# 전자통신, 프라이버시, 그리고 '전자사생활 보호법 1986
## : 기술 발달에 뒤처진 법체계

Jan H. Samnoriski, John L. Huffman and Denise M. Trauth

이 글은 미국방송교육협회가 발행하는 'Journal of Broadcasting & Electronic Media' (제 40 호.'96.10 월호)에 실린 "Electronic Mail, Privacy, and the Electronic Communications Privacy Act of 1986 Technology in Search of Law"를 번역한 것이다.....편집자 주

이 글은 전자사생활이 처한 현재의 상황에 관한 고찰이다. 좀더 구체적으로 말하자면 컴퓨터의 대량 보급으로 만들어진 환경 속에서 발생하는 전자통신과 기타 관련된 커뮤니케이션상의 문제점을 다루고 있다. '전자사생활 보호법'이 1986 년에 통과(U.S.C. 18, §§2510-2711)된 이래, 이 법이 과연 전자사생활을 충실하게 보호하고 있는지에 관한 의문이 제기되어 왔었다.

이 글에서 우린 전자 통신의 사생활이 '전자사생활 보호법' 하에서 어떤 보호를 받고 있는지 규명하려 한다. 우선 현재의 법에 대해서 검토한 다음 '전자사생활 보호법'의 허점을 보여주었던 몇 건의 판례를 검토할 것이다. 사례와 관련 문헌의 검토를 통해, 회사 직원들이 사무공간에서 주고받는 전자통신 내용에 대한 무제한적인 감시와 절취를 허용하는 허점이 현재의 '전자사생활 보호법' 속에 있음을 보여주려고 한다.

## Ⅰ. 개 요

1993 년 봄, 텍사스주 미연방지방 법원 소속의 한 판사에 의해 전자사생활 보호에 관한 새로운 판례가 마련되었다. 그는 오스딘 소재의 출판사 겸 컴퓨터 게임 제작사의 컴퓨터 관련 장비를 압류한 미연방비밀조사국의 행동은 '전자사생 활보호법' (이하 '보호법')을 위반한 것이라고 판결하였다. 이 사건(Steve Jackson Games Incorporated, et al., v. United States Secret Services, United States of America, et al. (1993))에 대한 판결은 '보호법' 제정 이후 당시까지 내려진 관련판례 중 가장 비중 있는 것이었으며, 동시에 언론과 관련된 법체계 전반에 있어 의미 있는 진보적인 것이었다. 왜냐하면, 컴퓨터 통신 상의 전자게시판에 전자적 형태로 저장된 정보에 대한 정부의 압수 행위에 제동을 건 최초의 사례였기 때문이다. 이 법원의 결정은 1994 년 제 5 순회항소법원(Circuit Court of Appeals')의 재판에서도 지지를 받았다. 이 사건으로 말미암아, 대중적인 관심은 무르익었지만 마땅한 판례가 거의 없어 세간의 주목을 받지 못했던 전자통신 사생활에 이목이 집중되기 시작한다. 사실, '정보 가로채기'는 공적이건 사적 영역이건 언제나 중요한 관심거리 중 하나였다.

하지만 오늘날과 같이 전자통신이 발달한 세계에서 이러한 관심은 복잡다단한 문제를 만들어내고 있으며, 점점 더 어려운 질문을 우리에게 제기하고 있다. 1994 년 8 월,

아리조나주 항소법원은 아주 어려운 결정에 직면했다. 증거품으로 압류한, 직원(Pima County Assessor's Office)들의 전자통신 메시지가 담긴 백업(backup) 테입을 과연 전통적 의미의 '공적 문서(public documents)'로 봐야 할 것인지가 문제였다. 이에 대해 법원은, 공공기관 종사자들이라 할지라도 자신의 업무용 컴퓨터에 보관한 사적인 문서의 프라이버시는 보호받을 충분한 이유가 있다는 말로 의견을 대신했다(Star Publishing Company v. Pima County Attorney's Office, 1994, at 1). 1994 년 4 월, 매사츄세츠주 대법원은 전자통신을 통해 모욕적인 내용의 글을 다른 노조 조합원에게 보낸 경관을 해고한 것은 정당하다고 판결하였다(Plymouth Police Brotherhood v. Labor Relations Commission, 1994). 가장 최근의 경우로는, 1995 년 9 월, 미연방수사국(FBI) 요원들이 미국 최대의 컴퓨터통신 서비스업체인 아메리카온라인(America Online)의 수천명의 가입자들의 전자통신 사서함을 뒤져서 수십명의 가입자들을 '유아 포르노물(child pornography)' 거래 혐의로 체포한 사건도 있었다.

문제의 핵심은 기술의 발달이 새로운 법적 영역을 만들어낸다는 데 있다. 방송이나 연설, 인쇄매체 등 전통적인 매체에서 언론의 자유를 지키려고 고안된 법들은 컴퓨터통신이 창출한 가상공간에서의 언론자유를 지키는 데 역부족이라는 사실이 드러나고 있다. 여기서 가상공간이란, 전자통신이 이뤄지는 곳을 말하며, 컴퓨터와 통신, 소프트웨어, 데이터, 전자통신망 등을 포괄하는 개념이다. 입법자들이나 사법당국은 자신들이 급속도로 변화하고 있는 복잡한 상황 즉, 통신 사용자들이 상호간에 정보를 교환하고, 저장하며, 방대한 양의 정보에 자유로이 접근하고, 싼 값에, 별다른 부담 없이 오랜 시간 통신망을 헤집고 다니는 그런 상황에 놓여 있음을 자각하고 있다. 입법가에 의해 법률이 기초되는 순간 법조문이 낡아 버리는 그런 상황이 닥친 것이다. 국가정보하부구조(National Information Infrastructure, NII)에 대한 계속된 논의와, 이제는 더 이상 새로울 것도 없는, 전국을 디지털 광섬유로 연결시키자는 '정보고속도로(Information Highway)'제안과 맞물려, 전자사생활 보호는 그 어느 때보다 첨예한 문제로 대두되고 있다. '전자데이터베이스'에서부터 '발신인의 전화번호를 알려주는 장치' 등과 같은 커뮤니케이션기술의 발달은 사생활보호와 관련된 수많은 문제를 일으켜 왔다. 그와 함께 최근 들어 전자통신 사용자의 수가 급증함에 따라 그들에게 관심이 모아지고 있다. 전자통신 사용자에 대한 추정치는 발표 때마다 조금씩 다르지만, 1995 년 초에 인터넷 사용자는 3 천만명으로 추산(Davis, 1995)되었고, 한 달에 160,000 명 꼴로 신규사용자가 증가(Kim, 1994)한다고 보고되었다. 하지만 이러한 수치는 인터넷에 연결되지 않은 기타 통신망 사용자를 포함하지 않은 것으로 판단된다.

이 글은 전자사생활의 실태에 관한 고찰이다. 좀더 구체적으로 말하자면 컴퓨터가 만들어 놓은 환경 속에서 전자통신 및 이와 관련된 커뮤니케이션상의 문제점을 다루고 있다. '보호법'이 1986 년에 통과(U.S.C. 18, §§ 2510-2711)된 이래, 이 법이 과연 전자통신 사용자들의 전자사생활을 충실하게 보호하고 있는 지에 관한 의문이 제기되어 왔었다. 예전엔 연방대법원은 기업의 사용자가 직원의 전자통신 내용을 감시・도청할 수 있는 권리를 인정해 왔다(Simmons v. Southwestern Bell Telephone Company). 하지만 캘리포니아주의 한 판사는 이러한 사용자의 권리를 인정한 법률을 전화 등의 전통적 매체

범위를 벗어나 전자통신에까지 확대 적용하는 데에 반대했다. 그는 전자통신에 대한 판단은 새로운 입법 영역에 속한다고 밝혔다(Lee, 1991).

이 논문에서 우린 전자통신의 사생활이 '보호법' 하에서 어떤 보호를 받고 있는지 규명하려 한다. 우선 현재의 법에 대해서 검토한 다음 '보호법'의 허점을 보여주었던 몇 건의 판례를 검토한 다음, 사례와 관련 문헌의 검토를 통해 현존하는 '보호법'이 사무공간에서 전자통신의 내용에 대한 무제한적인 감시와 절취를 허용하는 허점이 있음을 보여주려고 한다. 전자통신 사용이 확산됨에 따라, 기존의 법률이 기술발달의 속도를 따라가지 못하는 사례가 점차 증가하고 있다. 인쇄매체에 허용되었던 전통적인 보호책을 전자 매체에 단순히 확대·적용시키는 것만으로는 한계가 있음이 많은 사례에서 드러나고 있다. 새로운 커뮤니케이션 기술에 의한 이러한 상황변화에 대해, 입법자는 능동적으로 대응하기보단 수동적으로 반응하는 양상이다.

이어지는 이 논문의 다음 장들에서 다루게 될 내용은 다음과 같다.

1. 전자통신에 대한 개괄적 접근 및 프라이버시의 발전과정에 대한 고찰
2. 전자통신 도청 문제를 다룬 주요 법률 사건을 고찰
3. '보호법'과 전자통신 사생활이 처한 현실 사이의 괴리를 파악
4. '보호법' 제정 뒤의 판례(스티브 잭슨 게임사건을 중점적으로)와 연관 지어 법률의 보완
5. 프라이버시권이 처한 현실과 '보호법' 사이의 괴리를 조정해 줄 여러 관련요인들 하나하나의 중요도를 평가한 다음, 전자통신 사생활을 보호할 대안 제시

## Ⅱ. 전자통신 개관

전자통신에는 '컴퓨터 네트워크를 통한 메시지의 즉각적인 송수신'이란 의미가 담겨있다. 전자통신 사용자들은 자신만의 비밀 암호(password)를 사용하여 중앙컴퓨터에 접속하는데, 때론 가정에서 기존의 전화선과 개인용 컴퓨터를 연결시켜 접속하기도 한다. 중앙컴퓨터와 접속이 되면 전자사서함(electronic mail box)이 놓여진 자신의 계정(account)에 접근한다. 바로 이전자사서함을 이용하여 사용자들은 동일 시스템 또는 다른 네트워크에 속해있는 사용자들과 메시지를 송수신할 수 있다. 전자통신은 저렴한 가격의 대중적인 매체라고 할 수 있다.

가장 큰 규모의 전자통신 시스템인 '인터넷'은, 전 세계에 산재해 있는 수천 수백개의 기관과 기업들을 연결시켜 놓은 것이다. 하지만 각각의 사용자들이 자신만의 주소를 가진다는 점에서, 인터넷 역시 전통적인 우편 체계를 닮았다고 볼 수 있다. 즉, 사용자의 (전자)주소만을 보아도 현재 사용중인 컴퓨터의 소재지를 알 수 있는 것이다. CompuServe, GEnie, Prodigy, America Online 과 같은 '통신서비스' 업체들은 '비영리 시스템'인 인터넷의 접속을 도와주는 컴퓨터 정보 서비스를 운영하고 있다. 그리고 이들 상업적 전송망을 통해 교육이나 연구와는 관련 없는 정보를 전송할 경우에도 역시 사적인, 즉 유료의 접속 서비스를 이용해야만 한다. 통신 사용자들은 인터넷을 통해 수천개의 도서관과 데이터베이스, 그리고 기타 여러 정보제공 기관에 접근할 수 있다(Krol 1994). 사기업의 사내

통신망은 회사 컴퓨터에 의해 움직여지며, 회사의 소유이다. 교육기관이나 공공기관의 컴퓨터는 정부 소유다.

비록 다른 계정으로의 접근은 암호(password)에 의해 제한되어 있지만, '시솝(sysop)'이라 불리는 '시스템 운영자'는 자신이 운영하는 시스템에 속해 있는 모든 계정에 자유로이 접근하여 개인사서함에 저장되어 있는 메시지를 볼 수 있다. 기업체에서도 관리자들은 종업원들이 저장해 놓은 컴퓨터 파일에 접근할 수 있으며, 심지어 종업원들간의 사적인 메시지도 볼 수 있다. 교육기관에서는 시스템 관리자는 통신망에 떠있는 모든 정보를 마음대로 불러내거나 읽을 수 있으며, 교수와 학생들이 주고받는 메시지 뿐만 아니라 다른 기관의 동료연구자 사이에 오가는 메시지도 볼 수 있다. 현행 '보호법'에 의하면, 기업의 사용자나 시스템 운영자들의 이러한 '검열' 행위는 합법적인 것이다. 이러한 검열의 가능성과 잠재성, 그리고 실제로 벌어지고 있는 잘못된 행동과 시스템 운영자의 직권 남용 등의 문제가 전자사생활에 관한 관심을 이끌어 내고 있다. 전자통신과 관련하여 해결되지 않는 수많은 문제점 중 하나는, 컴퓨터 데이터베이스와 전자게시판과 관련한 보다 큰 문제로부터 기인한다. 이들을 어떻게 분류할 것인가? 이들은 출판업자인가, 단순한 컴퓨터 파일 보관창고인가, 뉴스가판대와 비슷한 것인가, 도서관인가, 사적인 회의장인가,공공 전송업자인가, 아니면 이들 중 둘 이상의 조합인가, 이도 저도 아닌 것인가? (Levinson, 1992).

## Ⅲ. 사생활

사생활에 관한 구체적인 언급이 헌법에 명시되어 있지 않지만, 관습법(common law) 상 법적배상을 요하는 사생활 침해 유형은 법률학자들이 대별해 놓은 네 가지로 압축된다. 미국 법학회(the American Law Institute)가 펴낸 '보상받아야 할 불법행위(수정판)'에 따르면, 첫째, 진실이지만 당황스러운 사실의 출판 또는 공포 둘째, 허위 사실 유포와 명예 훼손, 셋째, 절도 넷째, 고독권 침해(혼자 있는 상황의 침입) 등 네 가지 유형이 제시되어 있다 이 중 마지막 네 번째 유형이 전자사생활 침해 사안과 가장 관련이 깊다.

워랜(Samuel Warren)과 브랜다이스(Louis Brandeis)는 1890 년에 Harvard Law Review 에 기고한 '사생활에 관한 권리(the Right to Privacy)'란 논문에서 프라이버시권을 다루었다. 그들은 프라이버시권이 헌법상의 신체적 자유권(혹은 고독권 a right to be left alone)을 규정한 원칙의 일부분으로 내재되어 있다고 주장하였다. 그들에 따르면 프라이버시권은 불가침의 성격을 띠고 있으며, 상업지향적인 신문이나 사진가, 혹은 화면이나 소리를 기록 복제할 수 있는 현대적 기계를 소유한 자들로부터의 예상되는 침해에 대해 개인의 사생활을 보호할 수 있는 원칙을 현행법에도 이끌어 낼 수 있다고 지적하였다.

워랜과 브랜다이스의 견해는 후일 대법원의 판결로 구체화되었으며 결국 프라이버시권을 탄생시킨 밑거름이 되었다. 예를 들어, Roe v. Wade(1973)사건에서 재판부는 "프라이버시권이 헌법에 구체적으로 명시되어 있진 않다. 하지만, 그 동안의 일련의 판결을 통해 법원은 개인의 프라이버시권 혹은 프라이버시에 속하는 영역이 헌법 속에 존재함을 인정해왔다."고 판결하였던 것이다. Griswold v. Connecticut(1965) 사건에서 재판부는,

"권리장전(the Bill of Rights)의 구체적인 보호조항에는 취약한 부분이 있으며, 역설적이지만, 이러한 취약 부분은 바로 보호조항이 존재함에 따라 창출된 것이다. 결국, 다양한 보호조항이 프라이버시의 영역을 창출해낸 셈이다."라고 언급하였다. O'Connor v. Ortega(1987)사건에서 재판부는, "사기업 종업원이 아닌 공무원이라는 이유만으로 한 개인이 '조용히 살 권리(Fourth Amendment rights : 행복추구권)'를 잃는 것은 아니다. 공공부문에 속한 다양한 직종을 감안할 때, 한 사업장의 종사자가 어느 정도의 사생활 보호를 기대할 수 있는 지는 각각의 경우에 비추어 세심하게 판단해야 한다."고 판시하였다. (수정헌법 제 4 조에 따르면, "개인이 부당한 수색이나 압수의 위험없이 자신의 마음 속이나 자신의 거처에 안전하게 있을 수 있는 권리는 침해 당할 수 없으며, 부당한 영장은 발부되어서도 안된다. 만일, 법원과 검사 사이의 정당한 약속하에 합리적인 사유로 영장이 발부된다 하더라도 적시된 장소와 사람 또는 물건에 한해서만 수색이나 압수가 이뤄져야 한다.")

이러한 수정 헌법 제 4 조는 전자사생활 침해를 다룬 재판에 적용되어 왔으며, 아래에 적힌 여러 법원의 판결에서도 논의되고 있다. 이와 비슷한 사례에는 수정 헌법 제 5 조("어떠한 사람도 정당한 법집행 절차에 의하지 않고는 생명이나 자유, 재산을 빼앗겨서는 안된다. 또한 정당한 보상 없이 공공의 목적을 위해 사유재산권이 침해되어서도 안 된다.")가 적용되기도 하였으며, 이에 대한 연방법원의 견해는 수정헌법 제 14 조("모든 주는 미합중국 시민의 특권이나 면제사항을 축소하는 내용을 담은 어떠한 법도 제정 혹은 시행해서는 아니된다. 또한 정당한 법집행 절차 없이 개인의 생명, 자유, 혹은 재산을 강탈해서는 아니되며, 개인이 누릴 수 있는 공평한 법의 보호를 부정해서도 아니된다.")에 의해 각 주에까지 적용되었다.

## Ⅳ. 사 례

### 1. 도청사건과 전자 사생활 침해

과거 몇 년 동안 연방대법원은 주로 개인의 전화 도청과 관련된 사건에서 전자 사생활 침해문제를 다루어 왔다. 이러한 사례는 두 가지로 분류할 수 있는데, 하나는 공권력에 의한 침해이고 다른 하나는 전화도청을 둘러싸고 발생한 개인간의 다툼이다.

연방대법원이 처음으로 다룬 도청 사건은 Olmstead v. U.S.(1928) 사건이다. 이 사건의 쟁점은, 연방주류 단속청 요원들(federal prohibition agents)이 옴스테드의 통화를 도청하여 그의 유죄를 입증할 증거를 찾았다는 사실이었는데, 그는 결국 금주법 위반으로 유죄 판결을 받았다. 옴스테드는 즉각 항소하였지만 법원은, 유사한 사건에서 흔히 볼 수 있는 공권력에 의한 불법수색이나 압수가 없었으며, 도청 행위는 수정헌법 제 4 조에 반하지 않는다는 이유로 그의 항소를 기각하였다. 구체적이고 실질적인 침해가 없었다는 이유만으로, 전화도청의 위법성을 밝힐 수 있는 헌법적 근거를 찾으려 하지 않았던 것이다.

연방대법원은 상기의 판결을 지지하면서, 한편으론 전화 도청을 통해 얻어진 증거를 법정에서 채택할 수 없도록 하는 법률을 의회 차원에서 제정・통과시킬 수는 있다는 입장을

밝혔다. 하지만 정작 법원은, 수정헌법 제 4 조에 대한 확대해석을 기피하였던 탓에 그러한 입장을 취할 수 없었다.

수정헌법 제 4 조에 대한 상기 재판부의 견해와 다른 해석은 거의 40 년이 지난 1967 년 Berger v. New York 사건에서야 나타났다. 이 사건을 다룬 연방 분할 법원(a split Supreme Court)은, 유죄판결의 증거로 사용하기 위해 전화 도청을 인정한 뉴욕주법이 수정헌법 제 4 조 및 제 14 조를 위반하였다며, 도청을 통해 확보된 증거를 근거로 내려진 뇌물 사건에 대한 유죄판결을 뒤집었다. 이사건의 재판부는, 비록 뉴욕주 법이 정도를 벗어난 점은 인정되지만, 법원의 정당한 절차를 밟고 집행된 도청은 원칙적으로 허용할 수 있다는 입장을 밝혔다. 그러나 재판부는 이 사건의 경우 사법 수사관(law enforcement officials)이 이러한 기준을 지키지 못했음을 지적했다.

어떠한 경우라도 법집행의 미명 하에 수정헌법 제 4 조에 적시된 정당한 절차를 생략하여서는 아니 된다. 반드시 지켜야 할 공식적인 규율은 없다 하더라도, 우리에겐 오랜 세월을 거쳐 미국 시민의 기본적 권리로 인정되어온 프라이버시를 보호해야 할 의무가 있는 것이다. 도청 행위는 자유권에 대한 중대한 위협 중의 하나인 것이다.

같은 해 일어난 Katz v. United State(1967)사건에서 법원은, 불법침해 요건은 반드시 물리적인 형태로 발생해야 성립되는 것은 아니라고 판결하였다. 이 사건에서 피고의 유죄를 입증하기 위해 제시된 증거는, 피고의 공중전화 통화내용을 도청・녹취한 것이었다. 연방 요원은 Katz 가공중전화로 도박에 관한 정보를 유출함으로써 연방법을 위반하였다는 요지의 증거를 제시하였다. 이 에 Katz 는 연방대법원에 즉각 항소하였다.

연방대법원은 Katz 에 대한 유죄판결을 번복하면서, 수정헌법 제 4 조의 취지는 장소(places)가 아닌 사람을 보호하는 것이라는 입장을 밝혔다. 비록 수정헌법 제 4 조가 프라이버시에 관한 일반적 권리로 해석되진 않았지만, 정부의 침해로부터 개인을 보호하였던 것이다. 이 판결을 통해 연방대법원은, 수정헌법의 제 4 조의 적용 범위를 공중전화 박스에서 전화를 거는 사람에게까지 확대하였다.

공중전화 박스에 들어가 문을 닫고 동전을 넣고 전화를 거는 사람은 자신의 통화 내용이 세상에 알려지지 않을 것이라고 생각할 권리가 있는 것이다.

재판부는, 도청 장치가 공중전화 박스에 직접적으로 설치되지 않았다는 사실은 위법 여부를 판가름하는 데 있어 중요한 의미를 가지지 못하며, 정부가 전화 도청을 하려면 법원의 영장이 발부되어야 한다고 밝혔다. 이 사건의 경우, 담당요원이 정당한 절차를 밟지 않았으며 따라서 도청행위는 불법이었다고 결론지었다.

United States v. Miller(1976) 사건에 대한 연방법원의 판결은, 수정헌법 제 4 조가 규정하는 사생활의 영역에 은행이 취득한 개인의 정보까지 포함되진 않음을 보여주었다. 위 사건에서, 주류의 불법 유통과 관련하여 정부를 속인 죄로 유죄판결을 받은 피고는, 자신의 유죄를 입증한 증거는 수정헌법 제 4 조를 위반하여 얻어진 불법적인 정보라고 주장하며, 컴퓨터 자료를 포함한 은행의 거래기록을 말소하려고 하였다. 이에 대해 법원은, 은행 거래 내역은 피고의 사생활 영역이라고 볼 수 없으므로, 증거를 얻는 과정에서 발생한 거래 기록의 압수는, 수정헌법 제 4 조에 대한 침해가 아니라고 판결하였다.

법원은, United States v. White 사건을 인용하며, 예금자는 은행에 건네준 자신에 관한 정보가정부기관에 건네질 것이라는 위험을 감수해야 한다고 경고하였다.

본 재판부는, 수정헌법 제 4 조가, 제 3 자에게 누설되거나 스스로의 선택에 의해 정부기관에 넘겨진 정보의 획득마저 금지하는 것은 아니라는 것을 거듭 주장하여 왔다. 비록 그 정보가 애초에 제한된 목적으로 사용될 것이며 신의를 저버리지 않을 것이라는 제 3 자의 약속 하에 공여되었다 할지라도 말이다.

컴퓨터나 여타 매체에 전자적 형태로 저장된 정보에 대한 접근권 문제는 United States v. Davey(1970) 사건에서 재차 거론되었다. 몇몇 관련자들의 신용 내역에 관한 미국세청(Internal Revenue Service)의 내사가 개입된 이 사건에서, 담당 수사관은 사설신용조사기관에 기록 제출을 요구하였다. 하지만 이 기관은 '고객과 맺은 선서(affidavits)에 관한 법률적 문제점'을 제기하며 자료 제출을 거부하였다. 이에 대해 제 2 순회항소법원은 정부측의 손을 들어주며, 정부가 요구하는 모든 정보는 공개되어야 한다고 판결하였다. 정부는 정보의 저장 장소나 저장 형태, 검색 방법에 관계없이 필요하다고 판단되는 모든 정보 제출을 요구할 권한을 가진다고 재판부는 판결하였다.

정부가, 수탁자(depository)에게 정보를 제공하지 않았다는 사실 때문에, 정보를 요구할 수 없는 것은 아니다고 재판부는 말했다. 요구한 자료의 제작에 드는 합당한 요금을 지불하는 한, 정부는 그 정보에 대한 접근권을 가진다고 판결했다.

Simmons v. Southwestern Bell Telephone Company(1978) 사건을 맡은 오클라호마주 서부 연방지방법원은 종업원들의 전화통화를 도청 감시한 이 전화회사의 행위는 1968 년에 제정한 '범죄예방 및 치안유지 관련법(the Omnibus Crime Control and Safe Streets Act of 1968)'(아래에서 논의될 것임) 제 3 항에서 규정한 예외 조항에 속하므로 아무런 문제가 없다고 판결하였다. "프라이버시권에 대한 헌법 차원의 보호는 우리 법체계에서 비교적 새로이 등장한 사안이라고 본다. 때문에, 어떤 근거로 프라이버시권이 제기되었든지 간에, 그것이 개인의 사생활에 대한 정부의 침해가 발생했을때만 보호해야 한다고 생각한다."는 것이 이 사건을 맡은 재판부의 견해였다.

이와 비슷한 사례로 Briggs v. American Air Filter Co., Inc. (1980) 사건을 들 수 있는데, 여기서도 재판부는 통화내용을 도청・감시한 사용자의 행위를 무죄라고 판결하였다. 이 사건의 내막을 살펴보면, 사용자 중 한 사람이 경쟁 관계에 있는 회사에 기밀사항을 누설하는 두 종업원에게 누차 경고해왔다고 한다. 일상적인 업무시간 동안, 그 사용자는 내선전화(extension phone)를 통해 자신의 의심에 확신을 가질 만큼 충분히 그들의 통화내용을 엿들었고, 이 사실을 안 두 직원은 '범죄예방 및 치안유지 관련법'의 도청 금지조항을 어기고 자신의 프라이버시를 침해하였다는 이유로 소송을 제기했다. 하지만 결과는 패소였다. 재판부의 판결 요지는 다음과 같다. 이 사건의 피고(사용자)는 내선 전화를 통해 통화를 엿들었으며, 내선전화를 통한 도청은 '범죄예방 및 치안유지 관련법' 상의 도청행위에 속하지 않으며, 그러므로 위법 사실은 인정되지 않는다.

위에서 논의된 사항을 요약하면 다음과 같다.

ⅰ) 연방대법원은 프라이버시에 관한 일반적 권리가 도청에 대해서도 적용된다는 사실을 인정하였으며, 동시에 적법한 절차를 밟아 영장을 발부 받은 법집행 기관은 도청을 할 수도

있음을 인정하였다. ⅱ) 정부는 자료의 저장 형태 및 장소에 관계없이 모든 정보에 대한 접근권을 가진다. ⅲ) 개인은 타인(예컨대 은행과 같은)이 가지고 있는 자신에 대한 정보를 소유할 수 없으며, 따라서 이러한 정보에 대해 개인의 프라이버시권을 주장할 수 없다. ⅳ) 근무중인 경우, 사용자는 직원의 통화 내용을 사적인 것이라 할지라도 감시할 수 있다. v) 이미 발견된 이러한 미비점에 대해 의회는 전자사생활 보호를 한층 강화시킨 법안을 제정・통과시켰다.

## 2. '전자사생활 보호법'

통신과 컴퓨터 기술에서 일어난 변화에 부응하기 위해, '전자사생활 보호법' (the Electronic Communications Privacy Act of 1986)이 1986 년에 통과되었다. 이 법은 1968 년에 제정되었던 '범죄예방 및 치안유지 관련법' 제 3 조를 수정한 것이다(공법 99-508). 입법 배경을 살펴보면, 전자통신 기술의 급격한 변화로 인해 수정헌법 제 4 조의 영역을 가택 등에 대한 부당한(unwarranted) 압수・수색을 제한시킬 수 없게 된 것이 주된 이유였다. 새로운 사생활 침해 기법의 발달로 생겨난 위협에 대항할 수 있는 새로운 법안이 필요했던 것이다.

'보호법' 이전의 법안인 '범죄예방 및 치안유지관련법' 제 3 조는, 대법원이 수정헌법 제 4 조의 연장선상에서 기초하였으며, Katz 사건에서 문제되었던 전자 도청 문제를 다루고 있다. 이 법의 제 3 조(Title Ⅲ)는 정부의 전화통화 도청 권한에 제한을 두었다. 비록 그 법안이 씌여진 시대에는 드러나지 않았지만, '범죄예방 및 치안유지 관련법'의 허점은 음성으로된 도청 행위만을 문제 삼았고, 전화선과 같은 공공망을 사용했을 경우만 제재 대상으로 포함했다는 점이다. 그 결과 점차 성장하는 비음성, 디지털 형태의 통신 행위는 보호할 수 없었다. 본질적으로 1967 년에서 1986 년 사이의 프라이버시 관련 법안은 '들을 수 있는 것'만을 보호했다고 볼 수 있다.

'보호법'은 기술진보로 인해 생긴 법과 현실의 괴리 상황에 대해 문제가 제기되고 있다. 컴퓨터,무선 및 휴대 전화의 대량 보급, 그리고 통신망에서의 정보 가로채기 기술의 발달은 그로 인해 생겨난 폐해에 대한 적절한 조치를 요구하였는데,이러한 상황을 가리켜 의회는 "개인 및 사업정보를 보호하는 미국의 역량 손실"로 표현하였다. 특히 의회는, 신기술 평가를 담당하는 집행부서인 기술평가국(Office of Technology)이 1985 년 10 월에 내놓은 보고-"전자통신에 대한 보호조치는 약하고 모호하거나 거의 존재하지 않는다."-내용에 주목하였다.

음성통신 영역은 '범죄예방 및 치안유지 관련법' 제 3 조에 의해 보호받고, 일급 우편물은 '미우편법'에 의해 보호되었지만, 전화선과 같은 공공망을 이용하지 않는 새로운 형태의 통신은 연방법 차원의 보호를 전혀 받지 못하였다. 의회는 각종 침해로부터의 보호 부족으로 잠재적인 통신사용자들의 일부가 사용을 꺼리는 대신 불법 사용자수가 확산되지 않을까 두려워하였다. 의회는, 이러한 상황에서 제정된 '보호법'이 시민의 프라이버시권과 정부의 정당한 법집행 필요를 조화롭게 해줄 것이라고 믿었다.

'보호법' 제정에 모종의 타협이 없었던 것은 아니다. 최종법안의 많은 조항들은, 법집행 기구가 아닌 바로 연방정부의 '음성・정보통신 도청 능력'을 위험에 빠뜨리지 않기 위해

미법무성의 공조하에 초안이 기초되었다. '범죄예방 및 치안유지 관련법' 제 3 조에 포함되지 않은 몇몇 조항이 '보호법'에 구체화 되어졌다. 한 개인이 전화 도청의 대상임을 본인에게 알려주는 것을 범죄로 취급하는 부분이 포함된 것이다. 그 법은 또한 외국전자통신 시스템과 관련, 정부의 해외정보활동에 대해서는 현상 유지를 지켜 주었다.

'보호법'의 가장 중요한 특징은 디지털화된 통신 내용(혹은 자료)의 도청을 불법으로 간주하고 있음을 구체적으로 명문화 하였다는 데 있다. 나아가 이 법은 전자적 형태로 저장된 메시지에 대한 불법적 접근을 금지함으로써 정보가 저장된 컴퓨터시스템은 보호하지만, 공중에 의해 일반적인 접근이 가능한 시스템은 보호대상에서 제외하였다. 그리하여 '보호법'은 사적인 시스템은 보호하고, 공적인 시스템은 보호대상에서 제외하였다.

'보호법'에는, 시스템 공급업체의 직원들이 자사 시스템 상의 통신내용을 엿듣거나, 가로채거나, 폭로할 수 있도록 한 중요한 예외조항들이 포함되어 있다. 이 법에 따라 통신내용을 폭로할 수 있는 경우는,

- 발신자 혹은 수신자의 합법적 동의를 얻은 경우
- 회사 종업원이거나 허가를 받은 사람의 경우, 혹은 통신설비의 소유주인 경우
- 서비스 제공자가 고의성 없이 정보를 획득한 경우, 혹은 법 집행기관이 범죄와 연관되어 있다고 판단하여 의도적으로 통신내용을 폭로할 경우

예외조항을 기초하면서 미하원 사법위원회(the House Judiciary Committee)는, 시스템운영자가 자기 시스템에 대한 불법적 행위의 증거를 찾는다며 무분별하게 사용자들의 통신내용을 검색하는 행위는 용납되지 않는다고 경고했다.

반면, 또 다른 조항에서는 시스템운영자가 시스템 운영상의 서비스 정도와 수준을 체크하기 위해 통신내용을 감시하는 것을 허용하고 있다.

§ 2518 조항에 따르면, 정부는 수색영장을 발부 받은 후에, 정보의 저장 기간에 관계없이 시스템운영자에게 비음성통신 기록 제출을 요구할 수 있다. 대부분의 경우 판사는 일방적으로 결정을 내릴 수 있다. 즉, 영장발부 사실을 사전에 시스템운영자나 이용자에게 알려줄 필요가 없다는 뜻이다. 그러나, 국가안보에 위협을 가하는 "긴급상황"이 발생하였거나, 조직 범죄가 연루된 경우에는 영장발부 이전에도 도청이 허용된다. 또한, 이러한 예외적 상황이 발생하였을 경우에 시스템운영자는 자신이 운영하는 시스템의 통신내용을 감시하거나 때로는 폭로할 수도 있다.

이 밖에도 '보호법'의 다른 조항들은 전자통신에 관한 광범위한 사항을 포함하고 있는데, 그 중에는 펜 레지스터(Pen Register :통화를 나눈 전화번호를 계속 기록하도록 고안 되어진 장치)사용을 합법화한 것과 무선전화통화의 radio portion 에 대해서는 통화내용 절취를 허용하는 부분도 들어있다. '보호법'을 위반할 경우 최고 5,000 달러의 벌금과 6 개월 금고형에 처해지며, 상업적 이익을 얻기 위해 법을 위반할 경우에는 최고 250,000 달러의 벌금과 1 년 금고형이 부과된다. 재범인 경우 형량은 증가한다.

## Ⅴ. '전자사생활 보호법' 제정 이후의 상황

### 1. '전자사생활 보호법' 제정 이후

'보호법'이 1986 년에 제정된 이후, 자신의 전자통신 내용을 누군가가 읽어 프라이버시가 침해되었다고 주장하는 일련의 고소 사건이 발생했다. 이 중, 한 사건을 제외하고는 모두 기각, 철회되었으며, 미제 사건으로 남은 것도 있다. 최종판결이 난 한 사건은, 엡슨(Epson)사의 전자 통신 담당 관리자였던 쇼어즈(Alana Shoars)가 제기한 집단소송 사건이었다. 쇼어즈는, 회사 임원 중 누군가에 의해 종업원들의 전자통신 내용이 일상적으로 감시・도청되고 있음을 발견한 직후 자신이 해고되었다고 주장하였다. 쇼어즈는, 회사의 전자통신을 관리하면서 종업원들의 전자 통신상의프라이버시는 인정되며, 회사 시스템상 어떤 침해로부터도 안전하다는 경영진의 말을 들어왔었다고 진술했다.

전자통신 감시 사실을 인지한 후 그녀는, 도청사실을 무시하고 직장을 계속 다니든지 도청을 막으려다 직장을 잃든지, 둘 중 하나를 선택하라는 강요를 당했다고 한다. 그로부터 얼마 후 그녀는 해고당했다. 그러나 엡슨사는 그녀의 해고가 '전자통신 도청' 또는 '프라이버시' 문제와 아무런 관련이 없다고 주장하였다

쇼어즈는 엡슨사를 상대로 잇달아 두 개의 소송을 제기하였다. 그 회사가 캘리포니아 주법이 보장하는 프라이버시권을 침해하였다는 것이 소송 이유였다. 두 개의 소송 중 하나는, 그녀와 700 명의 엡슨사 종업원의 프라이버시권이 침해 당한 것에 대한 집단소송이었으며, 다른 하나는 그녀에 대한 부당한 해고와 관련된 것이었다. 그녀가 소송의 근거로 삼은 캘리포니아 주법에 따르면, 관련 당사자의 동의 없이 행해지는 도청이나 기밀사항 복제는 불법이었다.

1990 년 6 월, 캘리포니아 고등법원의 쿠퍼먼(Barnet M. Cooperman) 판사는 엡슨사를 상대로 한 집단소송을 기각하였다. 그는, 캘리포니아주법은 전신과 전화 도청을 금지하고 있을 뿐, 전자통신은 도청 보호 대상이 아니라고 기각 사유를 밝혔다. 프라이버시와 관련된 현행법을 전자통신과 같은 새로운 통신기술의 발달로 초래된 상황에까지 확대 적용하는 것은 입법의 영역이지법원이 해야 할 일은 아니라고 말했다.

1991 년 1 월, 닛산 자동차 회사에 근무하는 두 명의 정보시스템 종업원이 캘리포니아주 법원에 소송을 제기하였다. 소송 이유는, 회사가 자신들의 전자통신 내용을 절취하거나 도청함으로써 자신들의 프라이버시권을 침해하였다는 것이었다.

이 도청 사건으로 말미암아, 한 사람은 해고당하였고, 또 한 사람은 강제 사직 당하였다. 하지만이 사건은 법원 밖에서 사적으로 해결되었다.

1988 년 3 월에 일어난 Thompson v. Predaina 사건은 전자게시판 운영자가 전자통신 사생활을 침해함으로써 발생하였다. 이 사건에서, 법대 3 학년인 린다 톰슨은, '전문가의 선택'이란 전자게시판을 운영하는 '시솝' Bob Predaina 를 상대로 소송을 제기하였다. 톰슨은 Predaina 가 자신의 허락 없이 자신의 전자통신을 침해하였다고 주장하였다. 인디아나주 남부 연방지방법원에 제기된 이 소송은 '주법'과 '보호법'을 동시에 관련 근거로 내세웠다. 하지만 이 사건도 원고가 자발적으로 소송을 철회하는 것으로 종결되었다.

앞서 기술한 바와 같이, 이 시기에는 어떤 식으로든 판례 또는 판결 지침을 확립했었어야 할 사건들이 유야무야 종결되는 것이 대부분이었다. 판결을 내리고 싶어도 마땅한 선례가 태부족인 상황은 1993 년에 이르러서야 비로소 변화의 기회를 맞게 된다.

## 2. 스티브 잭슨 게임사 사건

Steve Jackson Games Incorporated, et al., v. United States Secret Services, United States of America, et al. (1993)사건에 대한 판결은 '보호법'과 관련한 새로운 법적 토대를 마련해 주었다. 이 사건의 담당 재판부는, 컴퓨터 통신상의 전자게시판에 전자적 형태로 저장된 정보에 대한 정부의 압수 행위는 '보호법'을 위반한 것이라고 판결하였다.

1990 년 3 월 1 일, 잭슨 게임사의 한 직원이 벨사우스(Bellsouth)사의 소프트웨어 도난 사건에 연루되었다고 판단한 미연방비밀조사국(U.S. Secret Service) 요원들은 텍사스주 오스틴시소재의 회사사무실에 대한'수색 영장'을 발부 받았다. 그 결과, 세 대의 컴퓨터를 압수하였으며, 그 중 한 대는 전자게시판 서비스에 이용되던 것이었다. 컴퓨터와 관련된 소프트웨어도 함께 압수되었다.

이 수색은, 비밀조사국 요원들이 벨사우스사의 '911 비상체계 관련 서류' 도난 사건에 관한 정보를 입수하는 방편으로 행해졌다. 도난 당한 벨사우스사 소유의 서류 파일은, 전국에 걸쳐 다수의 전자게시판에서 발견되었는데, 그 중 하나가 잭스 게임사 종업원이 운영하는 것이었다. 비밀조사국이 발부 받은 잭슨 게임사 수색 영장에는, 911 프로그램 관련 서류뿐만 아니라 암호해독 프로그램과 여타 관련 인사들까지 수색 대상으로 명기되어 있었다. 압수와 몇 차례의 추가 수색에도 불구하고 아무런 혐의점이 발견되지 않았다.

잭슨 게임사는, '전자사생활 보호법'을 비롯한 세 가지 법에 대한 위반 혐의로 비밀조사국과 미연방정부를 법원에 제소하였다. 잭슨 게임사는 소장을 통해 비밀조사국의 위법 행위로 인해 회사가 금전적 손실을 입었다고 주장하였다. 압수된 장비가 넉 달이 지난 후에야 돌아오긴 했지만, 그 동안 잭슨 게임사는 두 명의 간부 직원을 일시해고(lay-off)시켰고 출판 예정일이 지연되었으며, 수입 손실도 입었다. 또한 비밀조사국의 조사과정에서 몇몇 컴퓨터 파일들이 말소되기도 하였다고 잭슨 게임사는 밝혔다

연방지방법원 판사인 스팍스(Sam Sparks)는, 비밀조사국 패소 판결을 내리면서, 만약 요원들이 잭슨 게임사에 대한 조사를 했었다면, 그들의 시스템 운영에 아무런 하자가 없었다는 것을 알았을 것이라고 말하였다. 스팍스 판사는, 요원들과 동행한 컴퓨터 전문가들이 단 몇 시간만에 모든 파일을 복사할 수 있었기 때문에, 컴퓨터 파일과 장비를 압수할 필요는 없었다고 덧붙여 지적하였다. 스팍스 판사는, 비밀조사국 요원들이 밟은 압수 수색 절차는, 법원의 허락 없이 행해지는 침해로부터 컴퓨터 시스템과 자료를 보호하기 위해 고안된 '보호법'의 관련 규정을 위반하였다고 말했다. 그들의 행위는 법이 설정한 정부의 권한을 넘어선 것이었다.

기술적으로 전자통신 내용에 대한 절취 행위가 발견되진 않았지만, 요원들이 이용자들간의 전자통신 내용이 저장된 컴퓨터를 압수한 것 자체가 '보호법'을 위반한 것이라고 말했다. 스팍스 판사는, 비밀조사국에서 이용자들의 전자통신내용을 알 수 있는 유일한 방법은 '보호법'에 규정된 절차를 지키는 것 뿐이라고 말했다.

스팍스 판사는, 비밀조사국의 불법 행위는 마땅히 법 아래 보호받아야 될 재산, 상품, 사업 정보, 회사 서류, 그리고 한 회사와 네 명의 시민의 전자통신 내용을 압수하는 결과를

초래했다고 말하며, 피고는 원고에게 5 만달러 이상의 손해배상을 하라고 판결하였다. 또한 스팍스 판사는, 자신의 판결이 컴퓨터 범죄를 막으려는 정부의 노력에 미칠 영향을 인정하면서도, 법원은 사생활 보호와 관련된 법을 자의적으로 수정하거나 개정할 입장이 아니라는 의견을 밝혔다. 다른 판결을 기대한다면 비밀조사국 요원들은 먼저 의회로 가야 할 것이라고 말했다. 그는, 비밀조사국에 대해 요원들의 철저한 교육, 철저한 조사, 관련법의 철저한 준수를 주문하였다

## V. 결 론

### 1. 암호화

'보호법'과 현실의 괴리를 줄이기 위해서는, 관련 당사자의 상충되는 이해를 조화시키는 것 뿐만 아니라 통신기술 상의 다양한 발전에 대한 충분한 고려가 필요하다.

전자통신 사생활 보호에 관한 사회적 관심이 고조되면서, 통신 내용이 손쉽게 절취되거나 누군가에 의해 조작되는 것에 대한 걱정도 높아가고 있다. 이런 관심과 걱정에 부응하여, 소프트웨어 기술자들은, 정부 기관을 포함한 그 어떤 이도 전자통신 내용을 엿볼 수 없도록 하는 정교한 프로그램을 고안하였다. '암호화 프로그램'이라고 알려진 이 장치는, 특별한 열쇠(special key)를 가진 해당 수신자만이 암호를 풀고 내용을 읽을 수 있으며, 만약 다른 이가 그 내용을 읽으려 한다면 즉시 분절적인 암호들로 해체되도록 고안 되었다. 특수 디지털 처리된 서명 암호(signature codes)를 통해 메시지 발신자가 사기꾼이나 방해꾼이 아닌 메시지의 원작자임을 알 수 있도록 해주었다. 기종이 다른 컴퓨터와도 호환되는 다수의 프로그램이 상품으로 나와있는 상태며, 한번에 한해 무료로 전송 받을 수도 있다. 하지만, 이런 암호화 프로그램의 자유로이 유통되기까지는 논란도 적지 않았다.

미국가안전보장회의(the National Security Agency; NSA)와 미연방수사국(FBI)은, 새롭게 등장한 정교한 '암호화 프로그램'들이 자신들의 해독 능력 밖에 있다는 이유를 들어 이 프로그램의 시중 유통에 강력히 반발하였다. 정부는, 암호화 기술의 사용이 널리 확산될 경우, 법집행이나 국가안전보장의 목적으로 전자통신을 도청하는 것 자체가 불가능해질 것을 우려하였다. 연방정부가 나서서 두 개의 암호화 프로그램 수출을 막으려고 했던 적도 있었다. 하나는 'ViaCrypt of Phoenix 사'가 개발한 것이고, 다른 하나는 텍사스주 오스틴시에 위치한 'Austin Code Works 사'가 개발한 제품이었다. 또한 미 국가안전보장회의는 적대국가의 정부나 테러리스트들에 대한 감시 능력을 지키기 위해서라도 암호화 기술 수출에 제한을 가할 필요가 있다고 주장하기도 했다. 정부의 수출 저지 노력에 반대하는 사람들은, 정부의 행위가 정상적인 경제 활동을 방해할 뿐만 아니라, 출판의 자유를 보장한 수정헌법 제 1 조에 저촉된다고 주장하였다(현재, 미국 대배심원단은 암호화 기술 판매에 대한 조사를 벌이고 있다).

암호화 기술에 대한 논쟁은 해를 거듭할수록 가열되었고, 클린턴 행정부가 1993 년에 내놓은 제안으로 새로운 국면을 맞이한다. 클린턴 행정부는, 암호화 기술에 관한 국가적 표준을 만들자고 제안하였다. 이 제안에서 클린턴 행정부는, 표준형의 '클리퍼 컴퓨터

칩(clipper computer chip)'을 사용해 스크램블 처리된 음성과 데이터를 암호화·해독하고, 두 명의 독립적인 법정 대리인(escrow agents)를 두어 만능열쇠(universal key)를 맡기자고 제의하였다. 그리하여, 도청에 대한 법원의 허가가 나면, 열쇠를 가진 사람은 정해진 암호화 코드를 확인한 다음, 법집행 기관에 열쇠를 전송해 주어 도청한 메시지를 해독할 수 있게끔 한다는 것이다. 이 제안에 대한 반대자들은, 법안에 명시된 두 명의 법정 대리인은 행정부에 소속된 '국가 표준 기술 연구소(the National Institute of Standards and Technology; NIST)'와 재무성(the Treasurry Department)에 소속되어 있기 때문에 독립성이 보장되지 않는다고 주장하였다. 클린턴 행정부는 1994 년 7 월에 그 제안을 철회하였다.

이상에서 한 가지 분명히 알 수 있는 사실은, 암호화 기술 그 자체만으론 '전자통신 사생활 보호'라는 복잡한 문제를 궁극적으로 해결할 수 없다는 것이다. 결코 깨뜨릴 수 없는 암호화 코드사용이 보편화 되어지면, 최근에 미연방수사국(FBI)이 '아메리카 온라인'을 통해 유아 포르노물을 배포한 사람을 전자사서함 수색을 통해 일망타진한 것과 같은, 정당한 법집행 노력을 움츠려 들게 할 것이다. 하지만 같은 차원에서, 정부가 원할 때마다 만능열쇠를 사용하여 개인의 프라이버시를 침해할 수 있도록 한다면, 미국 시민의 프라이버시권 보호 수준은 후퇴할 것이다.

## 2. 제안된 해결책

전자통신 사생활과 관련된 논쟁을 통해 두 개의 상충된, 경쟁하는 이해관계가 등장하였다. 하나는, 정부와 시민(private citizens) 사이의 대립된 이해로서, 둘 사이의 균형이 반드시 필요하다. 또 다른 하나는, 이 역시 균형관계가 요구되는데, '시민 대 시민이 아닌 다른 개인과 기업' 사이의 대립된 이해다. 이 각각에 대해선 서로 다른 법률적 접근이 필요할 것이다.

시민들의 프라이버시 보호 요구와 정부의 정당한 법집행 사이의 균형을 맞추려고 한다면, 현재의 수정헌법 제 4 조를 창의적으로 해석·적용하는 것으로 충분할 것이다. 최근에, 미공군 형사항소법원이 프라이버시 관련 사건을 해결하는 과정에서 보여준 접근 방법은, 연방 재판체계에 도입할 만한 가치가 있어 보인다.

United States v. Maxwell(1995) 사건에서 군사법원은, 보통군사재판에서 네 가지 '서비스 신용저하 행위'로 군법 제 134 조를 위반한 혐의가 인정돼 유죄판결을 받은 한 고위급장교(officer)에 관한 판결을 내렸다. 맥스웰(James A. Maxwell Jr.) 대령은 연소자의 적나라한 성행위를 담은 파일을 전자통신을 통해 '아메리카 온라인'에 전송했다는 죄목으로 유죄 판결을 받았다. 그러자, 맥스웰 대령은, 아메리카 온라인 상의 자신의 전자통신 사서함으로부터 유죄를 입증할 증거를 압수한 행위는 수정헌법 제 4 조에서 보장한 프라이버시권을 위반한 것이라고 주장하며, 항소하였다.

군사법원은 Smith W. Maryland(1979) 사건에 대한 연방대법원의 판결로부터 유래된 '두 갈래시험(two-prong test)' 방법을 원용하여 이 사건을 다루었다. 담당 재판부는, 수정헌법 제 4 조를 근거로 프라이버시권을 주장하는 사람들은,

첫째, 실제적으로 보호받고자 하는 프라이버시 영역을 제시하여야 하며

둘째, 개인이 보호받고자 하는 프라이버시 영역은 그가 속한 사회로부터 합리적임을 인정받을 수 있는 것이어야 한다.

라는 내용의 판결기준을 제시 하였다.

이에 근거하여 군사법원은, 수정헌법 제 4 조에 보장된 피고(맥스웰 대령)의 프라이버시권이 박탈되어왔다는 것은, 사회에 의해 합리적인 것으로 받아들여질 수 있는 프라이버시권을 정부가 항상 침해해왔음을 의미한다고 지적하였다. 이로써 이 사건의 재판부는 아래와 같은 중요한 발견을 한 셈이 되었다.

일반적으로 정보통신 서비스의 가입자들의 전자메시지 전송은 수정헌법 제 4 조에 의한 보호대상에 속하며, 서비스 이용자들은 실제적이고 정당한 프라이버시 보호를 기대할 수 있다.

더군다나, 재판부는 우리 사회가 상기한 수준의 프라이버시 보호는 논리적으로 당연한 것으로 받아들일 준비가 되어 있다고 말하며 다음과 같은 판결 이유를 밝혔다. "오늘날과 같이 통신커뮤니케이션이 발달한 시대에, 한 사회는 앞서와 같은 프라이버시권에 대한 기대를 합리적인 것으로 인정해야 한다. 재판부는 '보호법'이 이미 그와 같은 권리를 명백히 인정하고 있음을 믿는다. "

이와 같은 전자통신 프라이버시권을 인정한 상태에서 정부는, 사법권을 가진 행정장관(magistrate)이 특정 전자사서함에 대한 수색을 통해 범죄 사실을 가릴 수 있고 그 이용자가 범죄를 저질렀음을 밝힐 수 있는 개연성이 있다고 인정한 경우에만 프라이버시권을 침해할 수 있는 것이다.

맥스웰 사건에서 재판부는 수색 영장의 타당성을 인정하였으며 따라서 맥스웰에 대해 유죄판결을 내렸다. 하지만 이 사건이 프라이버시 관련사건에 진정으로 기여한 바는, 법원이 전자통신이용자들의 헌법에 보장된 프라이버시권을 인정하였다는 점이다. 프라이버시권에 대한 법원의 이러한 '인정' 사례를 미연방 재판 체계에 채택한다면, 개인의 전자통신 프라이버시권과 정부의 정당한 법집행이라는 상충하는 이해를 성공적으로 조정할 수 있는 데 까지 나아갈 수 있을 것이다.

정부의 침해로부터 뿐만 아니라, 다른 개인이나 기업에 의한 침해로부터 전자통신 메시지를 보호할 수 있는 또 다른 법적 수단이 반드시 강구되어야 한다. 주에서 통용되는 관습법 상의 손해배상 영역은 너무 파편적이고 전자통신의 영역으로부터 너무 멀리 떨어져 있기 때문에, 거기에 전자통신 프라이버시 보호에 관한 실질적인 기대를 거는 것은 무리한 일이다. 실질적으로 가능한 해결책은, 일반 우편물에 대한 우편 규정(postal regulations)에 전자통신물까지 포함하는 방향으로 규정을 개정하는 것이다. 통신방해 행위에 대해 규정하고 있는 'U.S.C. 18 §1702'에 따르면, 타인의 기업이나 비밀을 몰래 엿보는 행위 및 타인의 우편물을 당사자가 보기도 전에 개봉・절취 소실하는 것은 불법이라고 되어있다. 여기서 이 법이 보호하는 우편물은, 우체국이나 공인된 장소에 저장 중이거나, 우편배달부의 수중에 있는 것에만 한정된다. 이 법의 영역을 전자통신에까지 확장한다면 컴퓨터 시스템과 디스크 드라이브, 터미널 등 메시지가 보관된 모든 것을 포괄하게 될 것이다. 이러한 법의 확장은 전자통신 사용자들이 현재 안고 있는 많은 프라이버시 문제를 해결해 줄 것이다.

'전자통신'을 우편물에 비유하는 것에 대해 의문을 제기할 사람도 있을 것이다. 그들은, 전자통신은 프라이버시권에 대한 기대가 낮은 '우편엽서'나 '벽보 게시 행위'와 비견할 수 있으며, 따라서 프라이버시에 대해서는 보다 낮은 수준의 보호 대책으로 충분하다고 생각할 것이다. 하지만, 전통적으로 전자통신 사용자들의 프라이버시에 대한 기대치는 일반 우편 사용자들과 매우 비슷한 양상을 보여왔다. 일반 우편 사용자들은, 그들의 편지 내용이 비밀 보장을 받는다는 일반적인 가정하에 편지를 주고 받는다. 전자통신을 보다 낮은 프라이버시권이 적용되는 개념으로 바꾸는 것은, 그 내용을 모든 사람들이 본다 해도 아무런 의미 또는 가치가 없는 것으로 전자통신의 지위를 떨어뜨리는 결과를 낳으며, 보편화 추세에 있는 전자통신의 유용성을 현저히 훼손시킬 것이다.

이 글에서 제시한 프라이버시 보호 대책과 합치하든 혹은 다른 법률의 조항과 일치하든 간에, 새로이 등장하는 통신수단인 전자통신을 반드시, 하루바삐 현재의 법체계 속으로 끌어 들여야 할 것이다. 일관된 조치가 취해지질 않을 경우에는, 21 세기의 가장 효율적이고 유용한 통신 수단으로 급속히 발전할 수도 있을 통신 수단의 확산을 제한하거나 수단 자체의 성격을 바꾸는 결과를 낳을지도 모른다.