[토론회]

3500만명 개인정보 유출 사태의 원인 및 대책 마련을 위한 토론회

■ 일시 : 2011년 8월 16일(화) 오전 10시
■ 장소 : 환경재단 레이첼카슨룸
■ 주최 : 공공미디어연구소, 진보네트워크센터
■ 후원 : 방송통신위원회 양문석 상임위원, 환경재단

프로그램

○ 사회 : 양문석 위원

○ 발제
-네이트-싸이월드 개인정보 유출 사태로 본 정보인권의 문제 / 오병일 (진보네트워크센터)
-개인정보 보호를 위한 보안대책과 기업의 책임 / 이동산 (페이게이트 이사)

○ 토론
-전응휘 (녹색소비자연대 이사)
-김학웅 (변호사, 법무법인 창조)
-최민식 (한국인터넷기업협회 정책실장)
-김광수 (방송통신위원회 개인정보보호윤리과 과장)

[발제1]

개인정보 유출 피해 최소화를 위한 법제도적 대안
- 인터넷 실명제와 주민등록번호를 중심으로

오병일 (진보네트워크센터 활동가)

매해 역대 최대 규모의 개인정보 유출이라는 부끄러운 기록이 경신되고 있다. 2006년 2월, 게임사이트 리니지에서의 120만 명 규모의 명의도용, 2008년 1월 옥션 회원 1,081만 명의 개인정보 유출, 2010년 2000만 건의 개인정보 유출에 이어, 지난 2011년 7월 말, SK커뮤니케이션즈가 운영하는 네이트와 싸이월드에서 해킹에 의해 회원 3,500만 명의 아이디와 이름, 주민번호, 비밀번호, 전화번호, 이메일 주소 등 개인정보가 유출된 사고가 발생했다. 이제 올해 4월 발생한 현대캐피털 고객정보 175만 건 유출은 사소해보일 정도다. 이제 국민 대다수의 개인정보가 유출된 상황이라는 점은 이미 지난 2008년 옥션 사태 당시부터 지적되었다.

옥션 사태 이후에도 수차례 토론회를 통해 개인정보보호를 위한 법제도적 개선방안이 제시되었다. 여기서 다시 정보사회에서 개인정보 보호의 중요성이나 개인정보보호원칙을 되풀이할 필요는 없을 듯하다. 그것보다는 과거에 제시되었던 방안이 과연 효과가 있었는지, 그리고 이제 과거의 오류를 되풀이하지 않기 위하여 보완될 점은 무엇인지 검토하는 것이 바람직할 것이다. 개인정보 침해방지 대책은 개인정보의 수집, 보관과 관련한 제도적 대책과 보안과 관련한 기술적 대책으로 나뉠 수 있을 것이다. 이 글에서는 주로 제도적 대책과 관련된 문제를 다루고자 한다.

1. 인터넷 실명제가 문제다.

지난 8월 8일, 방송통신위원회는 '인터넷상 개인정보보호 강화방안'을 발표하였다. 옥션 사태 직후에도 방송통신위원회는 '인터넷상 개인정보 침해방지 대책"을 발표한 바 있다. (2008년 4월 24일)

올해 내놓은 방안에서 방통위는 현재의 문제점으로 ① 과도한 개인정보 수집, ② 기업의 보호조치 미흡, ③ 이용자 권리행사 부족을 짚고 있다.

정보사회에서 해킹이나 내부자 공모에 의한 개인정보 유출은 어찌보면 필연적으로 발생할 수밖에 없다. 100% 완벽한 보안이란 있을 수 없기 때문이다. 그러나 해킹 등에 의한 개인정보 유출을 줄이거나, 유출로 인한 피해를 최소화할 수는 있다. 그 중 핵심적인 것 중 하

나가 개인정보를 과도하게 수집하지 않는 것이다. 유출될 개인정보 자체가 없으니 이보다 완벽한 보안이 어디 있겠는가. OECD 가이드라인[1]과 UN 가이드라인[2]에서 모두 공통적으로 내세우고 있는 제1원칙이 '수집제한의 원칙'인 것도 이 때문일 것이다.

2008년에도 이러한 원칙을 몰랐던 것이 아니다. 방통위는 2008년 발표한 대책 문서에서 '주민등록번호 등 서비스 제공과 무관한 개인정보를 과다 수집하는 관행으로 개인정보 침해의 중요 원인이 됨'이라고 지적했다. 또한, '야후, MSN, 아마존닷컴 등 외국 주요사이트는 성명, 이메일, 생년월일 등 기본정보만 수집'하는데 반해, '국내 사이트의 73% 이상이 주민등록번호를 수집('06)'하고 있다고 분석하고 있다. 그리고 이에 대한 대책으로

□ 전자상거래 등 법적 권리 관계가 발생하는 경우에 한해 주민번호를 수집토록 하고, 일반적 포털 등은 수집을 제한하는 방안 추진
□ 현행 선언적 규정인 개인정보 필요 최소한 수집 규정의 실행력 확보를 위해 벌칙 적용 등 제도 개선 추진
□ 주민번호 제공 없이도 본인 확인을 받아 인터넷에 가입할 수 있도록 사업자의 대체수단(i-PIN 등) 제공 의무화

등을 들고 있다.

그러나 이 때 발표된 대책이 이후 얼마나 실효성이 있었는지 의문이다. 이번에 해킹을 당한 SK커뮤니케이션즈를 비롯한 많은 포털들이 주소, 전화번호, 휴대폰번호, 직업 등 서비스 이용에 필수적이지 않은 개인정보를 보유하고 있고, 여전히 대다수 국내 인터넷 기업들이 주민등록번호를 수집, 보유하고 있는 상황이다. 왜 그럴까?

기업들이 서비스 제공에 필요한 이상의 과도한 개인정보를 보유하고 있는 것은 당연히 1차적으로 기업의 책임이다. 그러나 정부 역시 기업들의 과도한 개인정보 보유를 규제하기 위한 실효성 있는 법적 조치를 취하지 않은 책임이 있다. 특히, 주민등록번호의 경우 오히려 정부가 그것의 수집을 조장했다고 말할 수 있을 정도다. 대표적인 것이 인터넷 실명제(제한적 본인확인제)다.

3500만 명 개인정보 유출 사고 이후, 수많은 언론과 전문가, 국회 입법조사처, 블로거까지 인터넷 실명제를 주범으로 지목하고 나섰다. 그러나 방통위는 여전히 인터넷 실명제가 개인정보 유출과 무관하다고 주장하고 있다. 지난 8월 3일 방통위가 발표한 해명자료[3]에 따르면, 방통위는 '인터넷실명제(본인확인제) 폐지를 검토한 바가 없'으며, '본인확인제와 해킹으로 인한 개인정보유출이 상관관계가 있다고 단정하기는 곤란'하다고 하고 있다. 이 해명자료에서 방통위는 "가장 대표적인 본인확인방법으로 사용되는 주민번호를 통한 실명인증의 경우에도, 정보통신서비스제공자들은 신용평가정보사 등 전자서명법에 따른 공인인증기관 등으로부터 본인인증을 받은 후, 본인 확인정보(본인인증 결과값)만을 보관하도록 되어 있

1) 개인데이터의 국제유통과 프라이버시 보호에 관한 가이드라인
2) 컴퓨터화돈 개인 정보파일의 규율에 관한 UN 가이드라인
3) [해명자료] 전자신문 보도(8.3) 관련 방송통신위원회 입장

으므로, 본인확인제가 주민번호 등 개인정보 수집을 의무화하는 것은 아니"라고 밝혔다. 즉, 인터넷 실명제는 주민등록번호 수집을 의무화하는 것은 아님에도 기업들이 자발적으로 수집했다는 것이다. 이는 정말 비겁한 변명이라고 하지 않을 수 없다.

물론 인터넷 실명제 법제화 이전에도 일부 기업들은 자체적으로 인터넷 실명제를 시행하고 주민등록번호를 수집하고 있었다. 그러나 최근 들어 기업들의 태도는 변화하는 모습을 보이고 있다. 2009년 유튜브의 인터넷 실명제 거부를 전후하여 기업들은 오히려 인터넷 실명제가 국내 기업들에 대한 역차별 규제라고 주장하며, 최시중 위원장에게 인터넷 실명제의 폐지를 건의하기도 하였다.[4] 그럼에도, 인터넷 실명제는 기업들이 주민등록번호를 보관하도록 하는 근거로 인식이 되어 왔는데, 이는 정보통신망망 시행령 제29조(본인확인조치) 3호에서 '게시판에 정보를 게시한 때부터 게시판에서 정보의 게시가 종료된 후 6개월이 경과하는 날까지 본인확인정보를 보관할 것'이라고 규정하고 있기 때문이다.

방통위 역시 지금까지 그렇게 이해해온 것으로 보여진다. 방통위가 주민등록번호 대체수단으로 권고하고 있는 i-PIN 홈페이지[5]를 보면, i-PIN과 '주민등록번호 실명확인'을 비교하면서, i-PIN은 주민등록번호가 웹사이트에 저장이 안되는 반면, '주민등록번호 실명확인'은 '개별 웹사이트에 저장'이라고 설명하고 있다. 만일 본인확인제가 주민등록번호 의무화를 전제하지 않는다면, 어떻게 이런 설명이 가능하다는 말인가?

최소한 방통위는 기업들의 주민등록번호 보관을 방치해온 것에 대해 책임이 있다. 인터넷 실명제가 주민등록번호 보관을 의무화하는 것이 아님을 기업들에게 설명하고, 주민등록번호를 보관하지 않도록 계도한 바가 있는가? 나아가 2008년에 발표한 대책에서 '전자상거래 등 법적 권리 관계가 발생하는 경우에 한해 주민번호를 수집토록 하고, 일반적 포털 등은 수집을 제한하는 방안 추진'한다고 하였으나, 실제로 주민등록번호의 수집을 제한하는 법제화는 추진되지 않았다. 고작 일정 규모 이상의 사업자에 대해 주민등록번호 외의 회원가입 방법을 의무적으로 제공하도록 하였을 뿐이다.[6][7] 그러나 주민등록번호를 이용한 본인 확인 방법은 여전히 보편적으로 이용되고 있다.

어쨌든 이제 기업들도 인터넷 실명제를 빌미로 주민등록번호를 남길 명분은 없게 되었다. 유출 사고 직후 SK커뮤니케이션즈는 앞으로는 주민등록번호, 주소 등의 개인정보를 보관하지 않겠다는 방침을 밝혔다. 다른 기업들도 인터넷 실명제 존속 여부와 상관없이 주민등록

---

4) [오마이뉴스] 국내 포털만 잡는 실명제... "우리도 구글처럼!" (2010.4.1)
http://www.ohmynews.com/NWS_Web/view/at_pg.aspx?CNTN_CD=A0001356205

5) http://i-pin.kr/

6) 제23조의2(주민등록번호 외의 회원가입 방법) ① 정보통신서비스 제공자로서 제공하는 정보통신서비스의 유형별 일일 평균 이용자 수가 대통령령으로 정하는 기준에 해당하는 자는 이용자가 정보통신망을 통하여 회원으로 가입할 경우에 주민등록번호를 사용하지 아니하고도 회원으로 가입할 수 있는 방법(이하 "대체수단"이라 한다)을 제공하여야 한다. ② 제1항에 해당하는 정보통신서비스 제공자는 주민등록번호를 사용하는 회원가입 방법을 따로 제공하여 이용자가 회원가입 방법을 선택하게 할 수 있다.

7) 2008년 발표한 대책에서 방통위는 '유출 개인정보를 이용한 인터넷상 명의도용 방지' 대책으로 '이름과 주민번호를 통한 본인확인 외에 추가로 휴대폰 등을 이용한 본인확인 절차를 사업자들이 도입토록 유도'하겠다고 밝혔다. 참으로 엉뚱한 대책이 아닐 수 없다. 타인의 주민번호를 도용하려는 사람이 왜 휴대폰 등을 이용한 본인확인 절차를 이용하려고 하겠는가?

번호 보관을 중단하고, 기존에 수집된 주민등록번호 역시 삭제해야할 것이다.

그러나 방통위의 설명대로 인터넷 실명제가 주민등록번호의 보관을 의무화하는 것이 아니라고 할지라도, 개인정보유출과 상관이 없는 것은 아니다. 여전히 주민등록번호 실명확인을 허용하는 한, 유출된 주민등록번호를 이용한 명의 도용은 계속될 것이기 때문이다. 왜 개인정보를 훔치려고 하는가? 당연히 개인정보가 가치가 있기 때문이다. 주민등록번호를 이용한 실명확인, 즉 인터넷 실명제는 그 활용도를 높임으로써 주민등록번호 도용을 부추긴다. 이미 중국에서는 인터넷을 통해 한국 국민의 주민등록번호가 공공연하게 거래되고 있다고 한다.[8] 8월 8일 발표한 대책에서 방통위는 '중국發 해킹 발생시 범인을 신속히 검거하고 인터넷상에 노출된 개인정보를 삭제토록 중국 정부기관 및 인터넷 유관단체와 공조를 강화'하겠다고 밝혔다. 당연히 인터넷 상에 노출된 개인정보를 삭제하도록 중국 정부와도 협조해야할 것이다. 그런데, 언제는 하지 않았던가? 이미 몇 년 전부터 중국 등 해외에서 한국 국민들의 주민등록번호가 노출되거나 거래되어 왔다.[9][10] 주민등록번호의 이용 자체를 고유 행정목적으로 최소화하여 그 이용가치를 줄이지 않는 한, 주민등록번호 도용의 위협은 계속될 수밖에 없다.

2. 아이핀(i-PIN)은 대안이 아니다.

개인정보 유출 사고가 터질 때마다, 그리고 주민등록번호 수집이 문제가 될 때마다 방통위는 아이핀을 대안으로 내세워왔다. 또한, 개인정보보호법 시행령을 제정하는 과정에서 행정안전부는 아이핀 도입 의무화를 추진하고 있다. 그러나 과연 아이핀이 대안이 될 수 있는지 의문이다.

우선, 불필요한 인증 요구의 문제는 여전히 남는다. 인터넷 실명제의 근본적인 문제는 서비스 이용에 필수적이지 않음에도 불구하고, 본인 인증을 요구한다는 점이다. 그 방식이 이름-주민등록번호 확인 방식이든, 아이핀 방식이든, 공인인증서 방식이든 이 문제는 여전히 남는다. 금융거래와 같이 본인 인증이 필요한 서비스도 있겠지만, 일반적인 인터넷 서비스에서 본인 인증을 요구하는 것은 넌센스이다. 그 자체가 필요 이상의 개인정보 수집이며, 인증 과정에서의 보안 문제를 야기할 수밖에 없다. 본인 인증 자체를 하지 않으면 되는데, 왜 주민등록번호 문제를 해결하기 위해 굳이 아이핀을 이용해야 하는지 의문이다.

둘째, 아이핀 역시 주민등록번호에 기반한 시스템이다. 따라서 주민등록번호 수집 및 도용의 문제를 여전히 가지고 있다. 아이핀을 개설할 때 자신의 이름과 주민등록번호를 입력하고, 휴대폰, 신용카드, 공인인증서, 대면확인 등의 본인 확인 과정을 거친다. (이와 같이 추

8) [연합뉴스] 中인터넷 '한국실명신분증' 검색에 링크 139만건 (2011.8.2)
9) [헤럴드경제] 중국 포털에 내 주민번호가 떠돈다 (2009.11.25) [한겨레] 한국인 주민번호·아이디·암호…'건당 1원'(2010.3.30)
10) 2010년 국정감사에서 한나라당 안형환 의원이 방통위로부터 제출받은 '최근 3년간 주민등록번호 노출 해외사이트 점검 조사 결과' 자료에 따르면, 중국은 2008년 190건, 2009년 265건, 2010년 상반기 126건으로 해마다 주민등록번호 노출 사이트 수가 증가한 것으로 나타났다. [뉴시스] [국감]주민번호 노출 가장 많은 해외사이트는 '중국' (2010.10.8)

가적인 본인 확인 과정을 거친다는 사실 자체가 이름-주민등록번호 대조 방식이 본인 확인 수단이 될 수 없다는 것을 입증한다. 더구나 국민 대다수의 주민등록번호가 이미 유출되었고, 오프라인에서도 쉽게 타인의 주민등록번호에 접근할 수 있는 상황에서는 말이다.) 그러나 2차 확인 방법 역시 주민등록번호에 기반을 두고 있다. 이미 지난 2010년 6월, 무기명 선불카드, 대리인증제도, 대포폰 인증 등 아이핀 발급 체계의 허점을 이용해 아이핀을 불법 발급받은 사례가 적발되기도 했다.[11] 이후 방통위는 선불카드나 대리인증제도를 통한 본인 확인 방법을 제외하였지만, 여전히 대포폰을 통한 아이핀 발급 등 명의 도용의 위험은 남아 있다.

셋째, 100% 완벽한 보안이란 없다고 했을 때, 인증기관에서 보유하고 있는 개인정보 역시 유출되지 않으리라는 보장은 없다. 불필요한 인증은 6대 인증기관[12]에 의한 불필요한 개인정보 수집으로 이어지는데, 이들 인증기관에서 보유하고 있는 개인정보가 유출될 경우의 파급력은 일반 업체들의 그것보다 훨씬 클 것이다. 이들 인증기관은 개인의 인터넷 사이트 가입내역까지 보관하고 있으니 말이다. 이들 인증기관은 유료로 본인 확인 서비스를 제공하고 있는데, 국가나 나서서 이들 사기업들에게 개인정보 장사를 하게 하는 것도 납득하기 힘든 일이다.

넷째, 아이핀은 이름-주민등록번호 확인 방식의 인증을 대체하기 힘들다. 아이핀을 도입한 지 4년이 넘었지만, 2011년 8월 현재 아이핀 사용자는 360만 명에 불과하다고 한다.[13] 즉, 인터넷 이용인구의 10%도 채 되지 않는 것이다. 이용자들은 왜 아이핀을 사용하지 않을까? 불편하기 때문이다. 노인과 같이 기술에 익숙하지 않은 이용자에게는 더욱 복잡하게 느껴질 것이다. 이름-주민등록번호 확인 방식의 인증이 유출 및 명의 도용 위협에도 불구하고 여전히 주된 인증 방식으로 이용되는 것은 그나마 간편하기 때문이다. 자신 명의로 핸드폰이나 신용카드를 개설하지 않은 사람(예를 들어, 부부같은 경우 한 사람 명의로 핸드폰 가입이나 신용카드를 사용하는 경우도 있고, 노인들은 자식 명의로 가입하는 경우도 많다.)은 그나마 아이핀에 가입할 수도 없다. 물론 인증기관을 방문해서 대면확인을 하는 방법이 있지만, 인터넷 사이트에 가입하기 위해 누가 그러한 부담을 지겠는가?

3. 개인정보 유출 피해를 최소화하기 위한 몇 가지 대안

1) 인터넷 실명제는 폐지해야 한다.

비단 주민등록번호 수집 및 명의도용 문제가 아니더라도 인터넷 실명제는 그동안 많은 비판을 받아왔다. 악플을 규제하겠다는 인터넷 실명제 도입의 명분은 효과를 거두고 있는지는 여전히 의문인 반면, 이용자의 표현을 통제하고 추적하기 위한 수단으로는 효과적으로 활용되어 왔다. 2009년 유튜브의 인터넷 실명제 도입 거부 이후에는 자국 기업에 대한 역차별

11) [연합뉴스] 아이핀 불법발급 유통 적발 (2010.6.6)
12) 2011년 8월 현재 서울신용평가정보, 코리아크레딧뷰로, 한국신용정보, 한국신용평가정보, 한국정보인증, 공공아이핀센터 등 6개 기관이 아이핀을 발급하고 있다.
13) [이데일리] 인터넷 여전히 주민번호..아이핀 360만 불과` (2011.8.1)

이라는 인터넷 기업들의 성토도 쏟아졌다.

이 때문에 방통위에서도 지난 2010년 6월 10일 발표한 '방송·통신·인터넷분야 규제개선 추진계획'에서 본인확인제도를 개선하겠다고 밝힌 바 있다. 당시 발표에 따르면, 2010년 4월부터 12월까지 '인터넷규제 개선 추진반'을 운영하고 정부, 학계, 업계, 시민단체 등의 의견을 수렴하여 개선방안을 검토하겠다고 했으나, 현재 어떠한 의견수렴 과정을 거쳐 어떠한 결론이 내려졌는지는 전혀 알려져 있지 않다.

3500만 개인정보 유출 사고 이후에도 방통위는 인터넷 실명제는 개인정보유출과 관계가 없다는 입장이다. 그러나 주민등록번호를 이용한 본인 인증이 허용되는 한, 이미 유출된 주민등록번호를 통한 명의 도용 위협은 계속될 수밖에 없다.

2) 주민등록번호의 수집 제한

주민등록번호 문제는 이미 오래 전부터 많은 전문가와 시민사회단체에서 제기해왔다. 지난 2006년 리니지에서의 명의도용 사태가 발생했을 당시에도 시민사회단체에서는 주민등록번호의 민간 이용을 금지할 것을 요구해왔다. 그러나 당시 행정자치부의 대응은 고작 '보안 강화'와 '명의 도용자에 대한 처벌 강화' 정도였다. 이것이 명의 도용을 방지할 수 있는 대책이 될 수 없음은 그 이후 벌어진 사태가 보여주고 있다.

현행 주민등록번호의 문제는 첫째, 번호 자체의 고유 목적을 벗어나 지나치게 광범위하게 수집, 이용되고 있다는 점, 둘째 주민등록번호 자체에 생년월일, 성별, 출신지역 등 개인정보를 포함하고 있다는 점, 셋째 주민등록번호의 변경이 사실상 불가능해 한번 유출될 경우 그 피해를 회복하기 힘들다는 점 등으로 정리할 수 있다. 지금부터라도 이러한 문제를 하나하나 해결해나갈 필요가 있다.

우선 민간 영역에서 주민등록번호 수집을 원칙적으로 금지하고, 공공 영역에서도 주민등록번호는 해당 행정목적에 한정하여 제한적으로 이용될 필요가 있다. 이번에 방통위에서 인터넷 실명제가 주민등록번호의 수집을 의무화하는 것이 아님을 명확히 밝힌 만큼, 기업들은 인터넷 실명제 존속 여부와 무관하게 주민등록번호 수집을 중단하고 기존에 수집된 것도 삭제해야 한다. 방통위도 '현재 이용자의 동의를 받아 누구나 주민번호를 수집할 수 있으나, 이를 원칙적으로 금지하고 예외적인 허용 정책으로 전환'하겠다고 밝혔다.(8.8 대책) 큰 틀에서는 환영할만한 방향이지만, 구체적인 내용이 나온 바가 없어서 아직 판단하기는 이르다. 특히, 예외적인 허용에 무엇이 포함될 것인지가 관건이 될 것이다.

인터넷 실명제 외에 기업들의 주민등록번호 수집을 부추기는 또 하나의 요인은 전자상거래와 관련된 기록 보유를 의무화한 '전자상거래 등에서의 소비자보호에 관한 법률'이다. 이 법률 제6조[14] 1항은 거래에 관한 기록을 일정 기간 보존하도록 의무화하고 있는데, 2항에서

14) 제6조(거래기록의 보존 등) ① 사업자는 전자상거래 및 통신판매에서의 표시·광고, 계약내용 및 그 이행 등 거래에 관한 기록을 상당한 기간 보존하여야 한다. 이 경우 소비자가 쉽게 거래기록을 열람·보존할 수 있는 방법을 제공하여야 한다.

소비자가 동의를 철회하는 경우에도 보존할 수 있도록 하면서 관련 개인정보를 '성명·주소·주민등록번호 등 거래의 주체를 식별할 수 있는 정보'로 규정하고 있다. 시행령 6조에서는 거래기록에 따라 6개월, 3년, 5년의 보존기간을 규정하고 있다.

SK커뮤니케이션즈도 유출 이후 대책을 발표하는 자리에서 주민등록번호와 주소 등은 앞으로 수집하지 않고, 기존에 수집된 정보도 폐기하겠다고 했지만, 싸이월드에서 스킨이나 배경음악, 도토리 등을 구매한 경우에는 관련 법률에 의거하여 주민등록번호 폐기 대상에서 제외된다고 밝혔다. 이와 같이 기업들은 위 법률에 의거하여 주민등록번호를 수집, 보관하고 있는 실정인데, 과연 동 법률이 주민등록번호 수집을 의무화하고 있는 것인지 관련 기관에서 명확히 밝혀줄 필요가 있다. 즉, 성명, 주소, 주민등록번호가 거래의 주체를 식별할 수 있는 정보의 예시적 규정인지, 혹은 거래를 입증할 수 있다면 굳이 주민등록번호를 보관할 필요는 없는 것인지가 문제가 된다. 예를 들어, 전자결제 업체를 통해 거래를 했다면, 판매업체에서는 결제 기록만 보관하여 나중에 전자결제 업체를 통해 확인할 수 있으면 되는 것이지, 굳이 주민등록번호를 보관해야 하는지 의문이다. 만일 동 법이 주민등록번호 수집 의무화를 의미한다면, 법 개정을 고려해야할 것이다.

3) 유출된 주민등록번호 재발급

주민등록번호 수집을 제한한다고 하더라도, 이미 유출된 주민등록번호의 도용을 통한 피해를 어떻게 최소화할 것인지는 여전히 문제가 된다. 주민등록번호를 바꿀 수 없는 한, 이미 주민등록번호가 유출된 사람은 평생 도용에 의한 피해를 의식하면서 살 수밖에 없기 때문이다. 따라서 이미 주민등록번호가 유출된 사람의 경우에는 자신의 주민등록번호를 변경할 수 있도록 해줄 필요가 있다. 일반적인 것은 아니지만, 탈북자 등 주민등록번호를 변경한 사례도 이미 존재한다.[15] 주민등록번호 변경이 불가능한 것은 아니라는 얘기다. 주민등록법 시행령 제8조(주민등록번호의 정정)에서도 주민등록번호에 오류가 있는 등의 사유가 있을 경우, 주민등록번호를 정정할 수 있도록 하고 있다.

이와 관련하여 행정안전부는 8월 9일 발표한 보도자료[16]에서 "주민등록번호를 변경할 경우 동일인 확인을 위한 사회적 혼란 및 이를 이용한 사기 등과 같은 범죄에 악용이 우려되는 등 - 막대한 사회적 비용의 초래가 예상됨으로 매우 신중한 접근이 필요함에 따라 그동안 주민등록번호의 변경은 일체 허용하지 않아 왔음 - 또한 수십 년간 사용해 온 자동차 면허, 부동산 등기, 예금, 보험, 직장 등 각종 공부의 주민등록번호 변경이 필요하여 국민이 오히려 많은 불편을 겪을 우려가 있음"이라고 입장을 밝혔다.

---

②제1항의 규정에 의하여 사업자가 보존하여야 할 거래의 기록 및 그와 관련된 개인정보(성명·주소·주민등록번호 등 거래의 주체를 식별할 수 있는 정보에 한한다)는 소비자가 개인정보의 이용에 관한 동의를 철회하는 경우에도 정보통신망이용촉진및정보보호등에관한법률 제30조제3항의 규정에 불구하고 이를 보존할 수 있다.

③제1항의 규정에 의하여 사업자가 보존하는 거래기록의 대상·범위·기간 및 소비자에게 제공하는 열람·보존의 방법 등에 관하여 필요한 사항은 대통령령으로 정한다.

15) [연합뉴스] 탈북자 주민번호 변경 허용 추진 (2008.7.6)

16) (설명) <해킹당한 주민등록번호 변경요구> 경향 등 보도 (행정안전부 언론기사 해명자료 게시판, 2011.8.9)

행정안전부 지적대로 주민등록번호 변경으로 인한 일정한 혼란을 있을 수 있다. 또한, 주민등록번호 변경으로 인한 사회적 비용이 더욱 높아지는 이유 중의 하나가 그만큼 광범위하게 수집, 이용되고 있기 때문이기도 하다. 그러나 전체 국민들의 주민등록번호가 유출된 현재의 상황은 '사회적 혼란'이 아닌지 되묻고 싶다. 그리고 주민등록번호의 민간 수집 금지와 변경 요청이 이미 2008년 옥션에서의 개인정보 유출 당시부터 제기되었음에도 불구하고, 그동안 행정안전부는 사회적 혼란을 최소화하면서 주민등록번호 제도를 개선하기 위해 어떠한 노력을 했는가.

사회적 혼란이 우려된다면, 행정안전부는 지금부터라도 주민등록번호 제도 개선을 위한 장기적인 로드맵을 만들어야 한다. 주민등록번호를 민간에서 이용하지 않도록 최소화하는 것이 그 시작일 것이다. 장기적으로는 개인정보를 노출하고 있는 현재의 주민등록번호 체계를 일련 번호로 바꾸는 것을 목표로 해야 한다.

4) 과도한 개인정보 수집 제한

지금까지 과도하게 개인정보를 수집해왔던 기업들도 이제 관행을 바꾸어야 한다. 2009년 <개인정보 수집·유통 실태조사>[17]에 따르면, 주요 포털 사이트들은 주민등록번호를 비롯하여, 주소, 전화번호, 휴대폰번호 등 개인정보를 필수정보로 수집해왔으며, 심지어 직업을 수집하는 경우도 있었다. 이번 유출 사고를 계기로 여타 기업들도 서비스에 필수적이지 않은 정보들의 수집을 재고할 필요가 있다.

17) http://act.jinbo.net/drupal/node/3941

[발제2]

국내 보안구조 개선을 위한 발제

이동산 (페이게이트 이사)

1. 네이트/싸이월드 3500만명 개인정보 유출

가장 최근의 개인정보 유출의 주요 사례중 하나.
개인정보 유출은 내부자 PC에 설치된 프로그램을 통해 진행
프로그램의 관리자 통제 없이 이용자가 자의로 설치한 것임.

1.1 관리자 권한 제거 시도

사건이 있고 나서 회사 내의 보안체계를 보완하려고 시도하였지만 문제발생.
내부 직원들의 개인 PC 관리자 권한을 제거하고 프로그램 설치를 회사에서 통제하려는 시도를 하였지만 문제는 인터넷 뱅킹이나 관공서 사이트 접속에서 발생
인터넷 뱅킹이나 관공서 사이트 접속시 ActiveX를 설치/실행해야하며 초기 계획은 ActiveX 설치는 관리자 권한으로 진행하되 한번 설치된 ActiveX의 실행은 일반 유저 권한으로 충분할 것으로 예상
그러나 매번 실행시마다 관리자 권한이 필요

1.2 Program Files/NPKI folder

인터넷 뱅킹이나 관공서 사이트 접속시 꼭 필요한 공인인증서는 대부분 ActiveX로 통제된다.
KISA의 공인인증서 저장위치 스펙에서는 공인인증서를 Program Files/NPKI folder에 저장하도록 정의하고 있다.
이 폴더는 일반적으로 해당 PC의 관리자 권한이 있어야 접근이 가능함.
주요 뱅킹이나 관공서 사이트에서 공인인증서 사용이 필요하며 이때마다 NPKI folder 접근이 필요.

2. 개인정보를 요구하는 웹사이트의 서비스 종류

개인정보를 요구하는 주요 웹사이트 서비스 종류를 조사해보았고 이러한 서비스를 진행할 때 과연 꼭 개인정보를 무조건 제출해야한 하는지 검토해볼 필요가 있다.

2.1 전자상거래 지급결제에서 요구하는 개인정보

전자상거래 지급결제시 사용하는 주요 결제수단으로는 신용카드, 실시간계좌이체, 은행 가상계좌 입금 등이 있다.
각 지급결제수단별로 요구하는 개인정보는 아래와 같다.

2.1.1 신용카드 결제시 요구되는 개인정보

- 신용카드 ISP 회원가입시 : 카드번호, 카드비밀번호, 카드 CVV2/CVC2 Code(카드뒷면 카드번호 옆 3자리 숫자), 카드 유효기간 등
- 신용카드 안심클릭 회원가입시 : 카드번호, 카드비밀번호, 카드 CVV2/CVS2 Code, 기타(카드 발행일 등, 카드사별로 상이)
- 신용카드 ISP결제시 요구되는 정보 : ISP 인증서 비밀번호
- 신용카드 안심클릭 결제시 요구되는 정보 : 안심클릭 비밀번호

* 신용카드 결제시에는 회원 가입 초기에만 개인정보를 제공하며 이후에는 ISP인증서 비밀번호나 안심클릭 비밀번호로만 결제가능한 것이 바람직하지만
실제 ISP는 인증서 비밀번호 분실시 인증서 재발행을 언제든 다시 진행할 수 있으며 이 과정에서 개인정보를 제공해야한다.

* 안심클릭의 경우 안심클릭 비밀번호를 등록하지만 이후 결제과정에서 지속적으로 신용카드번호를 제공해야한다.

* 최초 한번은 강력하게 인증하더라도 이후 사용과정에서는 개인정보를 제공하지 않고 결제하는 것이 가능하지 않을까?

2.1.2 실시간 계좌이체 결제시 요구되는 개인정보

- 공인인증서, 계좌번호, 계좌비밀번호, 주민등록번호 등
- 계좌이체 결제를 꼭 실시간으로 진행하지 않는다면 개인정보 제공을 최소화하거나 다른 여러가지 채널을 병행하여 이용함으로 개인정보를 한꺼번에 제공해야하는 위험을 줄 일 수 있지 않을까?

2.1.3 은행 가상계좌 입금거래

- 지급결제 그 자체만을 보면 특별한 개인정보 요구되지 않음.
- 특별한 개인정보를 요구하지 않으며 실제 결제구조에서는 일체의 프로그램을 설치할 필요가 없지만 가상계좌 결제를 이용하려는 고객에게까지도 공인인증서나 신용카드 안심클릭 등의 결제를 대비한 ActiveX를 미리 설치하도록 할 필요가 있을까?

2.2 인터넷 뱅킹 이용시 요구되는 개인정보

- 인터넷 뱅킹에서도 계좌번호, 공인전자서명등이 요구됨
- 순수한 웹표준 환경에서 인터넷 뱅킹이 정말 불가능한것일까?

2.3 포탈 인터넷 실명제

- 각 인터넷 포탈에서 실명인증시 : 이름, 주민등록번호
- 실명인증이 필요없는 서비스를 제공하거나
- 실명인증을 한곳에서만 진행하고 이 정보를 다양한곳에서 활용하도록 하면 어떨까?

- OAuth, SAML, OpenID등 다양한 오픈 인증방식을 도입한다면 한곳에서 인증을 거친결과를 공유하는것도 가능해보임.

3. 국내 보안구조의 문제점

현재 국내 인터넷 서비스의 개인정보 보호를 위한 보안 구조의 문제점을 살펴보자.

3.1 모든 접속자를 잠재적 범죄자 취급

초기 접속시 다양한 개인정보를 요구하여 확인하는 인증방식은 유저를 잠재적 범죄자로 취급하는 인식에 기인함.
이러한 구조에서는 한번 인증을 통과한 이후에는 더이상의 자세한 통제를 하지 않는 서비스 구조를 유발하게 된다.
개인정보를 과도하게 요구하지 않는 일부 서비스 업체의 경우 최초 접속 유저들의 입력정보를 신뢰하여 업무처리를 하지만 이후 사이트내의 행동패턴이나 재접속 빈도, 경로 등의 정보를 취합하여 통계적인 필터링을 도입하는 경우도 구현 가능함.
즉 대부분의 정상적인 행위를 하는 선량한 유저를 보호하면서 비정상유저만을 걸러내는 방식의 구현도 가능하지만 현재의 보안구조는 모든 접속유저를 범죄자일지도 모른다는 의심하에 선량한 유저를 구분하기 위한 과도한 인증정보를 요구하고 있으며 조금은 다른 차원의 접근이 필요하다.

3.2 획일적인 보안체계

인터넷 인터넷 서비스 설계에서 병목현상을 제거하라는 논리가 존재함.
이것은 단일 취약점에 문제가 생겼을 경우 전체 소통에 영향을 미치는것을 방지하기 위한 아주 기본적인 개념이지만 현재 국내 보안체계는 너무 많은 단일 취약점이 존재함.
국민들은 대부분 동일한 벤더의 운영체제를 사용하고 동일한 브라우저를 이용하며 동일한 방식으로 보안구조가 설계된 사이트에 접속하여 서비스를 이용하고 있으며 이러한 단일 보안 취약점은 해커의 가장 좋은 공격목표가 될 수 있다.
만일 전국민의 본인확인 방식이 아이핀이라는 인증방식 하나로 통일된다면 이것역시 구조적 취약점중의 하나로 해커에게는 좋은 공격목표가 될 수 있음.

3.3 제도적 문제점

3.3.1 법규정에서 상세한 보안구조를 강제화

전자금융거래법 시행세칙을 살펴보면 인터넷 뱅킹이나 전자상거래 지급결제시 이용자 PC에 키보드보안 프로그램이나 안티바이러스를 접속시 ⭐ 우선적으로 ⭐ 설치하도록 강제하고 있음.
서비스 사업자가 보안프로그램을 설치하지 않아도 위법하고 이용자가 접속하기 전에 깔아도 위법하고 접속후 나중에 깔아도 위법함.
이미 Antivirus 소프트웨어를 사용중인 유저도 예외 없이 은행에서 제공하는 Antivirus 프로그램을 깔아야함.

법규정에서 상세한 사이트 보안구성을 강제하려는 시도는 좋지만 이것은 시간이 지나면서 새로운 창조적 서비스를 방해하는 요소가 될 수 있으며 보안규정 자체는 신기술이 탄생하면서 지속적인 업데이트가 필요하지만 법규정의 변경은 보안과는 별개의 변화관리 프로세스를 따르므로 현실과 동떨어진 규제가 되버리는 문제점이 발생.

3.3.2 부처간 협업 부재

국내 인터넷 이용환경에 영향을 미치는 가장 주요한 정부기관은 방송통신위원회와 금융감독위원회 2개 기관임.
인터넷 이용환경이나 국가 보안구조 등에 대한 담당부처는 방통위가 적절하지만 보안 비전문가 그룹인 금융위에서 국내 금융서비스 보안에 대한 모든 최종결정을 하고 있으며 방통위나 금융위는 상호 협력하는 관계는 아님.
보안에서 부처간 업무영역을 구분해서 접근하는 방식 자체가 보안을 저해하는 난센스임.
작년 공인인증 대안기술 허용을 위한 총리실 주최 미팅에 참석한적이 있었고 그때 느낀점도 정부 부처가 다르다는 이유로 분명히 다루어야할 보안에 관한 사항을 월권이라는 이유로 무시하고 넘어가는 경험이 있음.

4. 국내 보안구조 개선을 위한 대안

4.1 다양성의 확보

다양성의 확보가 무엇보다 중요하다.
하나의 획일화된 환경이나 구조는 해당 구조의 취약점 하나가 무너졌을 때 상상할 수 없는 파급효과를 예상할 수 있다.
예를 들어 인터넷 본인확인 구조를 아이핀으로 통일시킨다면 당장의 주민등록번호 유출에 대한 대응은 가능하지만 아이핀 구조의 보안취약점이 발생하거나 더이상 사용할 수 없는 상황이 되었을 때는 국내 인터넷 서비스가 중단되는 문제점을 충분히 예상할 수 있음.
좀 더 다양한 운영체제를 국민들이 이용할 수 있도록 인터넷 이용환경을 개선하고 브라우저나 보안 프로그램 등 좀 더 다양한 선택을 국민이 할 수 있도록 개선하는 것이 무엇보다 우선시되는 보안구조 개선의 방안이라고 생각

4.2 보안 컴프라이언스

보안은 이용자 PC에 바이러스 프로그램을 깔거나 관리자의 내부 DB접근에 대한 통제방식을 개선하는 등의 단편적인 방식으로는 보안성을 높일 수 없음.
검토가능한 모든 보안위험요소를 포괄하는 종합적인 대응만이 본질적인 보안성을 달성할 수 있다고 생각.
국제적으로 다양한 보안 컴플라이언스들이 존재함.
PCI, SOX, GLBA, HIPAA, ISP27002 등
PCI에서 다루고 있는 보안규정을 예들 들어보면
네트웍보호, 시스템 구성 관리, 저장된 데이터 보호 (암호화 등), 전송 데이터 보호, 내부 관리자 시스템의 취약점 관리, 안전한 소프트웨어 개발 및 관리, 내외부 시스템 접근통제, 물

리적 보호, 모니터링 및 테스트, 보안정책 관리 등을 언급하고 있으며 보안규정은 주요한 변화가 발생될때마다 업데이트되며 실질적인 감사 및 보증은 민간차원에서 진행된다.
민간에서 다양한 창의적인 서비스를 계획하고 실시하지만 현실은 보안성 심의 등 정부규제에 의해 서비스 실시자체가 막히는 현실이다.
민간의 창의적인 서비스는 보안 컴플라이언스로 보안성을 검증받고 보안 컴플라이언스에 대해서 컴플라이언트하다면 창의적인 서비스를 허용할 수 있는 대전환이 필요하다.

4.3 웹표준 및 계몽

사업자는 어떠한 별도 프로그램을 설치하지 않아도 되는 웹표준 기반의 서비스를 설계하고 이용자는 프로그램 설치에서 무조건 "예"를 클릭하지 않도록 계몽이 필요하다.
웹표준은 앞서 말한 다양성이나 보안컴플라이언스 등의 이슈와 밀접하게 연계된 중요한 개념이다.
특정 벤더나 특정 서비스에 의존하지 않으면서 새로운 인터넷 환경에 능동적으로 대응할 수 있으며 동시에 보안성도 달성할 수 있는 지속가능한 인터넷 환경을 달성하는데 꼭 필요한 개념이다.
국민들이 웹표준에 대응하는 인터넷 이용 습관을 유지할 수 있도록 계몽하는 것도 꼭 필요하다.

5 국민은 선량하고 똑똑하며 능동적임

현재 국내 보안 구조는 국민들은 멍청하고 피동적이며 잠재적 범죄자임을 전제로 구성되고 있다는 느낌을 지울 수 없다.
그러나 실제로는 국민들은 선량하고 우리가 생각하는 것보다 훨씬 똑똑하며 능동적이다.
인터넷 이용자들이 올바른 선택(의심스러운 프로그램 설치 요구에는 "아니오"를 클릭)을 할 수 있도록 환경을 제공하고 인터넷 서비스 제공자들도 올바른 선택(보안컴플라이언스 준수)을 할 수 있고 정부는 이를 인정하는 환경이 필요하다.

[토론문]

개인정보유출사태 원인 및 대책 마련을 위한 토론회 토론문

최민식 (한국인터넷기업협회 정책실장)

o 발제문에서 오병일 국장님께서 언급하신 바와 같이 포털 등 인터넷기업에 대한 해킹의 근본 원인은 사회 모든 영역에 걸쳐 정보화가 급속하게 확대되어 주민번호 등 개인정보에 대한 수집과 활용이 보편화되었기 때문이며, 이러한 개인정보 수집과 활용에 대한 역기능으로 해킹에 의한 개인정보 유출, 오·남용 등 침해사고가 발생하고 있으므로 이러한 침해사고가 재발하지 않도록 그 원인에 대한 철저한 수사 및 관련 법·제도, 정책 개선 등의 강력한 대응이 필요하다고 생각합니다.

o 현재 이슈가 되고 있는 사항은 제한적 본인확인제, 거래기록보관 등 관련 법령에 의한 주민번호 수집 및 보관의무와 마케팅 등 기업의 필요에 의한 개인정보 수집이라 할 수 있습니다. 기본적으로 법이 개정되어 인터넷 기업의 입장에서도 부담이 되는 주민번호 수집·보관 의무가 없어진다면 인터넷기업 은 환영할 것입니다.

o 우리나라에는 주민번호를 수집·보관·이용하는 법령과 정책이 다수 존재하고 있으며[1], 특히 실명인증과 관련하여 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」[2], 「공직선거법」[3] 등이 있고 주민번호가 포함된 상거래 기록의 보관을 위한 「전자상거래등에서의 소비자보호에 관한 법률」, 주민번호 등 개인식별번호의 제공·이용을 위한 「신용정보의 이용 및 보호에 관한 법률」[4] 등이 있으며, 특히 온라인에서 대면 확인이 어려우므로 주민번호 등을 이용한 성인인증 수단이 필요한 「게임산업 진흥에 관한 법률」[5], 「청소년보호법」 등 인터넷기업이 준수해야하는 많은 법령이 있습니다.

o 일부 기업이 마케팅 목적으로 개인정보를 과다하게 수집하고 있다는 지적이 있으며 과거에는 많은 정보를 수집하는 것이 마케팅에 유리하다는 인식이 있었으나, 개인정보보호에 대한 인식의 확산 및 해킹 등 침해 범죄 심화에 따라 불필요한 개인정보는 수집

---

1) 국가법령정보센터(http://www.law.go.kr)에서 주민등록번호를 검색하면 618개의 법령이 나오는 등 주민등록번호는 우리나라에서 개인을 식별하는 수단으로 광범위하게 사용되고 있음.
2) 2007년 개정으로 게시판이용자의 본인확인제(제44조의5)를 도입하였고 2008년 개정으로 I-PIN 등 주민등록번호 외의 회원가입 방법을 도입하였음(제23조의2).
3) 2005년 개정으로 인터넷언론사 게시판·대화방 등의 실명확인을 도입하였음(제82조의6).
4) 같은 법 시행령 제29조(개인식별정보의 제공·이용) 법 제34조제1항에서 "대통령령으로 정하는 정보"란 생존하는 개인의 성명, 주소, 주민등록번호, 외국인등록번호, 국내거소신고번호, 여권번호, 성별, 국적 등 개인을 식별할 수 있는 정보를 말함.
5) 올해 7월 개정으로 게임과몰입·중독 예방조치 등을 위하여 정보통신망을 이용한 게임물 관련사업자는 게임물 이용자의 회원가입 시 실명·연령 확인 및 본인 인증을 하여야 함(제12조의3).

하지 않는 것을 원칙으로 현재는 고객에 대한 서비스를 원활히 하기 위한 필수 정보인 이메일, 전화번호 등의 연락처로 최소화하는 방향으로 기업의 정책이 변화되고 있습니다.

o 이제는 개인정보보호 수준에 따라 기업의 신뢰성이 보장되고 책임 있는 기업으로 자리매김 할 수 있으므로 인터넷기업들은 고객 개인정보보호를 위하여 적극적으로 노력하고 있으며 관련 법령에서 규율하는 이상으로 개인정보보호를 위하여 최고의 노력을 다하고 있습니다.

o SK커뮤니케이션즈를 비롯한 포털 등 인터넷기업은 평소 보안설비 투자 등 보안에 대한 기술적·관리적 보호조치에 많은 노력을 다하여 왔습니다. 그럼에도 불구하고 이번 해킹으로 인한 개인정보 유출 사고는 고도의 지능적인 수법에 의한 것으로서 불가항력적이라 해도 과언이 아닐 것입니다.

o 인터넷기업도 이용자의 개인정보보호를 위한 노력을 철저히 하고 있지만 해킹 등 범죄의 표적이 되고 있으므로 이용자도 자기정보에 대한 보호 노력을 철저히 할 필요가 있으며 기업들도 고객 중심으로 고객이 원하지 않은 개인정보에 대해서는 수집을 하지 않는 방향으로 개선되어야 할 것입니다. 이러한 점은 법적 준수 사항 이상으로 노력을 해야 할 것입니다.[6)]

o 또한 국가기관의 지속적인 관심과 지원으로 실행력과 실효성을 담보할 수 있는 구체적인 계획도 마련되어야 합니다. 국가적 차원에서 정보보호 인력의 양성과 정보보안 분야의 국가 연구개발(R&D) 사업의 확대를 추진해야 하고 정부 차원의 대응체계 뿐만 아니라 민간에서 역할을 수행할 수 있는 법·제도적 근거도 마련되어야 할 것이며, 기업에서 시행하고 있는 기술적·관리적 보호조치에 있어 기업의 입장을 충분히 고려하고 지원을 아끼지 않았으면 하는 바람입니다. 감사합니다.

---

6) SK커뮤니케이션즈는 '11년 9월경부터 기존 수집한 주민등록번호도 파기하고, 수집하는 정보는 아이디(ID), 이름, 비밀번호 변경을 위한 연락처, 실명확인을 위한 아이핀(I-PIN)이나 신용평가사의 실명인증 값, 생년월일, 성별 등으로 최소화하고 현재 방통위, KISA 등 유관기관 및 인터넷기업들과 공동캠페인 진행 추진중(자기정보보호 캠페인/비밀번호 변경, 휴면계정 정리 등) 적극적으로 전개 중임.

[토론문]

Auction 有感 2탄[7)]

김학웅(변호사 / 법무법인 창조)

1. 본인확인제(망법 제44조의5)의 두 가지 측면

o 표현의 자유의 본질적 요소인 익명표현의 자유(right to anonymous speech) 침해
o 유출되어서는 아니 되는 개인의 정보

2. 개인식별번호 관련 입법례

o 스웨덴 : 우리나라와 유사한 제도. 국가에 등록된 개인정보의 범위와 사용용도가 한정됨. but 사회보장체계를 위해서만 사용.
o 프랑스 : 중앙주민등록시스템(NIR : National Identification Register)에 개인식별번호부여를 포함 but 강제적 방식 x 자발적 요청에 의함. 수집 및 이용이 법률에 의해 엄격 규제.
o 미국 : 주민등록제도, 개인식별번호, 국가신분증 제도 x. 다만 신청지역, 발급그룹, 발급순서를 나타내는 각 3자리 숫자 총9개로 이루어진 사회보장번호(SSN : Social Security Number)가 개인식별번호와 같은 역할을 하지만 사회보장번호를 민간이 이용하는 것은 금지.
o 캐나다 : 사회보험번호(SIN : Social Insurance Number)가 있으나 그 용도는 벌금부과, 소득세 징수, 실업급여 등 15개 행정업무에만 사용할 수 있도록 엄격히 제한되며 그 외의 이용은 법률의 규정에 따라야 함.

3. 주민등록제도의 역사와 활용

o 시·도민증 : 한국전쟁으로 인한 신분확인의 필요성
o 1962. 1. 15. 기류법 제정 : 무장공비 침투로 인한 간첩 및 범죄자 색출의 목적
o 1962. 5. 10. 기류법 대체 입법으로 주민등록법 제정 ---> 이동산 이사님이 발제문에서 언급하고 계신 '모든 접속자를 잠재적 범죄자 취급'도 같은 의미일 것이다.
o 주민등록제도의 활용 : 활용 범위의 무제한성 ---> 상품으로서의 정보성 + .정보의 연

---

7) 지난 2008. 5. 2. 프레스센터 외신기자클럽에서 옥션 해킹사태 관련 토론회가 있었다. 그때 토론문의 제목이 『Auction 有感』이었다. 3년여가 지난 지금 토론자는 해킹을 당한 업체만 다를 뿐, 동일한 문제에 대한 동일한 토론에서 동일한 토론자(전응휘 이사님)와 함께 동일한 이야기를 반복해서 하고 있다. 이게 작금의 우리 상황이다.

결고리이자 핵심으로서의 주민등록번호 + 주민등록번호 입력을 강제하는 사회 = 해킹의 유혹(과거 하나로텔레콤 사태에서도 보여 지듯이 개인 정보 유출의 유혹은 개인정보를 수집.관리하는 자도 느낄 수 있다.)

4. 현행 법제도

o 처벌은 제대로 이루어지고 있는가?[8)]
o 손해배상은 제대로 이루어지고 있는가?[9)]
o 손해배상청구소송과 관련하여 제기되는 문제
  1) 피고 선정의 문제 : 과연 사업자만이 피고인가?
  2) 정책과 손해 발생 사이의 인과 관계는 없는가?
  * 사업자와 user의 관계 = 甲과 乙의 관계 / 방통위와 사업자의 관계 = 甲과 乙의 관계 ---> 오병일 활동가님이 발제문에서 적절하게 지적하고 있듯이, 방통위가 사안에 대해 "본인확인제와 정보 유출은 관계없다."고 태도로 수수방관하는 이상 사업자는 울며 겨자 먹기로 방통위의 정책에 따르고 소송의 피고가 되어야 하는 사태가 예상됨.
o 처벌과 손해배상은 문제의 근본적 해결책이 될 수 있는가? 잘못된 정책[10)]이 계속되는 한 근본적 해결은 요원함.
o 최근 제정된 개인정보보호법(법률 제10465호, 2011. 3.29, 제정. 시행 2011. 9.30)
  제6조(다른 법률과의 관계) 개인정보 보호에 관하여는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」, 「신용정보의 이용 및 보호에 관한 법률」 등 다른 법률에 특별한 규정이 있는 경우를 제외하고는 이 법에서 정하는 바에 따른다. ---> 결국 공은 다시 방통위로 넘어온 셈이다.

5. 개선 방안

o 주민등록번호 제도의 폐지, 대체입법 마련
o 과거 수집된 주민등록번호에 기반한 정보를 어떻게 처리할 것인지에 대한 고민이 입법에 반영되어야.
o 진정한 의미에서의 통합개인정보보호법 제정 ---> 개인정보보호법이 행안부 소관이고,

---

8) <정보통신망이용촉진및정보보호등에관한법률>
  제24조(개인정보의 이용 제한), 제24조의2(개인정보의 제공 동의 등), 제28조의2(개인정보의 누설 금지), 제48조(정보통신망 침해행위 등의 금지) 제2항, 제3항, 제49조(비밀등의 보호) 위반시 제71조에 의하여 5년 이하의 징역 또는 5천만원 이하의 벌금.
  제48조(정보통신망 침해행위 등의 금지) 제1항, 제49조의2(속이는 행위에 의한 개인정보의 수집금지 등) 제1항, 제66조(비밀유지 등) 위반시 제72조에 의하여 3년 이하의 징역 또는 3천만원 이하의 벌금.
9) 손해배상 소송 인용액은 십수만원에 불과. 더구나 사업자가 기술적 보호조치의무를 모두 이행하면 손해배상책임 없음.
10) 아이-핀(I-PIN)은 주민등록번호의 대안이 될 수 있을까? 개인정보 유출이 낮아질 가능성 有. but 문제의 근본 원인은 주민등록번호. 이 주민등록번호에 기반한 이상 아이-핀(I-PIN)은 미봉책일 뿐.

망법이 방통위 소관이라는 업무 분장의 문제는 국민의 개인정보보호라는 명제 앞에서는 부차적인 것일 뿐.

6. 작금의 소송 사태

o 권리 의식의 향상? 개인 정보 침해 관련 소송은 로또?
o 소송의 최대 수혜자는?
o 옥션 소송 당시 '착수금 3만원이면 200만원 배상' but 결론은? ---> 현대형 소송의 특징 중 하나인 '소액 피해 다수 피해자'가 의뢰인과 변호사 사이에서 발생하는 건 아닌지.
o 불법행위로 인한 손해배상은 안 날로부터 3년 / 있은 날로부터 10년. 상사 채무불이행으로 인한 손해배상청구소송은 있은 날로부터 5년 ---> 1심 판결 지켜본 후에 소송해도 늦지 않음.

7. 방통위에 대한 질문

o 2008년 옥션 사태 이후 어떤 정책을 지향했고, 그에 따른 연구 결과물이 있는지?
o 개인정보보호법에 대한 방통위의 입장은?
o 망법에 대한 현재의 입장을 고수할 것인지?