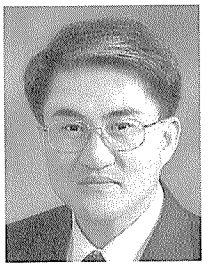
디지털시대의 E-Commerce와 프라이버시 보호문제



서 천 석
변리사 · 변호사(미국)

I. 머리말

전자상거래는 원격통신 특히 인터넷을 통하여 이루어지는 비즈니스 거래를 총칭하는 것으로 Electronic Commerce (e-commerce) 또는 E-Business(e-biz)라고도 부른다. 전자상거래의 응용은 1970년대 초기에 시작되어 1990년대 인터넷의 상용화와 더불어 급격히 발전하기 시작했다. 전자상거래는 전자기술이 가져다 준 신속성과 효율성을 지지기반으로 하여 시간 · 장소에 무관하게 실시간으로 원하는 상대방과 접촉할 수 있어 경제 · 사회의 변혁을 주도하는 또 하나의 산업혁명 즉 디지털 혁명이라고까지 일컬어지고 있다.

세계경제는 현재 정보기술과 인터넷의 발달로 「디지털 경제시대」로 이행하는 패러다임 변화(Paradigm Shift)를 겪고 있으며, 생산, 경영 및 상업 활동 등 기업 활동 전반에 혁신적인 변화가 초래되고 있다. 이러한 디지털 경제시대의 특징은 하나의 구심점이나 구체적 실체가 없이 모든 것이 수평적인 사이버 공간에서 전자부호로 이루어진다는 데 있다.

바야흐로 전통기업에 비해 구매의 편리성과 스피드, 저렴한 가격, 다양한 선택의 폭을 제공하는 순수 디지털 기업이 인터넷을 기반으로 한 기업과 경쟁의 1라운드에서 승리하고 있는 듯 하다. 국내 · 외에서 인터넷 비즈니스에 대한 관심과 투자가 폭발적으로 증가함에 따라 인터넷이 산업활동의 중심축으로 자리 잡아 가는 추세는 당분간 지속될 전망이며, 전자상거래가 미래 비즈니스의 핵심이 될 것이라는 데에 대해서도 이론의 여지는 없는 것으로 보인다.

그러나 컴퓨터 보급률이 나날이 증가됨에 따라 시 · 공간적 한계가 극복되는 긍정적인 측면보다는 오히려 부정적인 측면이 이제는 더욱 부각되고 있어 사회적인 문제가 되고 있다. 즉, 정보통신망의 발전과 함께 인터넷이 생활의 일상화를 차지하게 되면서 물건 구매시에 입력하는 각종 개인정보의 보호문제가 대두된 것이다. 특히 개인의 금융정보가 해킹이나 보안의 부주의로 타인에게 노출되면 심각한 경제적 피해를 입게 되기 때문에, 본 고에서는 그러한 개인의 은밀한 정보가 어떻게 침해되고 있는지 사례를 살펴보고 그 대책에 대해 간단히 언급하기로 한다.

II. 전자상거래의 개관 및 프라이버시 유출의 위험성

전자상거래는 狹義로는 컴퓨터와 네트워크라는 전자적인 매체를 통해 상품을 사고 파는 행위를 통칭하며, 廣義로는 개인, 기업, 정부 등 모든 경제 주체들의 활동과 상호 관계에서 정보와 가치를 상호 교환 · 공유하는 체계 모두를 포함하는 개념으로 사용된다.

전자상거래의 확산에 가장 큰 장애요인은 개방네트워크 체제로의 전환에 따른 보안문제를 들 수 있는데, 이러한 보안문제의 예로는 '개인의 메시지 가로채기', '개인정보의 불법적 수집', '해킹과 바이러스 침입에 의한 피해' 등을 들 수 있다. 또한, 금융거래시에 발생하는 신원확인, 권한인증 등을 통하여 입력하는 개인정보가

세계경제는 현재 정보기술과 인터넷의발달로「디지털 경제시대」로 이행하는 패러다임 변화(Paradigm Shift)를 겪고 있으며, 생산, 경영 및 상업 활동 등 기업 활동 전반에 혁신적인 변화가 초래되고 있다. 이러한 디지털 경제시대의 특징은 하나의 구심점이나 구체적 실체가 없이 모든 것이 수평적인 사이버 공간에서 전자부호로 이루어진다는 데 있다. 바야흐로 전통기업에 비해 구매의 편리성과 스피드, 저렴한 가격, 다양한 선택의 폭을 제공하는 순수 디지털 기업이 인터넷을 기반으로 한 기업과 경쟁의 1라운드에서 승리하고 있는 듯 하다.

개인 비밀키의 분실에 따라 쉽게 유출될 수 있는 점도 보안문제의 하나로 꼽을 수 있다. 한편, 인터넷을 통한 개인정보의 수집은 본인의 동의를 얻지 않더라도 쿠키(cookie) 또는 클릭스트림(clickstream) 데이터를 이용하여 쉽게 이루어질 수 있는 문제도 있다. 그리고, 개인이 이용하는 은행, 신용카드 회사, 각종 금융기관, 전자자금 이체 시스템 등 다양한 경로를 통한 개인의 신용정보는 점점 개인을 적나라하게 드러내는 추세이다.

III. 전자상거래에 있어서 프라이버시의 보호

1. 프라이버시의 개념

"개인정보"라 함은 생존하는 개인에 관한 정보로서 당해 개인을 알아볼 수 있는 부호·문자·음성·음향 및 영상 등의 정보(당해 정보만으로는 특정 개인을 알아볼 수 없는 경우에는 다른 정보와 용이하게 결합하여 알아볼 수 있는 것을 포함한다)를 포함함은 물론 사자(死者)에 관한 정보와 개인 비식별 정보 가운데 정보통신기술 등을 이용하여 개인을 추적할 수 있는 정보까지 포함하는 것으로 정의할 수 있으며, 본고에서의 "프라이버시" 또는 "데이터 프라이버시"의 보호대상이라 할 수 있다.

개인정보는 정보통신서비스제공자들이 일반적으로 수집하고 있는 성명, 주민등록번호, 전화번호, 주소, 전자우편주소 등에 이르는 일반 신상정보는 물론이고 생존자 및 사자의 성별, 신장, 체중, 혈액형, 지문, 유전자 정보, 병력 등 생리적 상태에 관한 정보와 생년월일, 혼인여부, 직업, 학력, 수입, 주거상태, 차종, 종교, 성적 취향, 전과기록, 병역정보, 정치단체 참여와 같은 사회경제적 상태를 확인할 수 있는 정보를 포함한다. 뿐만 아니라, 제 1·2 금융기관과 각종 신용정보기관이 보유하고 있는 신용금융정보 등 국내 각 행정·금융·신용·의료기관 등에서 보유하고 있는 개인에 관한 모든 정보가 프라이버시의 보호대상인 개인정보에 해당된다. 상기와 같은 개인식별이 가능한 정보 외에, 쿠키나 Internet Protocol 추적기술·바코드·도청장치·감시카메라·위성위치추적기술 등의 도구나 기술을 이용하여 개인을 추적 감시할 수 있는 다양한 신호와 음향·영상 등의 정보까지도 개인정보에 포함된다.

2. 프라이버시 침해의 유형별 분류

정부에서는 개인정보침해 고충처리 및 침해 예방활동의 추진과 개인정보 보호발전 방안 강구 및 정책시행을 위하여 개인정보 침해신고센터를 운영하고 있는데, 상기 센터에 접수된 신고사례들을 유형별로 분류하면 다음과 같다.

유 형 분 류	비 율(%)
타인에 의한 개인정보 훼손, 도용	43%
원하지 않은 정보(전자우편, 전화, 팩스 등) 수신	16%
개인정보 열람 및 정정요구, 회원 탈퇴 요구에 불응	8%
이용자 동의 없는 개인정보 수집	6%
동의 없는 제3자 제공 및 목적외 사용	5%
개인정보 수집 및 목적달성 후 미파기	3%
개인정보 수집시 고지 또는 명시의무 불이행	0.6%
안전성 확보 미조치	0.3%
과도한 개인정보 수집	0.1%
기 타	18%

가장 많이 접수된 프라이버시 침해의 유형은 '타인의 개인정보 훼손 및 도용'으로서, 주로 주민등록번호 도용에 의한 것이었다("AOL 사회저명인사 개인정보 해킹 사례" 참조). 그 주요 원인은 주민등록번호자동생성기의 불법 유통으로 인해 취득한 타인의 주민등록번호로 웹사이트에 회원으로 가입하는 사례가 빈번히 발생하고 있기 때문이다. '원하지 않은 정보수신'은 마케팅 수단으로 전화나 전자메일을 이용하는 사례가 늘면서 수신자가 수신거부의사를 밝혔음에도 불구하고 계속 광고성 전화나 전자메일을 보내는 경우이다. 이러한 사례는 보통 개인의 핸드폰 번호와 이름, 전자메일주소 등이 무단 유출되어 발생한 것이기 때문에 '이용자 동의 없는 개인정보 수집' 사례와 맞물려 있는 경우가 많다("DoubleClick 사례" 참조). '개인정보 열람·정정·삭제요구 불응'으로 신고된 건에 대해 ISP(인터넷서비스제공자)들은 대부분 처리과정상 지체되거나 과실로 누락된 경우라고 해명하고 있다. 그러나 이는 이용자의 권리요구에 대해 아직까지 ISP들이 민감하게 대처하지 못하고 있음을 반영하는 것이라 하겠다. 한편, '기타' 사례가 큰 비율을 차지하고 있는 것이 특이할 만한데, 여기에는 개인정보의 불법 가로채기 등이 포함된다("Councilman 사례" 참조). 마지막으로, '이용자 동의 없는 개인정보 제3자 제공'은 인터넷 서비스가 대중화되고 서비스 제공자간 연합이 활성화되고 있는 요즘 가장 논란의 대상이 되고 있는 사례("Amazon & Alexa 사례" 참조)이다. 회원수가 갖는 마케팅 효과를 대신하여 새롭게 채택되고 있는 서비스제공자간 업무 제휴라는 마케팅 전략은 개인정보의 이동 및 공유를 확산시켰고, 그 과정에서 이용자의 동의를 제대로 받지 못 하는 일이 빈번히 발생하게 된 것이라 하겠다.

3. 프라이버시 침해

가. 프라이버시 침해의 사례

① 아메리카온라인(AOL) 사회저명 인사 개인정보 해킹 사례

1996년 말, 클린턴 미국대통령, 유명언론인, 마이크로소프트사의 빌게이츠, 아메리카온라인(AOL)의 최고경영자인 스티브 케이스 등이 전자우편 폭탄 공격을 받았다. 공격자는 위 유명인사들의 전자우편 계정을 도용, 그들을 1,000여개의 메일링 리스트에 가입시켜 피해자가 하루 수천 건의 전자우편을 받도록 하였다. 공격 2일 후, 자칭 "Johny Xchaotic"이라고 자신을 밝힌 범인은 메일링 리스트를 이용한 전자우편 폭탄 공격의 용이함과 인터넷의 상업화 및 혼란에 대한 비난의 내용을 담은 메시지를 게시하였다. 이 사건으로 1,300여명의 저명인사들의 ID, 본명, 계좌번호 등을 포함한 개인정보 데이터베이스가 해킹당하고 이 데이터가 전자우편을 통해 유출되었다.

② Amazon & Alexa 사례

2000년 9월 초, 온라인 소매업체 Amazon.com은 고객들에게 개인정보 보호정책 변경을 공지하는 내용의 이메일을 보냈다. Amazon의 새로운 개인정보보호정책은 Amazon.com의 고객정보의 사용에 관한 것이었고, 그 중 핵심은 고객이 자신의 개인정보가 제3자에게 유출되지 못하도록 선택할 권리가 주어지지 않는다는 것이었다. Amazon.com의 신규 정책은 "고객정보는 기업가치의 일부이고, 이러한 정보는 외부에 판매되지 않을 것이다."라고 규정하면서도 "만일 Amazon.com 또는 그 보유자산이 제3자에게 인수되는 경우, 고객정보 또한 인수대상에 포함된다." 라고 분명히 규정하고 있다.

이에 대해 온라인 프라이버시 옹호단체인 Junkbbusters.com과 EPIC (Electronic Privacy Information Center)는 Amazon이 고객의 개인정보유출이 가능하도록 하는 것은 소비자들을 기만하는 것이 아닌가를 판정해 달라고 FTC(공정거래위원회)에 제소했다. 이들 소비자 보호단체는 Amazon의 정책변경이 제3자에게 개인정보를 '결코' 노출시키지 않겠다던 이전 조항과 어긋나므로 기만적이고 불법적이라고 주장했다. 이들은 또한 (1)고객의 사전 동의 없이는 고객신상정보 노출을 금지하고, (2)고객에게 신상정보와 구매이력을 삭제할 선택권을 부여하며, (3)고객이 요구할 시에는 다른 기업에게 노출시키거나 교환한 개인정보를 알리고 고객프로필에 대한 고객의 완전한 접근권을 허용하도록 FTC에 요청하였다.

2001년 5월, FTC는 고객의 개인정보를 제3자에게 제공할 수 있도록 한 Amazon의 새로운 개인정보보호정책이 개인정보보호법을 위반한 것이 아니라고 결정했다. FTC의 소비자보호 책임자는 Junkbbusters.com과 EPIC에 보낸 서한에서 "제3자에게 이용자들의 개인정보를 제공할 수 있도록 한 Amazon의 개인정보보호정책 변경은 Amazon이 당초 제3자에게 개인정보를 제공할 수도 있다고 이용자들에게 고지했던 만큼 소비자들의 권리를 침해한 것이라고 볼 수 없다."라고 밝혔다.

그러나, 상기 사건과는 별개로 Amazon과 그 자회사 Alexa Internet사를 상대로 제기된 여러 건의 집단소송에 대해 워싱턴주 서부지역을 관할하는 연방지방법원은 2001년 7월 최저 타협안을 승인하였다. 상기 타협안에 따라, Amazon은 Alexa의 데이터베이스에서 발견된 이용자 한 사람당 40달러(총 1.9백만 달러)를 배상해야 하였고, 보다 강화된 프라이버시 정책을 채택하였으며, 고객들이 자신의 개인정보가 수집되기 전 사전 동의권을 갖도록 개인정보보호정책을 개선하였다.

③ DoubleClick 사례

본 사례는 웹사이트상에서의 제3자 광고행위와 관련된 개인정보(특히 클릭스트림 데이터) 유출에 관한 것으로, 이해를 돕기 위하여 클릭스트림 데이터와 쿠키에 대해 간략하게 설명하기로 한다. 먼저, "쿠키"는 "인터넷 웹사이트에 의하여 형성되어 이용자의 컴퓨터에 저장되는 정보" 또는 "웹 이용자들을 식별하기 위하여 웹 서버에 의하여 이용되는 데이터 조각"을 의미한다. 이러한 쿠키에는 해당 웹사이트와 관련된 각종 개인정보가 저장되어 있기 때문에, 웹 서버는 이용자가 장래에 해당 웹사이트에 접속하는 경우 이전에 기록된 쿠키를 통하여 이용자가 누구인지, 어떠한 정보를 주로 검색하고 구매하였는지 등의 웹사이트 이용기록을 파악할 수 있다. 한편, "클릭스트림 데이터"는 이용자 개개인을 특정지을 수 있는 쿠키를 이용하여 수집된 정보로서, 웹사이트 상에서 이용자가 무엇을 좋아하고 무엇을 싫어하는지를 비롯해서 사용자의 행동에 대해 많은 것을 빠르게 파악할 수 있게 하는 정보를 말한다.

만약 A라는 회사가 어떤 쿠키(예: 숫자 987654)로 특정 브라우저를 인식하고, B라는 회사도 어떤 쿠키(예: 숫자 123456)로 같은 브라우저를 인식한다고 가정할 때, 회사 B는 회사 A의 클릭스트림 데이터를 획득하더라도 별다른 이득을 얻을 수는 없다. 왜냐하면, 각각의 웹 서버는 자신만의 고유한 쿠키를 사용하기 때문에 특정 이용자의 웹 서핑 행태에 관한 정보를 일반적으로 수집하는 것은 거의 불가능하다.

그러나, 상기와 같은 개별 웹 서버의 경우가 아닌 제3자 광고서버의 경

우는 사정이 달라질 수 있다. 예컨대, 각각 별개의 웹사이트 C·D·E가 모두 제3자인 F로 하여금 자신의 웹사이트에 광고를 할 수 있도록 허용한다면, F는 C·D·E의 사용자들이 이용하는 웹사이트들에 대해서 동일한 쿠키를 사용할 수 있다. 이 때, 각각의 웹사이트 C·D·E는 단지 그들 각각의 사이트 내에서 사용자들이 무엇을 하는지를 알 수 있을 뿐이지만, F는 그 모든 사이트의 사용자의 행위를 종합적으로 파악할 수 있는데, 이러한 문제점을 취급한 사례가 바로 이 DoubleClick 사례이다.

DoubleClick사는 인터넷을 기반으로 제품과 서비스에 대한 광고 선전의 일환으로 타인의 웹사이트에 배너광고를 제공하면서 쿠키를 이용하여 인터넷 사용자의 IP 주소, 브라우저 종류, 날짜와 시간 및 그 사용자가 배너광고를 클릭하였는지 여부 등에 관한 정보를 광범위하게 수집하였다. 2000년 1월말부터 여러 건의 소송이 제기되었는데, DoubleClick사가 상기 개인정보를 자사의 자회사인 Abacus를 통해 획득한 고객의 개인정보와 결합하고 있다는 혐의가 제기되었다.

그렇지만, FTC는 2001년 1월 Doubleclick이 자신이 이미 공개한 "프라이버시 보호정책"에서 개시한 목적 이외의 다른 목적에 고객들의 개인정보를 사용한 바 없다고 판단하여 본 사건을 종결하였고, 법원은 2001년 3월말 동 사건을 기각하였다. [154 F. Supp.2d 497(S.D.N.Y. 2001)]. 이 사건에서 법원은 DoubleClick의 쿠키를 통한 정보수집 행위는 DoubleClick의 배너광고를 게재한 웹사이트들이 이미 그러한 행위에 동의한 바 있다는 점 등을 판시의 주된 이유로 들었다. 참고로, DoubleClick이 자사의 인터넷 홈페이지에 밝힌 프라이버시정책을 살펴보면, "인터넷 광고를 제공하는 데 DoubleClick사는 어떠한 개인정보도 사용하지 않는다."고 함으로써 개인정보를 고객의 동의 없이 다른 목적으로 사용하지 않는다는 점을 명확히 하고 있다.

④ Councilman 사례

Councilman은 Interloc사의 부사장이었으며, Interloc사의 주된 사업은 희귀한 필사본 책의 목록 서비스를 "@Interloc.com"으로 끝나는 자사의 e-mail로 책 도매상들에게 제공하는 것이었다. 1998년 5월, Alibris사(캘리포니아 회사)는 Interloc사를 인수합병 하였으며, Councilman은 상기 희귀 필사본 책 목록 서비스 사업을 책임지게 되었다. 회사의 인수합병 와중에 Councilman은 Interloc사 시스템에 의한 전자 메시지의 전송에 관련된 사실을 알게 되었는데, Interloc사의 컴퓨터 시스템은 이메일을 송신할 때 대상 이메일을 스캔하고 저장하고 있었다. Councilman은 이러한 시스템을 이용하여 Amazon.com이 고객들에게 보내는 모든 통신문을 카피하고 가로챌 수 있도록 자사의 컴퓨터 코드를 조작할 것을 종업원들에게 지시하였다. 결과적으로, Councilman은 타사의 전자우편 내용을 가로채고 불법적으로 수집된 이메일 내용을 공개하려 공모한 혐의로 기소되어 최종적으로 유죄 판결을 받았다. [United States v. Councilman, 245 F. Supp.2d 319 (S.D.N.Y. 2004)].

⑤ 신용카드 번호, 유효기간, 비밀번호 유출로 인한 피해

피해자는 지난해 4월 28일 사이퍼스어학원에 등록하면서 학원비를 신용카드로 결제하였다. 그 직후, 사정이 생겨 학원 등록을 취소하였고, 다음달 25일 카드사로부터 배달된 신용카드대금청구서에 상기 매출이 취소되어 있는 것을 확인하였다. 그런데, 그 다음달 청구서를 살펴보니 5월 26일 1백만원의 매출이 12개월 할부로 발생되어 있었다. 전혀 이용한 적이 없는 곳에서 허위 매출이 발생되어 있었던 것이다. 이 사건은 학원 등록시 전자결제에 필요하다며 비밀번호 앞의 두 자리를 알려 달라고 해서 알려준 적이 있었던 것이 그 원인이었다.

⑥ 신용카드 명의 도용으로 인한 피해

2001년 동생 甲김은 언니 乙의 명의를 도용하여 신용카드를 발급 받았다. 언니 乙은 동생 甲이 여러 금융기관으로부터 신용카드를 발급 받아 무단으로 사용하여 피해를 보던 중 우연히 그 사실을 알게 되었다. 언니 乙은 즉시 일일이 신용카드를 취소하고 소정의 구제를 받았으나, 조흥은행 등 두 곳에서는 신용카드 회원가입을 적시에 취소해 주지 않아, 乙은 결국 신용불량자로 전락하게 된 것이다.

⑦ 판매원이 소비자 동의 없이 카드 부정사용

피해자는 2002년 4월 한 맛사지센터에 2,600,000원의 1년 등록비를 신용카드로 결제하고 회원으로 가입하였다. 3개월 후인 7월 맛사지센터 직원이 찾아와 신규가입자를 대상으로 12개월 무이자 할부 행사를 하고 있다고 말하면서 특별히 신규 가입한 것으로 처리해 줄 테니 신용카드를 가져와 새로 결제하면 이전에 결제한 카드대금은 바로 취소해 준다고 했다. 12개월 무이자 할부라는 말에 솔깃하여 어머니 카드를 가져가 2,600,000원을 새로 결제하고 이전 카드 결제한 것은 취소전표만 받아 왔다. 8월 말 카드청구 내역을 보니 어머니 카드로 3,590,000원이나 결제되어 있고 가맹점도 엉뚱한 곳이었으며 이전 카드 결제한 것도 취소가 되어 있지 않았다. 판매본사에 카드대금 청구 취소를 요청하니 가맹점이 틀리게 되어있어 취소 처리해 줄 수 없다고

하였다.

나. 프라이버시 침해에 관한 웹사이트 예

지금까지는 프라이버시 침해의 사례들을 살펴보았으나, 아래에 열거한 웹사이트에서 우리는 상황의 심각성을 인식할 수 있다. 이들 웹사이트들은 인터넷상에서 자신의 이름을 등록하고 물건을 구입하는 인터넷 상거래 과정에서, 일반 이용자들의 개인 신상정보들을 불법적으로 모아서 상업화된 데이터 베이스를 만들어 이용하고 있는 것이다.

① ACCURINT(www.accruint.com)

이 회사는 미국에서 가장 방대한 인명과 주소 데이터베이스를 가지고 있는데, 누구든지 25센트(한화 300원 정도)만 지불하면 상대방의 주소와 재산정도를 인터넷상에서 알아낼 수 있는 서비스를 제공한다.

② COURTLINK E-ACCESS(www.courtlinkeaccess.com)

이 회사는 미국내 주 법원과 연방법원의 소송기록들을 수집해서, 상대방 이름이 파산법정 기록에 있는지, 형사소송에 연루된 적이 있었는지, 가정법원에 기록상 이혼 경력이 있는지 등을 검색해 주는 서비스를 제공하고 있다.

③ CHOICEPOINT(www.choicepoint.net)

이 회사에서는 고용주가 근로자들의 신원검색을 할 수 있도록 해당 근로자의 개인정보와 각종기록을 검색해 준다.

④ USSEARCH(www.ussearch.com)

이 회사는 관련 비즈니스 업계 사람들의 신원조회 서비스를 해 준다.

⑤ RAPSHEETS(www.rapsheets.com)

이 회사는 5,000만 건의 범죄사건 기록을 보유하고 있어서 상대방의 사회보장번호(Social Security Number)만 입력하고 $5.95 달러를 지불하면 그 사람의 전과 여부를 확인해 준다.

III. 맺음말

최근 급속한 정보화 기술의 발달과 인터넷을 통한 정보화의 진전 등으로 많은 사람들이 편익을 누리고는 있지만, 이로 인한 역기능은 이미 심각한 사회적 문제로 대두되고 있다. 특히, 인터넷에서의 개인정보는 다른 일반 정보와 달리 온라인상에서 한 개인의 신분(ID) 또는 정체성을 나타낸다는 점에서 중요하다고 할 수 있다. 그러한 개인의 정체성이 앞서 살펴본 바와 같이 무분별하게 전자상거래에서 오·남용된다면 개인적 피해의 측면뿐만 아니라 국가적 차원에서도 커다란 손실일 것이다. 따라서, 네트워크 환경에서 이용자들이 안심하고 거래를 할 수 있도록 하려면 개인의 프라이버시 보장은 필수적 요건이며, 국가는 개인정보를 취급하는 모든 자를 적용대상으로 하는 적극적인 개인정보 보호 노력을 경주하여야 할 것이다.

한편, 경제구조의 복잡화 및 기술진보의 가속화와 개인의 프라이버시 문제를 단순히 제도와 법률적인 측면에서만 보호하고 규제하기보다는 업계 스스로 이용자의 개인정보 보호에 관심을 갖고 개인정보 보호에 관한 이용자의 요구사항을 적극적으로 찾아내어 그 보호방안을 마련하는 자율규제를 병행하여야 할 것이다. 덧붙여, 개인정보의 보호에 필요한 적절한 기술을 활용하는 것도 효과적일 수 있을 것으로 본다.

그러나, 무엇보다도 중요한 것은 이용자 개개인이 빠르게 변하는 디지털 사회에서 자신의 개인정보에 대한 결정권을 자각하고 스스로 행사하는 것이라 할 것이다. 즉, 적극적으로 자신의 개인정보에 대한 통제권을 확보하려는 노력이 상기 제도적 정비 혹은 기업들의 자율규제에 선행되어야 한다. 이에 전자상거래 이용자들이 자신의 프라이버시를 스스로 지키고자 하는 노력과 관련하여 다음과 같은 사항을 권고하고자 한다.

첫째, 기술적으로 더 나은 "Cookie Manager"를 채용하고 있는 최신 웹 브라우저를 사용한다.

둘째, 웹브라우저에 높은 수준의 프라이버시 세팅을 설정해 두고, 자신이 미리 설정해 놓은 프라이버시 보호수준에 불일치하는 웹사이트에 대해서는 회피하여야 할 것이다. 참고로, Microsoft사의 IE6에서는 "모든 쿠키 차단", "높음", "보통 높음", "보통", "낮음", 그리고 "모든 쿠키 허용" 등 6단계의 프라이버시 보호 수준을 선택할 수 있도록 하고 있다.

셋째, 민감한 개인정보(예: 신용카드번호, 은행계좌번호, 주민등록번호 등)를 입력할 경우에는 미리 당해 웹사이트의 프라이버시보호정책을 읽어볼 필요가 있다.

넷째, 상기와 같은 민감한 개인정보를 입력할 경우 당해 웹사이트가 "안전한 웹사이트(Secure Site)"인지 여부를 확인한다.

마지막으로, 이용자가 입력한 정보 중에서 "이메일주소"가 웹상에 일반인에게 공개되는지 여부를 확인한다.