용자에게 제공하고 있으며, 애플, 디즈니, eBay, HP, 마이크로소프트를 포함한 다수의 정보통신서비스 제공자들이 동 회사에서 제공하는 개인정보 취급방침 서비스를 통하여 개인정보 취급방침을 공개하고 있는 것으로 드러났다.³⁰¹⁾

정보통신망법시행령 제14조 1항 1호에 따라 이용자가 ‘쉽게 확인할 수 있는’ 개인정보 취급방침의 마련을 위하여, 방송통신위원회 등 감독기관은 모바일서비스 제공자로 하여금 이용자가 이해하기 쉬운 개인정보 취급방침을 마련할 수 있도록 노력하여야 한

300) Harris Interactive, Mobile Privacy: A User’s Perspective, p. 16.

301) http://www.truste.com/about_TRUSTe/press-room.html

다. 간소한 개인정보 취급방침의 내용은 통일된 개인정보 취급방침의 형식과 더불어 이
용자의 개인정보자기결정권을 확보하기 위한 중요한 요건이기 때문이다.

제6절 제3자 제공시 동의 방식/범위

개인정보의 제3자 제공에 대하여 개인정보보호법 등은 개인정보처리자에게 일정한 의무를 부과하고 있다. 그러나 모바일서비스에서는 과거에 비하여 보다 다양한 개인정보가 수집될 수 있고 또한 이러한 수집이 일회적인 것이 아니라 지속적으로 행해지게 된다. 즉, 모바일기기를 통하여 브라우징 기록, 위치정보, 이용하는 앱의 종류 등의 개인정보를 수집하고 이러한 정보의 지속적인 업데이트를 통해 보다 정확하고 최신의 개인 성향을 파악하는 것이 용이해졌다. 이에 따라 마케팅을 위해 이용자의 개인정보를 제3자에게 제공하거나 혹은 업무 위탁을 통해 처리하는 것이 급증하였다. 또한 메신저나 SNS 서비스를 제공하는 앱의 경우, 이용자가 보유하고 있는 제3자의 개인정보를 수집, 이용하여 서비스를 제공하는 경우가 많다. 카카오톡의 친구추천 기능이나 페이스북의 ‘알수도 있는 사람’ 기능이 이에 해당한다. 이와 같은 경우 자신의 전화번호, 이메일주소, 생일 등 기념일, 소속기관, 출신학교, 출신지역 등 서비스 이용자가 자신의 주소록에 저장할 가능성이 있는 다양한 신상정보에 대하여 정보주체가 이용을 통제할 수 있는 방법은 매우 제한적이다.

따라서 개인정보의 제3자 제공 또는 업무 위탁시 개인정보를 제공하는 자의 의무는 물론, 개인정보를 제공받는 자의 의무를 강화함으로써 정보주체를 더욱 강하게 보호하는 것이 요구된다.

1. 제3자로부터 개인정보를 제공받는 자의 의무 강화

개인정보보호법과 정보통신망법은 각각 개인정보의 제3자 제공시 개인정보처리자의 의무를 규정하고 있다. 개인정보보호법은 제17조에서 정보처리자의 개인정보 제3자 제공시 개인정보처리자의 의무를 규정하고 있다. 동조에 따르면 개인정보처리자는 수집한 개인정보의 제3자 제공시 정보주체의 동의를 받아야 하며 이 경우 동의를 획득과정에서 개인정보를 제공받는 자, 개인정보를 제공받는 자의 개인정보 이용 목적, 제공하는 개인정보의 항목, 개인정보를 제공받는 자의 개인정보 보유 및 이용 기간, 동의를 거부할 권

리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용을 정보주체에게 알려야만 한다.³⁰²⁾

정보통신망법 제24조의 2에 따르면 정보통신서비스 제공자가 이용자의 개인정보를 제3자에게 제공하기 위해서는 개인정보를 제공받는 자, 개인정보를 제공받는 자의 개인정보 이용 목적, 제공하는 개인정보의 항목, 개인정보를 제공받는 자의 개인정보 보유 및 이용 기간을 이용자에게 알리고 동의를 받아야 한다.³⁰³⁾

이와 같이 개인정보를 제3자에게 제공하는 경우 개인정보처리자는 제3자 제공의 사실과 제공받는 자, 제공받는 자의 이용 목적, 제공하는 개인정보의 항목, 보유 및 이용 기간을 이용자에게 알리고 동의를 받아야 하는 등 엄격한 의무를 부담하는 반면에, 개인정보를 제공받는 제3자는 매우 경한 의무만을 부담한다. 개인정보를 제공받는 자의 경우 개인정보보호법에서는 제20조에 따라 정보주체 이외의 자로부터 개인정보를 수집한 자에 대한 의무가 적용될 수 있는데, 동조는 정보주체의 요구가 있는 경우에 한하여 개인정보의 수집 출처, 개인정보의 처리 목적, 개인정보 처리의 정지를 요구할 수 있는 권리가 있다는 사실을 고지할 의무만을 부담한다. 정보통신망법상에서는 제24조의 2 제2항에 의해 단지 정보주체의 동의 또는 법률의 특별한 규정 없이 개인정보를 제3자에게 제공하거나 제공받은 목적 외의 용도로 활용하여서는 안된다고 규정할 뿐이다.

그러나 모바일서비스의 경우 제3자 제공에 대한 동의 역시 이용자가 인지하지 못하거나, 개인정보를 제공받는 제3자의 범위나 제공되는 개인정보의 범위가 지나치게 광범위할 수 있는 등 앞에서 검토한 개인정보 수집에 대한 동의 방식의 문제점이 동일하게 적

302) 제17조 제1항에 따라 정보처리자는 정보주체의 동의가 없어도 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우(제15조 제1항 제2호), 공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우(제3호), 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우(제5호)에는 개인정보를 제3자에게 제공할 수 있다.

303) 동조 예외규정에 따라 정보통신서비스의 제공에 따른 요금정산을 위하여 필요한 경우(제22조 제2항 제2호), 정보통신망법 또는 다른 법률에 특별한 규정이 있는 경우(제22조 제2항 제3호)에 정보통신서비스 제공자는 개인정보를 제3자에게 제공할 수 있다.

용될 수 있다. 무엇보다 모바일앱에서의 개인정보 수집과 제3자 제공에 대한 동의가 정보 수집이 행해지거나 제공이 이루어질 때마다 반복적으로 이루어지는 것이 아니라 최초 서비스 가입시에만 포괄적으로 이루어진다는 점에서 지속적인 침해가 일어날 수 있다. 또한 개인정보 제3자 제공에 대하여 정보주체가 동의를 하였다고 하더라도, 많은 경우 해당 정보는 동의를 한 즉시 제공되는 것이 아니라 마케팅 목적 등으로 장래의 불특정 시점에 제공되기 때문에 제공 시점에는 정보주체가 이를 알지 못하는 경우가 발생한다.

따라서 개인정보의 제3자 제공이 이루어지는 시점에 정보주체가 그 사실을 인지할 수 있도록 하는 방안이 마련되어야 한다. 이에 대해서는 EU 및 영국의 개인정보보호법제를 참고할만하다. EU개인정보보호지침 제11조는 개인정보를 정보주체가 아닌 제3자로부터 수집하는 경우에도 정보주체가 개인정보처리자의 신원, 개인정보의 사용 목적, 공정한 처리 보장을 위한 추가적 정보를 제공받을 것을 규정한다.³⁰⁴⁾ 영국 개인정보보호법의

304) EU 개인정보보호지침 제11조는 다음과 같다.

1. Where the data have not been obtained from the data subject, Member States shall provide that the controller or his representative must at the time of undertaking the recording of personal data or if a disclosure to a third party is envisaged, no later than the time when the data are first disclosed provide the data subject with at least the following information, except where he already has it:
 - (a) the identity of the controller and of his representative, if any;
 - (b) the purposes of the processing;
 - (c) any further information such as
 - the categories of data concerned,
 - the recipients or categories of recipients,
 - the existence of the right of access to and the right to rectify the data concerning him,
 in so far as such further information is necessary, having regard to the specific circumstances in which the data are processed, to guarantee fair processing in respect of the data subject.
- (1. 개인정보가 개인정보주체로부터 획득되지 않은 경우, 회원국들은 개인정보처리자 또는 그의 대리인이 개인정보를 기록하는 시점에서 또는 제3자에 대한 공개가 예정된 경우 개인정보가 최초로 공개되는 시점보다 늦지 않게 정보주체에게 적어도 다음의 정보를 제공할 것을 규정해야 한다. 단, 정보주체가 이를 이미 가지고 있는 경우는 예외로 한

경우 정보주체 이외로부터 개인정보가 취득되는 경우, 관련 시점³⁰⁵⁾ 전이나 그 이후 가능한 가장 빠른 시점에 정보주체가 개인정보처리자 또는 그 대리인의 신원, 개인정보 처리의 목적, 개별 상황에 따라 정보주체에 대한 처리가 공정할 것을 보장하기 위한 추가적 정보를 제공받거나, 즉시 입수할 수 있도록 할 것을 개인정보처리자가 최대한 보장하지 않으면 불공정한 처리가 됨을 규정하고 있다.³⁰⁶⁾ 즉, 우리 법제와는 달리 EU와 영국의 경우 제3자로부터 개인정보를 수집한 경우 정보를 제공받은 제3자인 개인정보처리자가 정보주체에게 그 사실을 알리도록 하고 있다. 단, EU개인정보보호지침의 경우, 제3자 제공에 대한 사실과 제공 항목들을 정보주체가 이미 알고 있는 경우에는 당해 의무를 면제할 수 있도록 하였다는 점에서 정보주체의 요구가 있을 때에만 해당 정보를 제공하도록 규정한 우리 법제와 결과적으로 큰 차이는 없을 것으로 보인다. 영국 개인정보보호법은 이러한 예외를 규정하고 있지 않아 EU개인정보보호지침보다 한층 강화된 보호를 부여하는 것으로 보인다. 그러나 다수가 이용하는 카카오톡과 같은 메신저 앱에서 주소록에 저장된 정보를 이용한 친구추천 기능과 같은 경우, 개별 사안마다 정보주체에게 적극적으로 알린다는 것은 매우 비현실적이다. 영국 개인정보보호법은 관련 항목의 제공 의무를 실현가능한 가장 빠른 시점에, 제공되거나 즉시 입수될 수 있도록 노력하게 하고 있어 해석상 융통성을 인정할 여지를 남겨두고 있다.

개인정보의 제3자 제공의 문제는 모바일서비스가 활성화되기 이전부터 많은 논란이

다.

(a) 개인정보처리자의 신원 및 대리인이 있는 경우 그의 신원

(b) 처리의 목적

(c) 개인정보가 처리되는 특정의 상황을 고려하여, 추가적 정보가 정보주체에 관해 공정한 처리를 보장하는 데 필요한 범위에서

- 관련 데이터의 범주,

- 수령인 또는 그의 범주,

- 정보주체에 관한 개인정보에 대한 접근의 권리와 수정의 권리의 존재)

305) “관련 시점”이란 개인정보처리자가 최초로 해당 개인정보를 처리한 시점, 또는 개인정보의 제3자 공개가 예정된 경우 실제로 공개되는 시점이나 실제 공개가 이루어지지 않더라도 개인정보처리자가 공개되지 않음을 인지하게되는 시점을 의미한다.(영국 개인정보보호법 제1부칙 제2부 2(2))

306) 영국 개인정보보호법 제1부칙 제2부 2항.

되어 왔다. 하나로통신 개인정보 유출 사건³⁰⁷⁾의 경우와 같이 개인정보 취급방침 또는 이용약관의 사후 개정에 따라 개인정보의 제3자 제공이 이루어지거나 명확하지 않은 제공 목적과 제공 대상, 이용범위를 명시한 동의에 기초해 제3자 제공이 이루어지는 경우, 제공받은 자가 실제로 개인정보를 이용 또는 다시 제3자에게 제공하여 이용됨으로써 실제 피해가 발생하기 전까지는 정보주체가 언제 누구에게 자신의 개인정보가 제공되었는지를 인지하기는 불가능하다. 그러므로 정보주체의 요구가 있을 경우에 한하여 정보주체에게 수집출처와 처리목적 등을 고지하도록 한 개인정보보호법 제20조는 실효성이 없다. 개인정보를 제공받은 자의 고지의무를 전혀 규정하고 있지 아니한 정보통신망법도 물론이다. 따라서 제3자로부터 개인정보를 제공받는 개인정보처리자로 하여금 원래 이루어졌던 동의에 따라 실제 정보 제공이 이루어졌음을 통지하도록 하는 의무를 부과하는 것이 개인정보 누설로 인한 피해를 사전에 차단하기 위한 방안으로 제시된다.

이와 같은 의무를 추가하는 것은 개별 사업자에게는 일견 과중한 부담을 지우는 것으로 보일 수 있을 것이다. 그러나 이용자들은 이러한 정보의 제공에 대하여 자신이 인지하지 못한다는 점에 대해 불안함과 불쾌감을 가지고 있으며, 이를 해소하는 것은 결과적으로 서비스제공자의 사업에도 플러스 요인이 될 것이다. 따라서 정보통신망법과 개인정보보호법상 정보주체 이외로부터 정보를 수집하는 경우, 정보주체의 요구 여부와 무관하게 수집 사실을 고지하도록 해당 규정을 개정함이 바람직하다.

307) 서울중앙지법 2011. 1. 27. 2010노2850, 서울중앙지법 2010. 7. 15. 2009고단1864. 동 사건에서 SK브로드밴드(변경 전 상호 하나로통신)는 자사가 보유하고 있는 고객정보의 데이터베이스에 대하여 마케팅을 위한 업무위탁계약을 체결한 마케팅대행사에 접근권한을 부여하여 업무협약을 체결한 한국스탠다드차트제일은행의 카드를 홍보하도록 하고, 마케팅 대행사는 고객의 개인정보를 동 은행에 제공하였다. 법원은 이와 같은 이용 및 제3자 제공은 가입계약 체결 당시 개인정보의 수집, 이용에 대한 동의의 내용에 포함된다고 보기 어려우며, 피고인 회사가 향후 인터넷 홈페이지를 통해 개인정보 취급방침상 활용목적에 하나포스멤버스카드 소개 항목을 추가하고 위탁업체를 명시한 것만으로는 정보통신망법 제22조 제1항에 따라 변경사항을 이용자에게 알리고 동의를 받은 것으로 볼 수 없으며, 따라서 이와 같은 행위는 고객이 예상한 범위를 벗어난 것으로서 위법한 행위라고 판단하였다.

2. 위치기반서비스의 약관동의방식의 개선

위치기반서비스사업은 위치정보사업자로부터 위치정보를 제공받는 것을 전제로 하고 있다. 따라서 위치기반서비스를 위해 개인정보의 제3자 제공은 필수적이다. 위치정보법은 제15조에서 위치정보사업자가 위치정보의 수집, 이용, 제공시 개인 또는 이동성 있는 물건의 소유자에게 동의를 얻을 의무와 위치정보의 보호를 위한 기술적·관리적 조치를 취할 의무를 부과하고 있다. 구체적으로 제18조에서는 위치정보사업자의 상호, 주소, 전화번호 그 밖의 연락처, 개인위치정보주체의 권리와 그 행사방법, 위치기반서비스사업자에게 제공하고자 하는 서비스의 내용, 위치정보 수집사실 확인자료의 보유근거 및 보유기간 등을 약관에 명시하여 동 약관에 대한 동의를 획득할 것을 규정하고 있다.

위치정보법의 경우 개인정보보호법이나 정보통신망법과 달리 개인정보를 제공받는 자, 즉 위치기반서비스사업자가 위치정보사업자로부터 위치정보를 제공받고자 하는 경우 사전에 약관을 통해 자신의 상호, 주소, 전화번호 등 연락처, 개인위치정보주체 및 법정대리인의 권리와 그 행사방법, 제공하고자 하는 서비스의 내용, 위치정보 이용·제공사실 확인자료의 보유근거 및 보유기간, 그 밖에 개인위치정보의 보호를 위하여 필요한 사항을 명시하고 이에 대한 동의를 획득할 것을 규정하고 있다.³⁰⁸⁾ 나아가 위치기반서비스사업자가 개인위치정보를 정보주체가 지정하는 제3자에게 제공하고자 하는 경우 위의 약관에 대한 동의와 더불어 제공받는 자와 제공목적은 고지하고 별도의 동의를 얻도록 하고 있으며, 이에 따라 위치정보가 제공될 때마다 즉시 정보주체에게 제공받는 자와 제공일시, 제공목적은 통보하도록 규정한다.³⁰⁹⁾ 이는 정보주체의 보호 측면에서 개인정보보호법이나 정보통신망법의 규정보다 진일보한 규정이라 할 수 있다.

308) 위치정보법 제19조 제1항.

309) 위치정보법 제19조 제2, 3항.

제5장 결 론

현대사회에서 기술의 급격한 발전은 과거에 예상하지 못했던 새로운 법적 문제점을 발생시킨다. 이러한 문제점들은 일반적으로 기술의 발전 속도를 법이 따라가지 못함으로써 나타난다. 여기에는 기술발전에 따른 사회적 인식의 변화로 인하여 새로운 내용의 개인적 권리가 인정됨에도 불구하고 이를 법적으로 보호하지 못하는 경우와, 법의 자체는 기존의 법체계 내에서 보호되나 침해 방법의 신규성으로 인해 침해행위를 기존의 법에 포섭시키지 못하는 경우, 혹은 침해가 용이해지거나 인지가 어려워져 집행상의 어려움이 발생하는 경우, 그리고 문제 자체를 입법부나 사법부가 이해하지 못하여 법규 포섭 여부를 판단하기 어려운 경우가 있다. 우리 헌법재판소가 2005년에 들어서야 개인정보자기결정권을 헌법상의 기본권으로 인정하고, 이보다 앞서 개인정보보호법제 자체가 1970년대 유럽에서의 컴퓨터 활용의 증대에 따른 프라이버시 침해가능성이 부각되면서 발전했던 연혁을 살필 때 개인정보보호의 문제는 이 중 첫 번째 경우에 해당된다 할 수 있을 것이다. 모바일서비스에서 개인정보보호의 문제는 이렇게 인정된 개인정보자기결정권을 현행 개인정보보호법과 정보통신망법, 위치정보법 등 기존의 법체계에서 침해행위를 포섭하지 못하거나 대규모 집행결손이 발생하여 제대로 보호하지 못할 가능성이 있다는 점에서 제기되는 것으로 볼 수 있다. 즉, 모바일서비스에서의 개인정보보호 문제의 해결은 이미 확립되어 있는 개인정보주체의 권리가 모바일 기술의 발전으로 어떻게 영향을 받는지를 검토하고 이를 효과적으로 보호하기 위한 입법적 방안을 찾는 방향으로 모색되었다.

모바일서비스와 관련된 기술발전은 스마트폰이나 태블릿 PC 등 스마트 모바일기기 하드웨어적 발전과, 여기에 설치되는 응용프로그램의 발전, 그리고 이를 통해 개인정보를 수집하고 처리하는 기술상의 발전을 의미한다. 즉, 하드웨어의 발전에 따라 데이터 처리능력과 통신기능, 기타 멀티미디어 기능 및 호환성이 비약적으로 증대하였고, 무엇보다 기존에 PC를 이용하던 것과 같이 다양한 애플리케이션 프로그램들을 설치하여 이용하게 됨으로써 개별 이용자에게 모바일기기의 의미가 단순히 자유로운 통화를 가능하

게 해주는 것으로부터 사적 영역과 공적 업무상 영역을 모두 포괄하여 정보를 저장, 처리하고 통신하는 주요 수단으로서 자리매김하였다. 또한 서비스제공자의 입장에서는 모바일 애플리케이션을 통하여 모바일기기에 저장된 정보나 기기로부터 직접 생성된 정보를 이용하여 이용자의 취향에 맞는 정보를 제공함으로써 마케팅 효과를 높이거나, 개인에 대해 매우 포괄적인 정보를 데이터베이스화하여 사업개발에 활용하는 등 행태정보를 이용한 영업수단을 확보하게 되었다. 그러나 이용자의 동의 또는 인지 여부와 무관하게 무한정에 가까운 개인정보를 추출해내고 이를 바탕으로 새로운 개인정보를 생성해낼 수 있다는 점은 모바일서비스에서 제기되는 특수한 문제점으로 꼽혔다. 실제로 수집목적의 적법성 이외의 아무런 요건을 부과하지 않고 있는 우리 법 아래서는 대체로 개인정보처리자가 스스로 광범위한 개인정보 수집목적 설정하고 이에 따라 자신이 원하는, 정보주체의 성향과 라이프스타일을 모두 파악할 수 있는 다양한 정보를 수집하고 있는 것이 현실이다. 이에 더해 개인정보보호법제가 비교적 새로운 법분야로서 법체계 및 집행권한의 배분이 아직 정비되지 못하여 이용자는 물론 개인정보를 활용하고자 하는 사업자에게도 혼란을 주고 있으며, 새로운 수단이 등장할 때마다 이러한 혼란이 가중되고 있다는 점도 문제되었다.

구체적으로는 첫째, 모바일기기를 통한 개인정보 수집에 있어 보호의 대상이 되는 개인정보의 범위가 개별 법률별로 상이하게 규정되어 있으며, 이들 정의들이 어떤 정보가 개인정보에 해당하는지에 대해 명쾌히 답을 주지 못한다는 문제가 드러났다. 즉, 정보주체는 자신이 제공하거나 자신의 기기로부터 수집되는 정보가 개인정보에 해당한다는 사실을 알지 못함으로써 자신의 정당한 권리를 행사하지 못하거나, 개인정보처리자는 수집하는 개인정보에 대해 개인정보 처리에 관한 원칙을 준수하지 않고 처리함으로써 의도하지 않게 불법을 저지르게 되는 경우가 발생하는 것이다. 모바일서비스 제공시 수집되는 정보가 항상 개인정보가 되는 것은 아니기 때문에 결국 개별 사안에 따라 검토될 수밖에 없으나, 이에 대해서는 감독기관의 일관된 판단 사례의 누적을 통한 가이드라인이 제시될 필요가 있고 가능한 범위에서 법원의 판단기준이 될 수 있는, 구속력을 가진 명령 형태의 지침을 통한 구체화가 요구된다.

둘째, 이용자가 자신의 권리를 실질적으로 행사하기 위한 제도적 보완의 필요성이 제

기되었다. 즉, 기술적으로 프로그램의 설치와 구동만으로도 모바일기기로부터의 정보 수집, 전송이 가능하며, 경우에 따라서는 특정 프로그램이 설치되어 있는지조차 이용자가 인지하지 못한다는 점에서 개인정보 수집/이용 등 처리에 관해 이용자가 충분히 이해하고 이에 대한 동의 획득 요건을 강화해야 할 필요성이 제기된다. 여기에는 현행법상의 동의 획득 절차를 강화함으로써 이용자의 실질적 결정권을 확보하는 방안과, 의도된 정보 처리에 대해 이용자의 알 권리를 보장하기 위해 개인정보취급방침을 사전에 제공받도록 하는 권리를 보충하는 방안, 효과적인 선택적 동의제도의 시행방안 등이 포함되었다. 동의 획득에 관한 문제는 개인정보자기결정권의 본질적 부분을 구성하는 것으로 설문조사 결과 이용자들이 가장 크게 불만을 가지고 있는 부분인데, 동의 획득 여부와 동의 획득의 시점에 대해서도 실질적 결정권을 행사하지 못하고 있는 것으로 나타났으며 동의 절차를 거치는 경우에도 형식적, 강압적 절차에 불과하다고 인식하는 이용자가 많았다. 또한 개인정보를 이용한 마케팅이 점차 사업을 위해 필수적인 것으로 인식되어가고 있으며, SNS나 위치정보서비스의 활성화에 따라 개인정보의 제3자 제공이 빈번해지는 현실에서 행태정보, 위치정보 등 제3자 제공시 이에 대한 정보와 정보주체의 권리의 고지를 현실화해야 할 필요성이 제기된다. 이에 대해서는 위치정보법의 규정을 참고하여 개인정보보호법과 정보통신망법에 개인정보를 제공하는 제3자의 고지의무를 강화하는 방안을 제시하였다. 이러한 접근은 유럽에서의 입법적 시도와 미국에서의 민간사업자단체에 의한 자율적 규제에서 공통적으로 발견되는 부분으로, 초기 사업자들의 강한 반발과는 달리 개인정보 처리 및 제공에 대한 투명성 확보가 장기적으로 이용자의 신뢰 확보에 기여함으로써 오히려 사업의 효율성을 증진시킬 수 있다는 공감대 형성에 따른 것이다. 정보주체의 권리 보호와 사업자의 서비스제공 효율성 사이의 균형을 모색하고자 하는 정책당국의 입장에서는 이를 참고할만할 것이다.

셋째, 개인정보 무단수집, 무단제공, 유출 등 침해 발생을 사전에 차단하기 위한 예방적 조치의 미흡 역시 문제로 제기되었다. 개인정보 침해의 경우 사후 원상회복이 거의 불가능하다는 점에서 여타 범죄 등 권리침해 행위보다 예방적 조치가 더욱 강하게 요구된다. 또한 정보주체는 물론 수사기관이나 감독당국 역시 유출 등 사고가 실제로 일어나 피해가 발생하기 전까지는 이러한 사실에 대해 사전에 인지하기가 매우 어려운 현실

이다. 따라서 영국 개인정보보호법의 제도를 참고하여 개인정보보호법상 일정규모 이상의 개인정보를 처리하는 공공기관에 한해 의무화하고 있는 개인정보영향평가의 대상을 민간 부문에 확대하고, 약관규제법상 표준약관의 등록의무와 같이 처리하는 개인정보파일의 등록의무를 부과하는 방안도 적극 검토될 필요가 있다.

마지막으로 통합적 규율을 위한 개인정보보호법이 제정, 발효되었음에도 불구하고 정보통신망법, 위치정보법, 신용정보법 등의 특별법과, 의료법, 교육법 등 각 개별 법률에 산재되어 있는 특별법적 규정들로 인하여 적용법과 담당기관이 파편화되어 있다는 문제가 있다. 특히 정보통신망법과 개인정보보호법은 대상과 내용에 있어 중복되는 내용이 지나치게 많으며, 동일 내지 유사한 의무에 대해 주무기관이 행정안전부와 방송통신위원회로 이분화되어 있다는 점은 입법론상 매우 바람직하지 못하다. 온라인, 오프라인 중심의 사업자를 막론하고 대부분의 사업자가 모바일서비스를 비롯해 온라인서비스를 제공하고 있으며, 오프라인으로 수집한 개인정보와 온라인으로 수집한 개인정보가 혼재된 데이터베이스를 통해 고객정보를 관리하고 있다는 점에서 이러한 구분은 무의미할 뿐 아니라 혼란만 가중시키는 역할을 한다. 예컨대 오프라인에서의 판매사업과 홈페이지 및 모바일 앱을 통한 고객관리를 함께 수행하는 자동차회사가 양자에서 수집한 개인정보를 종합하여 하나의 데이터베이스를 보유하는 경우, 이 회사에 대한 개인정보 감독기관은 어디라도 될 수 있는 것이다. 따라서 법률의 구조적 정비를 통해 이렇게 파편화된 적용법과 감독기관을 일원화하는 것이 개인정보보호의 효율성에 기여하는 방안이 될 것이다.

모바일서비스의 개인정보보호 문제는 대개의 신종 범죄와 같이 완전히 새로운 문제라기보다는 기존의 문제점이 기술환경의 변화에 따라 더욱 심화되는 양상을 보인다. 예컨대, 보이스피싱이 형법상 사기죄의 새로운 수단에 불과한 것과 같이 모바일서비스를 통한 개인정보 침해 문제도 모바일 애플리케이션, 모바일기기라는 새로운 수단의 등장으로 인한 문제이며, 개인정보보호의 문제라는 본질적인 부분에서는 차이가 없는 것이다. 이는 또한 사이버 범죄가 최초 등장했을 당시와는 달리 일반범죄와 사이버범죄를 동일 선상에서 보아야 한다는 온-오프라인 동등의 원칙과도 흐름을 같이 하는 것이다. 따라서 모바일서비스의 개인정보보호 문제를 접근하는 기본적인 틀은 가능한 일원화된 규

범의 체제 내에 효과적으로 사안을 포섭할 수 있는 제도들을 구체화하는 것을 원칙으로 접근해야 할 것이다.

참 고 문 헌

국내 문헌

- 국가인권위원회 보도자료, “인권위, 기업의 강제적 개인정보 수집 관련 일체 점검 및 가이드라인 제정 권고”, (2011. 10)
- 금주환, “일반적 평등원칙의 해석과 적용”, 법조 49권 12호, (2000).
- 김범수, “미국의 개인정보 유출 통지 제도의 현황과 시사점”, 人@Internet 2009년 9·10월, 한국인터넷진흥원, (2009. 10).
- 김민서, “한국 경쟁법의 역외적용과 국제법적 평가”, 『국제법학회논총』, 제51권 제3호 (통권 제106호), (2006. 12).
- 노영돈, “국내경제법의 역외적용과 국가관할권의 충돌에 관한 연구-경쟁법을 중심으로”, 『국제법학회논총』, 제47권 제1호(통권 제92호), (2002. 4).
- 박노형, “다국적기업의 거래상의 지위남용 행위에 대한 연구”, 공정거래위원회 (1997).
- 박인회, “스마트폰과 관련된 법적문제에 관한 소고”, 『월간 법제』, 법제처, (2011. 6).
- 박정훈, “우리나라 개인정보보호법제상의 추적가능 시스템에 관한 연구”, 『토지공법연구』 제52집, (2011. 2).
- 박정현, “스마트폰 시대의 모바일 마케팅”, 『마케팅』, 한국마케팅연구원, 제45권 제1호 (2011.1).
- 방송통신위원회 보도자료, “스마트폰 가입자 1,000만 돌파, 스마트 시대 본격 개막”, (2011.3.24).
- 방송통신위원회 보도자료, “애플 및 구글의 위치정보보호 법규 위반행위에 대해 시정요구 및 과태료 부과처분 공표”, (2011.8.3).
- 방송통신위원회, “LBS 산업육성 및 사회안전망 고도화를 위한 위치정보 이용 활성화 계획(안)”, (2010. 6).
- 방송통신위원회, “Smart Korea 강국 도약을 위한 스마트 모바일 시큐리티 종합계획”, (2010. 12).
- 방송통신위원회, “정보통신서비스 제공자를 위한 개인정보보호 가이드”, (2011. 1).

- 배종대, 형법총론(제8전정판), 홍문사, (2007).
- 소병천, “국내법의 역외적용에 관한 미국의 관행”, 『국제법학회논총』, 제49권 제3호(통권 제100호), (2004. 12).
- 윤중서, “인터넷 산업에 대한 법적 규제 및 활성화 방안”, 『저스티스』 통권 제121호 (2010. 12).
- 이상돈, 기초법학, 제2판, (2010).
- 이종관, “스마트폰의 고유 속성에 따른 법적 쟁점과 과제”, 『법연』, (2011. 7).
- 한국 인터넷진흥원, “2011년 상반기 스마트폰이용실태조사”, (2011. 7).
- 한국정보통신진흥협회, “이용자 관점의 스마트폰 이용실태분석 및 사후규제방안 연구”, (2010. 12).

해외 문헌

- Amir Efrati et al, “Mobile-App Makers Face U.S. Privacy Investigation”, Wall Street Journal, (5 Apr 2011).
- Association of National Advertisers, 『Vast Majority of Marketers will Utilize Mobile Marketing and Increase Spending on Mobile Platforms in 2011』, (2011. 1).
- Chris Lefkow, “US senators unveil mobile privacy, data theft bills”, AFP, (15 Jun 2011).
- Coda Research Consultancy, 『Worldwide Smartphone Sales Forecast to 2015』, (2010. 5).
- Eric Chabrow, "Rockefeller Submits Do Not Track Online Act", 『Government Information Security Articles』, (May 9, 2011).
- European Commission Com(2010)609 Final, Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, "A Comprehensive approach on Personal Data Protection in the European Union", (2010. 4).

- Federal Trade Commission, "Protecting Consumer Privacy in an Era of Rapid Change", (2011).
- Harris Interactive, "Mobile Privacy: A User's Perspective", (2010. 4).
- Information Commissioner's Office, "Data Protection Technical Guidance: Determining what is personal data", (2007. 8).
- James Crawford, 『The Creation of States in International Law』 , Oxford, Clarendon Press, (1979).
- Jemima Kiss, "South Korea fines Apple over location data blunder", UK Guardian, (2011. 10).
- Malcolm Shaw, 『International Law』 , Cambridge University Press, (2008).
- MMA Privacy & Advocacy Committee, "Mobile Application Privacy Policy Framework", (2011. 10).
- Monica Desai, Greg Louer, Ryan King, Maria Wolvin, "LBS Marketing—Why Federal Government Cares and What You Can Do About It", 『Mobile Marketing Association Working Paper』 , (2011).
- Peter Carey, Data Protection A Practical Guide to UK and EU Law 3ed, Oxford University Press, (2009).
- Richard Thomas, Information Commissioner, "Speech to RSA Conference Europe on data breaches", (2008. 10).
- Ryan Moshell, "And There Was One: The Outlook for a Self-Regulatory United States Amidst a Global Trend Toward Comprehensive Data Protection", 37 Tex. Tech. L. Rev. 357.
- Scott Thrum et al, 『Your Apps Are Watching You』 , (2011. 10).
- Strategy Analytics, "Cellphone Privacy Concerns Only a Short Term Barrier to \$10 Billion Location-Based Opportunity", (2011. 6).
- UK Information Commissioner, "Privacy & Law Enforcement, Technology development and its effect on privacy & law enforcement", UK Information Commissioner Study Project, (2004).

01248/07/EN WP 136, Opinion 4/2007 on the concept of personal data.

881/11/EN WP185, Opinion 13/2011 on Geolocation services on smart mobile device.

기사

- 경향신문, "이통사 위치추적 '불법장사' 정통부선 알고도 묵인", 2007. 2. 5.
- 동아일보, "'위치정보 수집 해명하라' 각국, 애플에 요구 확산", 2011. 4. 26.
- 매일경제, "아이폰 위치정보 수집 불법성 논란", 2011. 7. 26.
- 매일경제, "'아이폰 위치추적' 2만7천명 집단소송", 2011. 8. 17.
- 머니투데이, "SK컴즈, 개인정보수집 시도 '해프닝으로 끝나'", 2010. 7. 28.
- 아이뉴스, "방통위, 유튜브 행정조치 '안 하기로'", 2009. 4. 10.
- 아이뉴스, "세계 모바일 기기 56억대... 전년 비 11% up", 2011. 8. 5.
- 아이뉴스 "토종 앱 장터 T스토어 "잘 자랐네", 2011. 9. 8.
- 연합뉴스, "스마트폰 앱 1,400개 뿌려 80만명 위치정보 수집", 2011. 4. 11.
- 연합뉴스, "아이폰 위치추적 집단소송 1인당 100만원씩 청구", 2011. 7. 14.
- 연합뉴스, "일본 구글, 개인 캘린더 정보 유출 논란", 2009. 2. 13.
- 전자신문, "이메일 안주면 카카오톡 못쓴다 이상한 약관강요 논란", 2011. 9. 9.
- 중앙일보, "스마트폰 이용해 80만명 위치정보 무단수집", 2011. 4. 20.
- 한겨레신문, "인터넷실명제 유튜브 제외 '역차별' 논란", 2010. 4. 7.
- 한국경제, '카카오톡이 고압적인 개인정보수집에 나선 까닭', 2011. 9. 18.
- 한국일보, "80만명 위치정보 무단수집해 광고 이용한 업체 적발", 2011. 4. 27.
- YTN, "이통3사, '위치추적' 통보 무시 불법영업", 2007. 2. 4.

판례

- 대법원 2008. 10. 23. 2008도5526.
- 서울중앙지법 2007. 2. 8. 2006가합33062.
- 서울중앙지법 2008. 6. 12. 2008노1198.

서울중앙지법 2009. 11. 6. 2008가합75268, 2009가합91281(병합)

서울중앙지법 2010. 7. 15. 2009고단1864.

서울중앙지법 2010. 9. 16. 2008가합90021.

서울중앙지법 2011. 1. 27. 2010노2850.

헌재 1995. 9. 28. 93헌마50.

헌재 2005. 5. 26. 99헌마513, 2004헌마190(병합)

British Gas Trading Ltd. v. Data Prot. Reg., <1997/98> 1 Info. T.L.R. 393.

Timberlane Lumber Co. v. Bank of America, 549 F.2d 597(9th Circuit 1976), on appeal following remand, 749 F.2d 1378(9th Circuit 1979).

모바일 개인정보보호에 대한 이용자 인식도 조사

본 설문조사의 결과는 방송통신위원회의 주관으로 고려대학교 산학협력단이 수행하는 “모바일 서비스의 개인정보 활용 행태 및 보호방안 연구”의 기초자료의 목적으로만 사용됩니다.

(설문 1) 얼마나 많은 모바일 앱 서비스를 다운받아 이용하고 계십니까?

- ① 없다 ② 1-4개 ③ 5-8개 ④ 8-12개 ⑤ 13개 이상

(설문 2) 현재 스마트폰 등을 통한 위치정보 이용 및 모바일 앱 서비스 이용에 있어서 개인정보에 대한 불안함을 느끼십니까?

- ① 매우 불안하다. ② 불안하다. ③ 조금 불안하다. ④ 전혀 불안하지 않다.

(설문 3) 일반 PC를 통한 인터넷 사용과 달리 스마트폰, 태블릿PC 등의 모바일 서비스만이 내포하고 있는 개인정보 보호의 문제점이 있다고 생각하십니까?

- ① 매우 많이 있다. ② 많이 있다. ③ 조금 있다. ④ 일반 인터넷과 동일하다.

(설문 4) 모바일 개인정보에 있어서 우려되는 항목을 모두 골라주시기 바랍니다.

- ① 자신의 동의 없이 이루어지는 개인정보의 수집·이용
② 개인정보에 대한 통제 상실 (누가 자신의 개인정보를 처리하는지 모르는 경우)
③ 개인정보 정책에 대한 자신의 무지
④ 형식적인 동의절차
⑤ 모바일 보안 문제 (바이러스 스파이웨어, 해킹, 모바일 악성코드 등)
⑥ 원하지 않는 타인과의 정보공유 (자신이 동의하여 사용하고 있는 SNS서비스 등)

(설문 5) 스마트폰 등을 이용하여 모바일 애플리케이션을 이용하면서 자신의 개인정보를 스스로 통제하고 있다고 생각하십니까?

- ① 매우 그렇다. ② 그렇다. ③ 확실하지 않다. ④ 그렇지 않다. ⑤ 매우 그렇지 않다.

(설문 6) 모바일 앱 등의 서비스 이용 과정에서 개인정보에 대하여 자신이 가지고 있는 통제의 정도에 만족하십니까?

- ① 매우 만족한다. ② 만족한다. ③ 확실하지 않다. ④ 만족하지 않는다.
⑤ 매우 만족하지 않는다.

(설문 7) 개인정보에 대하여 스스로 결정하고 통제할 수 있는 이용자의 권리가 현재보다 높아져야 한다고 생각하십니까?

- ① 매우 그렇다. ② 그렇다. ③ 확실하지 않다. ④ 그렇지 않다. ⑤ 매우 그렇지 않다.

(설문 8) 다음 보기 중 어떠한 이용자의 어떠한 권리가 더 중요하다고 생각하십니까?

- ① 자신에 대한 어떤 종류의 개인정보가 어떻게 수집되고 이용되며 그러한 개인정보가 누구에게 제공되는지에 대하여 이용자가 알 권리
② 통신서비스 및 모바일 어플리케이션 이용에 있어서 간편하고 쉬운 접근과 사용

(설문 9) 수집되는 자신의 개인정보가 서비스 이용에 반드시 필요하지 않음에도 불구하고 “동의하지 않으면 서비스를 이용할 수 없다(take it or leave it)”는 생각에 어쩔 수 없이 취급방침에 동의한 경험이 있습니까?

- ① 매우 많다. ② 많다. ③ 별로 없다. ④ 전혀 없다.

(설문 10) 개인정보 수집 동의 과정에서 서비스 이용을 필요한 필수 개인정보 이외에 추가적인 개인정보에 대하여 “선택”하여 동의한 경험이 있습니까?

- ① 매우 많다. ② 많다. ③ 별로 없다. ④ 전혀 없다.

(설문 11) 원활한 서비스의 이용을 위하여 반드시 필요한 개인정보와 추가적인 개인정보를 구분하고, 추가적인 개인정보에 대하여 동의 여부를 선택할 수 있도록 하는 선택적 동의에 대하여 어떻게 생각하십니까?

- ① 매우 찬성한다. ② 찬성한다. ③ 잘 모르겠다. ④ 반대한다. ⑤ 매우 반대한다.

(설문 12) 특정 모바일 서비스를 사용하기 전에 이동통신사 또는 모바일 어플리케이션 제공자가 제시하는 “개인정보 취급방침”을 읽어보셨습니까?

- ① 대부분 꼼꼼히 읽고 숙지한다.
② 대부분 읽지만 숙지하지 않는다.
③ 가끔 읽지만 대부분 읽지 않고 동의한다.
④ 전혀 읽지 않고 동의만 한다.

(설문 13) 취급방침을 읽지 않고 동의하였다면 그 이유는 무엇입니까?

- ① 어차피 서비스를 이용하기 위해서는 동의를 해야만 하기 때문에
② 개인정보 취급방침에 대한 중요성을 느끼지 못하기 때문에
③ 많은 분량의 정보가 작은 화면에 한꺼번에 표시되어 읽기가 어렵기 때문에
④ 이해하기 어려운 전문 용어가 포함되어 있기 때문에

(설문 14) 일반 컴퓨터 사용과 비교할 때, 모바일 단말기를 통하여 개인정보취급방침을 읽거나 숙지하는 것이 더 어렵다고 느끼십니까?

- ① 매우 어렵다. ② 조금 더 어렵다. ③ 별 차이가 없다. ④ 오히려 더 쉽다.

(설문 15) 모바일 서비스의 개인정보 취급방침에 동의함에 따라 자신의 어떠한 개인정보가 어떻게 수집되고 이용되는지 알고 계십니까?

- ① 잘 알고 있다. ② 대강 알고 있다. ③ 잘 모른다. ④ 전혀 모른다.

(설문 16) 개인정보취급방침에서 제시된 '개인정보의 수집 목적'이 자신이 이용하고자 하는 해당 서비스의 주된 기능을 제공하는데 반드시 필요하지 않다고 생각해본 적이 있습니까?(예: 메신저 앱의 '개인정보 수집 목적' 항목에서 '마케팅, 광고 활용의 목적')

- ① 많이 있다. ② 가끔 있다. ③ 생각해본 적 있다. ④ 전혀 생각해본 적 없다.

(설문 17) 개인정보취급방침에서 개인정보 수집 목적에 비하여 자신의 개인정보가 과도하게 수집된다고 생각해본 적이 있습니까? (예: '마케팅, 광고 활용의 목적'에 따른 이용자의 신용카드 번호 수집)

- ① 많이 있다. ② 가끔 있다. ③ 생각해본 적 있다. ④ 전혀 생각해본 적 없다.

(설문 18) 특정 모바일 앱의 개인정보 취급방침에 동의하는 경우, 개인정보 수집 목적에 의하여 이용자의 개인정보가 제3자에게 제공될 수 있습니다. 이에 대하여 불안함을 느끼십니까?

- ① 매우 그렇다. ② 그렇다. ③ 잘 모르겠다. ④ 그렇지 않다. ⑤ 매우 그렇지 않다.

(설문 19) 자신의 개인정보가 제3자에게 제공되었다는 통지를 모바일 앱 회사 및 통신서비스사로부터 받은 적이 있습니까?

- ① 여러번 받은 적이 있다.
② 드물지만 받은 적이 있다.
③ 한번도 받아본 적이 없다.

(설문 20) 모바일 앱 회사 및 통신서비스사가 개인정보를 제3자에게 제공할 때 개인정보의 주체에게 통지를 해야만 한다고 생각하십니까?

- ① 매우 그렇다. ② 그렇다. ③ 잘 모르겠다. ④ 그렇지 않다. ⑤ 매우 그렇지 않다.

(설문 21) 앱 서비스의 무료 이용을 조건으로, 자신의 개인정보가 광고회사와 같은 제3자에게 제공된다면 어떻게 하시겠습니까?

- ① 어떠한 개인정보든 상관없이 동의할 수 있다.
② 개인정보의 유형에 따라 동의여부가 다르다.
③ 제3자 제공에 동의할 의사가 없다.

(설문 22) 앱 서비스의 무료 이용을 조건으로, 앱 공급자가 추가적인 개인정보를 요구한다면 그 허용 범위는 어느 정도까지입니까?

- ① 어떠한 정보도 제공할 의사가 없다.
② 취미, 관심사, 기혼여부
③ ②번 포함 + 전화번호, 주소, 이메일 주소 등의 연락처
④ ②,③번 포함 + 신용카드, 계좌번호 등 금융정보
⑤ ②,③,④번 포함 + 포함주민등록번호, 의료보험번호 등 고유식별번호
⑥ 모든 개인정보

(설문 23) 제3자 제공에 대한 동의의 의사가 없거나 제한되어있다는 이유로 서비스 이용이 불가하다면 그 해결방안은 어떻게 다루어져야 한다고 생각하십니까?

- ① 유료가 아닌 무료 앱이므로 이용자가 서비스 이용을 포기해야한다.
② 선택적 동의방식을 통하여 민감한 개인정보를 제3자 제공의 대상에서 제외해야 한다.
③ 제3자 제공 사실에 대한 통지가 제대로 이루어진다면 동의할 의사가 있다.
④ 무료 앱을 구실로 과도한 개인정보를 이용하지 못하도록 법적 제재가 이루어져야 한다.

(설문 24) 개인정보 처리 동의에 대하여 철회하고 난 후 자신의 개인정보가 완전히 삭제되었다는 느낌을 받았습니까?

- ① 매우 확신한다. ② 확신한다. ③ 여전히 불안하다. ④ 강한 의구심이 든다.
- ⑤ 잘 모르겠다.

(설문 25) 개인정보 동의 절차와 비교하여 철회 절차가 어떻다고 생각하십니까?

- ① 동의 절차보다 철회 절차가 훨씬 까다롭고 복잡하다.
- ② 동의 절차보다 철회 절차가 조금 더 복잡하다.
- ③ 잘 모르겠다.
- ④ 동의 절차보다 철회 절차가 조금 더 용이하다.
- ⑤ 동의 절차보다 철회 절차가 훨씬 더 용이하다.

(설문 26) 철회의 경험이 없는 이유는 무엇입니까?

- ① 개인정보 수집에 동의하였던 모바일 서비스를 현재 모두 이용하고 있기 때문에
- ② 모바일 앱의 삭제와 개인정보 제공 철회 사이의 차이점을 느끼지 못하기 때문에
- ③ 철회에 대한 별도의 필요성을 느끼지 못하기 때문에
- ④ 철회를 하기 위한 까다롭고 번거로운 절차 때문에
- ⑤ 동의 후 철회가 가능하다는 사실을 몰랐기 때문에

(설문 27) 개인정보 이용·수집에 대한 철회를 하지 않은 후, 그에 대한 문제점을 인식한 경험이 있으십니까?

- ① 자주 인식한다. ② 가끔씩 인식할 때가 있다. ③ 거의 인식하지 않는다.
- ④ 전혀 인식해본 적 없다. ⑤ 잘 모르겠다.

(설문 28) 모바일 개인정보취급방침의 개선을 위하여 정부 차원의 통일적인 지침이 마련되는 것에 찬성하십니까?

- ① 통일적 지침 마련에 적극 찬성한다.
- ② 일정 부분 그 필요성을 인정한다.
- ③ 정부의 적극적 개입은 최소한이 되어야 한다.
- ④ 민간의 자율에 완전히 맡겨야 한다.

(설문 29) 개인정보 관련법률 위반에 대하여 어떠한 제재가 적당하다고 생각하십니까?

- ① 매우 무겁게 처벌되어야 한다. ② 무겁게 처벌되어야 한다.
- ③ 가볍게 처벌되어야 한다. ④ 경고적인 조치로 충분하다.

(설문 30) 모바일 개인정보취급방침에서 개선되길 희망하는 사항을 모두 골라주십시오.

- ① 자신의 정보가 언제 누구에게 어떠한 방법으로 수집되고 이용되는지에 대한 쉽고 용이한 설명
- ② 반드시 필요한 개인정보와 추가적으로 수집되는 개인정보 사이의 명확한 구분
- ③ 무료 앱 서비스의 무분별한 개인정보 수집 자제
- ④ 정보 수집 동의 및 철회의 의사표시에 있어서 간편한 절차

(설문 31) “카카오톡”과 같은 메신저 앱 이용시 자신의 모바일 기기에 저장된 주소록 정보를 서비스 제공자가 수집·이용하게 됩니다. 이때 수집되는 주소록 정보에 대하여 어떻게 생각하십니까?

- ① 자신의 단말기에 저장된 정보이므로 자신의 개인정보에 해당한다.
- ② 타인의 전화번호, 이메일 정보이므로 해당 타인의 개인정보에 해당한다.

(설문 32) 카카오톡의 주소록 정보 수집·이용에 대한 동의 방식에 대하여 어떻게 생각하십니까?

- ① 자신의 개인정보이므로 자신의 동의만 있으면 된다.
- ② 타인의 개인정보를 카카오톡(제3자)에게 제공하는 것이므로 정보제공에 대한 타인의 동의가 별도로 필요하다.
- ③ 타인의 정보로서 타인의 동의가 필요하나 서비스의 주된 목적 달성을 위하여 필수불가결하다.
- ④ 타인이 자신에게 전화번호를 제공한 사실자체가 제3자 제공에 대한 동의라고 볼 수 있으므로 타인의 동의없이 자신의 동의만 있으면 무방하다.

(설문 33) 카카오톡 “친구추천” 기능과 관련하여 개인정보에 대한 불안감을 느낀 적이 있습니까?

- ① 매우 많이 느낀다. ② 느낀다. ③ 잘 모르겠다. ④ 별로 느끼지 않는다.
- ⑤ 전혀 느끼지 않는다.

(설문 34) 카카오톡 친구추천 기능에 대하여 어떻게 생각하십니까? (복수응답 가능)

- ① 업무와 같은 특별한 사정으로 인해 자신의 주소록에 저장되어있지만, 해당 제3자가 친구추천 기능을 통하여 자신의 전화번호를 수집할까봐 불안할 때가 있다.
- ② 자신이 모르는 상대방이 자기 전화번호를 가지고 있다는 사실이 드러나게 되어 불편하다.
- ③ 연락을 원하지 않는 상대방이 친구추천 목록에 나타나더라도 이를 무시하면 되므로 크게 신경쓰지 않는다.
- ④ 서비스의 특성상 필요한 기능이므로 이를 통해 자신이 제3자의 전화번호를 수집하거나 제3자가 자신의 전화번호를 수집하는 것은 무방하다.
- ⑤ 어떠한 사람이 자신의 전화번호를 저장하고 있는지 알 수 있다는 장점이 있다.

⑥ 일일이 전화번호를 등록하거나 업데이트하지 않아도 된다는 편리함이 있다.

(설문 35) (SK텔레콤 이용자 대상) SK텔레콤 분할에 따른 기존 개인정보 취급방침 동의에 대한 철회의 절차 및 방법에 대하여 알고 계십니까?

- ① 자세한 철회 절차 및 방법에 대하여 알고 있다.
- ② 철회가 가능하다는 사실은 알고 있지만 그 절차와 방법에 대해서는 모른다.
- ③ 개인정보 이전만을 통보받았을 뿐, 기존 동의 철회에 대한 내용을 통보받은 적은 없다.
- ④ 안내문을 받았지만 이를 확인하여 해당 내용을 읽어보지는 않았다.

● 저 자 소 개 ●

박 노 형

- 고려대 법학과 졸업
- 하버드대 법학과 석사
- 캠브리지대 법학과 박사
- 현 고려대 법학전문대학원 교수

방송통신정책연구 11-진흥-라-09

모바일 서비스의 개인정보 활용행태 및 보호방안 연구
(A Study on Mobile Data Protection)

2011년 12월 일 인쇄

2011년 12월 일 발행

발행인 방송통신위원회 위원장

발행처 방송통신위원회

서울특별시 종로구 세종로 20

TEL:

E-mail:

Homepage:

인 쇄 보람문화사
