

패킷감청의 문제점과 개선방안에 대한 토론회

일 시 • 2010년 2월 1일(월) 오전 10시

장 소 • 국회의원회관 소회의실



민주당
DEMOCRATIC PARTY

국회의원 우윤근 · 박영선 · 변재일 · 정책위원회

목 차

패킷감청의 문제점과 개선방안에 대한 토론회

1. 진행순서	1
2. 인사말	3
3. 발제문	
* 오동석 교수 (아주대 법학전문대학원) - 패킷감청의 헌법적 문제점	11
* 임종인 교수 (고려대 정보보호대학원) - DPI 기술 활용 민간 관심기반 광고서비스의 문제점 검토	33
4. 토론문	
* 권정호 (민주사회를 위한 변호사 모임)	49
* 이강신 단장 (한국인터넷진흥회)	
- 온라인 맞춤형 광고 가이드라인 제정 추진 현황	55
* 오길영 박사 (민주주의 법학 연구회) - 패킷감청의 헌법적 문제점	61
* 장여경 (진보네트워크센터 활동가) - 패킷 감청과 통신의 비밀	67
* 구태언 변호사 (김앤장 법률사무소) - 온라인 맞춤형광고(OBA)에 대한 입장 ..	75

진행 순서

1부

1. 국민의례
2. 내빈 소개
3. 발제자 및 토론자 소개
4. 인사말 및 축사

2부

1. 기술적 시연
2. 발표 및 토론
3. 폐회

인 사 말

국회의원 우윤근(민주당 원내수석부대표)

우리 헌법 제18조에서는 “모든 국민은 통신의 비밀을 침해받지 아니한다”고 규정함으로써 통신의 자유를 보장하고 있습니다. 이러한 통신의 자유는 모든 인간의 기본적 권리입니다. 통신비밀보호법에서 엄격한 요건을 정하여 통신의 자유를 제한하는 것도 이러한 이유에서입니다.

그러나 패킷감청이 가능해짐으로써 전기신호 형태로 흐르는 패킷(packet)을 제3자가 중간에 가로챌으로써 당사자도 모르게 같은 내용을 실시간으로 들여다볼 수 있게 되었습니다. 이 사용자가 인터넷에 접속하여 무엇을 보고 어떤 글을 남기는지, 어떤 전자우편을 보내고 받는지, 메신저로 어떤 대화를 나누는지 등을 정보기관이 실시간으로 들여다볼 수 있습니다.

또한 컴퓨터와 연결되는 통신회선을 감청하는 것이기 때문에 혐의자 외에도 그 컴퓨터를 이용하는 사람이라면 누구나 다 감청을 당할 수 있습니다. 작년 남북공동선언 실천연대에서 패킷감청을 당했다는 주장이 제기되면서 패킷감청이 충분히 가능하고 문제가 심각하다는 사실이 밝혀졌습니다.

패킷감청은 대상자가 누구인지를 불문하기 때문에 패킷감청이 통비법상 허용되는지부터 큰 문제가 아닐 수 없으며, 설사 패킷감청을 했다 하더라도 정보기관이 지득한 정보가 대상자 이외의 다른 사람의 정보인 경우 정보기관이 폐기하는지, 또는 어떻게 활용하는 것인지 알 수가 없습니다.

감청이란 혐의가 있는 수사대상자에 한정하되 통신비밀보호법에 정한 절차에 따라 실시되어야 한다는 것은 부언의 여지가 없습니다. 절차의 문제를 따지기 이전에 감청대상이 과연 감청을 받아야 하는 사람인지에 대한 문제가 무엇보다 우선된다고 볼 수 있습니다. 패킷감청에서 문제가 되는 것은 바로 절차의 문제 이전에 감청의 대상 자체에 대한 문제에서부터 시작되는 것입니다.

따라서 무분별하게 패킷감청이 이루어지지 않도록 하고, 정보기관이 감청자료를 무분별하게 활용하는 것은 입법적으로 엄격하게 통제되어야 합니다.

우리나라의 경우 외국과 달리 감청에 대해 수사기관의 처분과 재량에 맡겨두고 있는 경향이 매우 강합니다. 감청 과정이나 그 후 법원이나 국회가 감독할 제도적 장치가 전혀 없다고 하여도 과언이 아닙니다. 법제도 보완이 반드시 필요한 부분이라고 할 수 있습니다.

오늘 이 토론회가 패킷감청에 대한 문제점과 대안을 모색할 수 있는 귀중한 자리가 되리라 믿습니다.

감사합니다.

인 사 말

국회의원 박영선(법사위원, 정보위 간사)

안녕하십니까? 민주당 박영선 의원입니다.

우리나라 초고속 인터넷은 1999년 처음 상용서비스를 시작한 후, 10년만에 가입자수가 1,600만명을 넘어 가구당 보급률이 97%에 달하고 있습니다. 그리고 인터넷으로 가능한 서비스도 검색, 웹서핑, 이메일, 블로그, 카페, P2P다운로드, 메신저, 인터넷뱅킹, 인터넷 (화상) 전화, 트위터, 인터넷 TV 등 계속 발전하고 있습니다. 인터넷 강국답게 인터넷뱅킹 고객수와 인터넷전화 가입자 수도 증가하고 있습니다.

나아가 스마트폰의 출현으로 휴대폰으로도 자유롭게 무선 인터넷에 접속할 수 있게 되었고, 스마트폰 가입자수도 계속 늘어날 전망입니다.

우리 국민 대부분이 시간, 장소 제한을 받지 않고 인터넷 생활을 하고 있다는 말입니다. 과학기술의 발달로 상상만 했던 일들이 현실이 되어 가고 ‘멋진 신세계’가 펼쳐지고 있습니다.

그러나 2009년 8월, 국가보안법 위반 혐의로 기소된 피고인이 ‘인터넷 패킷감청’을 당했다는 사실이 언론에 보도된 이후 국가정보원, 기무사 등이 오래전부터 패킷감청 장비를 보유하고, 최근 장비 보유대수가 3배 가까이 늘었다는 사실도 알려지면서, 법제도 미비로 인한 사생활 침해 문제의 심각성이 제기되고 국민들의 불안도 커지고 있습니다.

단어 자체도 생소한 “패킷감청”이란, 인터넷 회선에서 오가는 전자신호(패킷)을 빼내어 해당 컴퓨터의 화면을 고스란히 다른 컴퓨터에 복사하는 기술입니다. 즉, 패킷감청을 하게 되면 사이트 접속, 인터넷 뱅킹, 인터넷 전화, 메신저 대화 등 인터넷으로 하는 개인의 모든 활동을 통째로 들여다 볼 수 있고, 감청 대상자 뿐만 아니라 회선을 공유하는 다른 인터넷 사용자 까지도 광범위하게 감청할 수 있습니다. 특히 기술적으로 대상을 구분할 방법이 없고, 감청의

흔적도 남지 않는 ISBN 감청기도 있어 사생활의 비밀과 통신의 자유 등 기본권 침해가 심각하게 우려되고 있는 현실입니다.

무시무시한 내용이지만 인터넷을 사용하는 국민 대다수가 패킷감청 장비를 가진 누군가에 의해 사생활이 통째로 감시당할 수도 있다는 것입니다. 패킷감청 기술은 ‘빅 브러더’를 떠올리게 합니다. 조지오웰의 〈1984〉에 나온 것인데, 많은 사람들의 뇌리에 충격적으로 남아 있는 이유는 ‘빅 브러더’체제는 미디어 네트워크의 감시가 이루어지는 사회체제에서 개인이 아무리 발버둥쳐도 그 체제바깥으로 빠져나갈 수 없다는 것을 보여주었기 때문일 것입니다.

패킷 감청 자체가 그런 감시체제의 도구라고 보는 것은 지금 단계에서 너무 지나친 비약이 아니냐고 할 수도 있지만, 패킷감청 기술은 포괄적으로 우리의 생활 하나하나를 들여다 볼 수 있다는 점에서 단순한 수사방법의 하나로 보는 것과는 차원을 달리하는 기본권 침해 문제를 야기할 수 있고 인간의 존엄성 문제와 연결되어 있기 때문에, 패킷감청에 대한 법제도 보완을 진지하게 논의하는 오늘 토론회는 중요한 의미가 있다고 생각합니다.

오늘 토론회는 패킷감청의 기술적 과정을 직접 보고, 적절한 대안은 없는지 살펴보는 자리가 될 것입니다. 과학기술의 발전에 맞추어 우리 법제를 아날로그에서 디지털로 어떻게 변화시켜야 하는지 발상의 전환이 필요합니다.

특히 기술적으로 제한할 수 없는 것을 법으로 제한하는 건 패킷 감청만 합법화할 위험성도 있다는 점을 염두해 두고 감청장비 도입에 대한 법적 규제를 포함하여 심도 있는 논의가 이루어졌으면 합니다.

오늘 존정하는 변재일, 우윤근 두 의원님과 패킷감청에 관한 인식을 같이 하고 공동 토론회를 개최하게 된 것을 매우 뜻 깊게 생각합니다.

감사합니다.

인 사 말

국회의원 변재일(민주당 정책위 수석부의장)

안녕하십니까?

국회 문화체육관광방송통신위원회 소속 변재일 의원입니다.

오늘 법사위를 든든하게 떠받치고 있는 존경하는 우윤근, 박영선 두 의원님과 공동으로 토론회를 갖게 된 것을 매우 뜻 깊고 기쁘게 생각합니다. 아울러 조금은 부담스러운 주제일 수도 있는 이번 토론회에 흔쾌히 발제를 맡아주신 고대 임종인교수님, 아주대 오동석교수님, 시연을 맡아주신 인권운동사랑방, 토론자로 참석해주신 오길영 박사, 권정호 변호사, 장여경 활동가, 구태인 변호사님께도 감사의 말씀을 드립니다.

정보통신기술의 눈부신 발전에 의한 유비쿼터스 환경은 우리들에게 새로운 편익과 혜택, 그리고 국가발전의 동력을 제공해주지만 그 역기능도 결코 만만치 않습니다. 유비쿼터스 사회는 필연적으로 “감시사회”의 본질을 가지고 있기 때문입니다.

오늘 이 토론회에서 다루게 될 패킷감청(Deep Packet Inspection) 문제는 이미 현실화된 우리 사회의 역기능입니다. 하지만 이 문제가 갖는 사안의 엄중함에 불구하고, 작년 8월말 인 권단체들의 기자회견으로 실체가 드러나기는 하였지만 권력기관의 운용 실태는 정확히 알려져 있지 못하며 공론화되지 못한 아쉬움이 있었습니다. 이러한 와중에 최근 세계적인 논쟁이 되고 있는 패킷감청(DPI)기술의 상업적 이용을 도입하려는 시도가 우리나라에서도 일부 기업에서 추진되고 있음이 알려졌습니다.

감시와 수집이 일상화되고, 모아진 정보가 권력에 의해 악용되거나 민간에 의해 유출될 경우, 심각한 프라이버시 침해가 발생할 것입니다. 따라서 국회에서는 불균형적이고 불완전한 현재의 통신비밀보호법과 개인정보보호법체계를 보완하여 보호의 공백을 메움과 동시에 예방적이고 효과적인 역감시체계를 구축해 나가야 할 것입니다.

제가 알기로 오늘 이 토론회는 국회에서 열리는 최초의 패킷감청(Deep Packet Inspection) 관련 토론회일 뿐만 아니라, 일부 연구자들의 발표를 제외한다면 실제로 우리나라 최초로 열리는 패킷감청의 법적 기술적 문제점에 대해 공개토론회로 알고 있습니다.

어렵게 마련된 자리인 만큼, 현행 헌법과 법률의 범위에서 허용될 수 있는 것인지 법률적 검토와 DPI기술을 민간부문에서 상업적으로 이용될 경우 어떠한 문제가 있는지에 대해서 심도있는 논의가 이뤄지길 기대합니다.

감사합니다.

인 사 말

국회의원 박지원(민주당 정책위 의장)

헌법이 보장하는 국민의 기본권 수호는 불법 감청 퇴치로부터

문명의 이기를 이용한 국가기관의 대국민 범죄행위가 민주주의 국가 대한민국에서 자행되고 있습니다.

2008년 방송통신위원회의 공식 통계에 따르면 국가정보원은 전체 감청건수 중 98.5%를 차지하는 것으로 나왔습니다.

방통위의 '09년 상반기 인터넷 감청협조 자료'에 따르면, 패킷감청을 포함해 인터넷 서비스에 있어 게시판이나 이메일을 들여다본 건수는 2008년 1,152건, 2009년 상반기 799건에 달하는 것으로 집계됐는데, 이 가운데 거의 대부분의 감청은 이메일 감청이 아닌 패킷감청인 것으로 나타났습니다.

국가정보원이 사용한 '패킷 감청 기술'은 인터넷 이메일은 물론 웹서핑 등 대상자가 쓰는 인터넷 이용 내용을 원격으로 똑같이 엿볼 수 있는 기술입니다. 이는 당사자 뿐 아니라 같은 회선을 사용하는 직장 동료, 가족들의 인터넷 내용도 감청할 수 있다는 것입니다.

참으로 무섭고 어이가 없습니다.

지난 국정감사에서 방통위는 총 11대의 인터넷 패킷감청 설비를 인가한 내역이 확인됐습니다. 현행 통신비밀보호법상 정보·수사기관은 감청 설비를 설치하면 국회 정보위원회에 통보하게 돼 있고, 국가기관은 방통위에 신고를 해야 합니다. 그러나 설치 후 방통위에 신고한 국가기관은 한 군데도 없었습니다.

민주주의 대한민국에서 생활의 필수품이 된 개인 인터넷을 통째로 감청하고, 통제한다는 것은 민주주의 국가임을 거부하는 것이고, 초고속인터넷 가구당 보급률이 95%로 OECD 30개

국중 1위인 우리나라의 자존심을 일거에 추락시키는 국제적 수치이고 범죄행위입니다.

인터넷 메일은 물론, 웹서핑 등 인터넷 이용자 개인의 사생활의 비밀과 자유(제17조), 통신의 비밀(제18조)이 적나라하게 파헤쳐 지고 있다는 것은 국민의 헌법상 기본권을 철저히 침해하는 것이 아닐 수 없습니다.

정부 비판적 인물들을 요시찰인으로 지목하여 일거수 일투족을 감시·통제, 도·감청하던 군사독재시절로 회귀하는 것 같아 매우 우려스럽고 걱정이 앞섭니다.

오늘 이 토론회는 국민의 사생활과 통신 비밀 보호라는 헌법상 기본권을 지키고, 국가기관의 불법적 감시와 통제가 없는 자유로운 세상을 만들기 위한 매우 뜻 깊은 행사가 아닐 수 없습니다.

아무쪼록 발제자와 토론자로 참석하신 여러 전문가들의 고견을 충실히 듣고 국회가 법과 제도의 개선을 통해 국민의 권익을 수호하는 보루의 역할을 감당할 수 있기를 기원드립니다. 감사합니다.

2010년 2월 1일

민주당 정책위의장 박 지 원

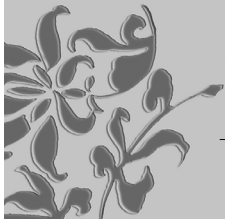
.....패킷감청의 문제점과 개선방안에 대한 토론회

01

패킷감청의 헌법적 문제점

오 동 석

(아주대 법학전문대학원 교수)



I. 들어가는 글

네트워크 회선에서 실시간 감청을 하는 패킷감청(Deep Packet Inspection)이 통신의 자유에 대한 중대한 위협요인으로 떠올랐다. 그런데도 실질적으로 감청범위를 확장하기 위한 통신비밀보호법의 개정 시도는 줄기차게 계속된다.¹⁾

패킷감청은 2008년 국가보안법 위반 혐의로 구속 기소된 박동기 남북공동선언실천연대 정책위원을 대상으로 발부된 통신제한조치 허가서에서 드러났다.²⁾ 이 허가서는 해당 사건을 수사하던 국가정보원이 서울중앙지검을 거쳐 통신제한조치를 청구하자 서울중앙지법이 2008년 6월 12일 발부한 것이었다. 여기에는 “대상자가 근무처...에 자신의 명의로 설치, 사용 중인 하나로텔레콤(주) ‘광랜W’ 초고속 인터넷 회선에 대한 전기통신 내용의 지득·채록 및 실시간 착·발신 IP 추적” 그리고 “대상자 주거지...에 처 ... 명의로 설치한 KT ‘뉴메가패스’ 초고속 인터넷회선...에 대한 전기통신 내용의 지득·채록 및 실시간 착·발신 IP추적”이 포함되어 있었다.³⁾

인권단체들은 세 가지 의문점을 제시하였다. 첫째, 패킷감청이 적법하게 이루어졌나, 둘째, 패킷감청은 어느 정도 자세하게 이루어졌나, 셋째, 사용된 감청 장비는 누구의 것인가 등이 그것이었다. 더불어 국가정보원 등 정보수사기관들이 패킷감청을 어느 시점부터 실시해왔는지도 추가적인 의문점이었다.

* 이 글은 오동석/ 오길영, 국회정보위원회의 연구용역보고서(2009.12.31)를 기초로 하여 2010. 1. 16. 우리법연구회에서의 발표문을 수정·보완한 것이다. 연구회 참석회원 모두가 실무적·학술적 관점에서 논평을 해준 것에 대하여 감사의 뜻을 전한다. 그런데 이 글은 논문으로서의 완성도를 갖추지 못하였으므로 인용을 삼가기 바랍니다.

** 아주대 법학전문대학원 교수, 헌법학

1) 가장 최근에는 선진한국을 위한 통신비밀보호법 개정방향, 주최: 국가안보전략연구소, 2009.12.1, 토론자로서 참가한 소회로는 그 자리는 토론회의 이름을 빌어 감청의 확장을 일방적으로 홍보하는 장이었다. 반대의견은 그저 액세서리(accessory)일 뿐이었다. 내 생각엔 대한민국헌법도 그 자리에선 액세서리에 불과하였다.

2) 2009년 8월 31일 인권단체들이 이를 비판하는 기자회견을 개최하였다(진보네트워크센터, “패킷 감청 의견,” 2009.10.29).

3) 이와 관련 한겨레21 제776호(2009.9.4, <http://h21.hani.co.kr/arti/cover/cover_general/25658.html>, 검색일: 2009.12.3.) 참조.

이와 관련한 패킷감청 문제가 2009년 국정감사에서 다루어졌다. 먼저 10월 7일 국회 문화체육관광방송통신위원회의 방송통신위원회에 대한 국정감사에서 서갑원 의원은 2002년부터 당시까지 총 11대의 “인터넷 패킷 감청설비”가 방송통신위원회에 신고되었음을 밝혔다.⁴⁾ 이 장비들은 국방부, 대검찰청, 경찰청 등에서 사용되는 것으로 보인다.

그런데 통신비밀보호법 제10조의2 제2항에 따르면 경찰·군의 정보 관련부서나 국가정보원의 감청 장비는 방송통신위원회가 아니라 국회 정보위원회에 별도로 통보하도록 규정되어 있다. 따라서 이들 기관이 보유하고 있는 인터넷 패킷 감청설비의 규모가 얼마인지가 문제인 것이다. 이와 관련하여 10월 22일 방송통신위원회 국정감사에서 변재일 의원은 2002년 하반기 이후 방송통신위원회에 의해 인가된 전체 감청설비 가운데 82%가 정보기관에서 도입한 것으로 추정하였다.⁵⁾ 물론 정보기관이 직접 수입·제조한 감청설비는 여기에서 제외된다.⁶⁾

서갑원 의원은 인터넷 패킷감청이 “같은 회선을 사용할 경우, 법원의 통제 없이 국민의 사생활이 통째로 실시간 감시될 수 있다”고 우려를 표시했다. 10월 8일 국회 법제사법위원회의 법제처 국정감사에서 박영선 의원은 패킷감청이 감청의 범위가 너무 광범위하여 통신의 자유와 사생활을 침해할 우려가 있다고 지적하였다. 또한 “통비법 제3조제2항에 규정된 최소 침해의 원칙에 반하는 것이며 포괄 영장 금지 원칙에도 어긋나는 것”이라고 지적하였다. 이에 대하여 법제처장은 문제를 검토하겠다고 답변하였다. 10월 9일 고등법원 국정감사와 10월 20일 대법원 국정감사에서도 박영선 의원은 패킷감청이 사무실이나 아파트 등에서 같이 회선을 나눠 쓰는 다른 이들의 모든 개인정보까지 열어 볼 수 있기 때문에 법원의 영장 발부가 특별히 신중해야 한다고 지적하였다. 이에 대해 서울지방법원장과 대법원 법원행정처장은 패킷감청 문제를 제도적·기술적으로 검토하겠다고 답변하였다.⁷⁾

나는 질문을 달리 한다. 즉 ‘패킷감청이 적법하게 이루어졌는가’를 묻는 것이 아니라 ‘패킷감청은 적법할 수 있는가’를 묻는 것이다. 달리 말하면, 수사기관은 패킷감청을 적법하게 시행할 수 있는가, 나아가 법원은 패킷감청을 허가할 권한을 가지고 있는가, 더 나아가 국회는 패킷감청을 허용하는 입법을 할 권한을 가지고 있는가 하는 질문에 대한 답을 구하는 것이기도 하다. 이 글은 이러한 질문에 대한 나의 헌법적 답이다.

결론부터 말하면 패킷감청은 헌법적으로 절대 허용될 수 없는 절대금지의 영역이다. 즉 그

4) 통신비밀보호법 제10조의2 제1항에 따라 정보수사기관이 아닌 국가기관은 감청설비 도입에 관하여 방송통신위원회에 신고하여야 한다.

5) 2009년 10월 29일 국회 정보위원회 회의에서도 정보기관의 패킷감청 장비 문제가 다루어질 것으로 보이지만, 그 결과는 알려지지 않았다(진보네트워크센터, 2009.10.29).

6) 통신비밀보호법 제10조 제1항은 국가기관의 경우 감청설비의 제조수입 등에 대하여 방송통신위원회 인가를 받지 않도록 규정하고 있다.

7) 진보네트워크센터, 2009.10.29.

것은 헌법 제37조 제2항 단서의 본질적 내용 침해에 해당하는 것이어서 금지된다. 따라서 헌법 제18조 “모든 국민은 통신의 비밀을 침해받지 아니한다.”는 규정은 해석상 ‘통신에 대한 패킷감청에 대한 허가는 인정되지 아니한다’는 내용을 포함하고 있다고 나는 주장한다. 헌법 제21조 제2항 “언론·출판에 대한 허가나 검열과 집회·결사에 대한 허가는 인정되지 아니한다.”는 규정으로부터의 유추해석이다. 그것은 새로운 패킷감청 기술에 대하여 ‘기본권을 최대한 보장해야 하는 원칙과 최소한 제한해야 한다는 원칙’⁸⁾을 적용한 결과로서 헌법적 기준을 통과할 수 있는 방안이 도출되지 않는 이상 패킷감청은 허용될 수 없기 때문이다.

II. 패킷감청의 개념과 특성

인터넷을 통한 정보전달은 각각의 파일을 패킷(packet)이라는 단위로 잘게 쪼개어 송신한 뒤 이를 받아보는 컴퓨터가 해당 패킷을 재구성해 이를 다시 화면에 구현하는 형태로 이루어진다. 통상적인 통신제한조치는 전자우편의 경우 이미 주고받은 것을 나중에 열어보는 것이다. 패킷감청이 그것과 다른 점은 ‘인터넷 회선’ 자체를 감청하는 점이다. 즉 패킷감청이란 이용자가 인터넷을 이용하는 과정에서 인터넷 회선을 통해 전기신호 형태로 흐르는 패킷을 제3자가 중간에 가로챌으로써 같은 내용을 실시간으로 들여다보는 것이다. 패킷감청에는 ‘Shallow Packet Inspection(아래 “SPI”)’과 ‘Deep Packet Inspection(아래 “DPI”)’이 있다.⁹⁾

패킷감청의 문제를 심도 있게 분석하고 비판한 오길영은 다음과 같이 말한다.¹⁰⁾

“SPI의 경우는 이미 오랜 시간 사용되어온 전형적인 네트워크 기술이다. 따라서 패킷 감청 자체는 그리 최신기술이 아니다. 또한 SPI의 경우에는 법률적 의미의 감청과 관련하여 특별한 문제도 없기 때문에 패킷 감청 자체가 모두 불법성을 함유하고 있는 것도 아니다. 새로이 개발된 DPI 기술만 문제가 될 뿐이다.”¹¹⁾ “따라서 ‘국정원이 패킷 감청을 했다’에서의 패킷 감청이라는 용어는 그리 정확한 표현이 아니다. ‘Inspection’이라는 용어가 비단 ‘감청’의 의미만 있는 것도 아니고, 나아가 패킷 감청이 DPI만 있는 것도 아니기 때문이다.”¹²⁾

패킷의 구조는 단순하지는 않지만 크게 두 개의 부분으로 나누어져 있다. 우편으로 송달되는 편지에 비유할 수 있다. 헤더부는 편지봉투에 해당하여 그 결봉에 도착지가 기재되어 있

8) 헌재 1991.7.22. 선고 89헌가106 결정.

9) 이 글에서 별도의 언급이 없는 한 패킷감청은 DPI를 의미한다.

10) 오길영, “인터넷 감청과 DPI(Deep Packet Inspection),” 민주법학 제41호, 민주주의법학연구회, 2009.12, 411.

11) 오길영, 앞의 글, 411.

12) 오길영, 앞의 글, 411의 주 48).

는 부분이며, 데이터 영역은 봉투 속에 들어있는 편지지로서 우편을 통해 전달되어야 할 내용물이다.¹³⁾ 다시 오길영의 글을 길게 인용한다.

원래 인터넷 네트워킹 기술의 기본원칙은 헤더부에 적힌 주소(출발지와 목적지)에 의해 전송되는 방식이다. 따라서 헤더부의 정보가 없다면 주소가 적혀있지 않은 편지봉투와 같은 운명이 되는 것이다. 우체국에서 그러하듯 때로는 헤더부를 검사해 볼 필요가 있다. 이 우편물이 주소대로 잘 우송되고 있는 것인지, 또는 우편번호가 잘못 적힌 것은 아닌지 말이다. 이렇듯 어떠한 이유에 의해 헤더부의 내용을 검사하는 행위가 SPI이다. 집배원이 겉봉의 내용을 살피는 것이 불법이 아닌 것처럼, SPI는 불법의 이유가 없다.

SPI 기술은 주로 네트워크 방화벽(Firewall) 시스템을 위해 개발되어 왔고 현재 널리 사용되고 있다. 즉 기업이나 조직의 차원에서, 기업·조직의 내부를 구성하고 있는 컴퓨터의 정보 보안을 위해 외부에서 내부, 내부에서 외부의 네트워크에 침입하는 것을 차단하는 기술로 사용된다.

한편 DPI는 데이터 영역까지 살피보는 검사를 말한다. 즉 집배원이 그 겉봉을 뜯어 내용물을 살피는 행위에 해당한다. 이러한 행위는 불법임은 물론 감청에 해당하는 것이다. 설사 내용을 다 읽어보고 원래대로 잘 집어넣어서 목적지에 고스란히 전달한다고 하여도, 그 행위의 불법성은 소멸하지 않는다.

원래 DPI 기술은 네트워크 접속문제의 해결, 바이러스(Viruse)나 웜(Worm)의 차단, 그리고 최근 DDoS(Distributed Denial-of-Service Attack, 분산 서비스 거부) 사태로 유명해진 '서비스 거부(Denial-of-Service Attack, DoS)'를 해결하기 위해 개발되어 사용되었다.¹⁴⁾

집배원이 우송의 목적으로 겉봉의 내용을 살피는 것은 법적 문제가 없지만, 그가 그 외의 목적으로 겉봉의 내용을 살피거나 그 외의 자가 겉봉의 내용을 살피는 것도 사생활의 비밀에 대한 침해가 된다. 물론 그것의 법적 제재 여부는 또 다른 판단영역이다. 그것은 패킷에 대해서도 마찬가지일 것이다.¹⁵⁾

그런데 DPI 감청 과정은 피의자가 사용하는 인터넷 회선에다 감청용 회선을 브릿지(Bridge)하고, 거기에 노트북을 연결한 후 DPI 프로그램을 가동시키는 것으로 시작된다. 만약 피의자가 이메일을 작성하여 송신한다면 패킷으로 조각난 데이터가 피의자의 컴퓨터를 떠나 회선으로 진입하자마자 DPI 프로그램이 작동하여 '우편집배원을 강제연행'한 후 그 데이터를

13) 오길영, 앞의 글, 413.

14) 오길영, 앞의 글, 413-4.

15) 오옴은 더 이상 우편집배원의 비유가 적절치 않다고 하지만(Ohm, Paul, "The Rise and Fall of Invasive ISP Surveillance," Working Paper Number 08-22, Legal Studies Research Paper Series, 2008.9.9, 1-82), 나는 여기에서 그 비유를 사용하였다.

‘포괄적으로 압수’한다. 이때 패킷감청에는 두 가지 방식이 있다.¹⁶⁾ 하나는 패킷 자체를 포괄적으로 압수한 후 감청기관의 컴퓨터상에서 DPI하고(포괄적 수색), ‘필요한 경우 구체적 압수’ 후 DPI가 끝나면 패킷을 가던 길로 보내는 방법이다. DPI과정은 DPI프로그램이 당해 패킷을 읽어 들이면서 노트북의 메모리나 임시폴더에 저장하는 방식을 사용한다. DPI가 끝나면 원본은 가던 길로 돌려보내고 메모리나 임시폴더에 남아있는 복사본은 삭제된다. 이때 100개의 패킷이 DPI되었다면 메모리나 임시폴더에 100번의 저장이 필요하다.

다른 하나의 방법은 원본과 동일한 복사본을 즉시 만드는 것이다(우편집배원 체포 후 그의 우편행낭 포괄적 압수 후 포괄적 복사). 원본은 가던 길로 보내고 복사본을 국정원의 노트북 메모리나 하드디스크로 옮긴(포괄적 복사 압수) 후 천천히 DPI하는(포괄적 수색 후 필요한 경우 구체적 압수) 방법이 있다. 수사기관이 패킷을 확보한 당시에는 조각들에 불과하더라도, 수사기간이 그 이메일 내용을 열람하기 위해서는 반드시 재조합이 필요하다.

따라서 패킷 감청을 이용하면 대상자가 인터넷을 통해 접속한 사이트 주소와 접속시간, 대상자가 입력하는 검색어, 전송하거나 수신한 게시물이나 파일의 내용을 모두 볼 수 있다. 이 메일과 메신저의 발송 및 수신내역과 그 내용 등과 같은 통신내용도 모두 볼 수 있다.¹⁷⁾

패킷감청은 피의자의 컴퓨터를 오가는 길목을 지키고 있는 것이므로 피의자가 접속하는 모든 웹페이지 주소의 목록과 이동경로 및 로그인 정보, 해당 웹페이지에의 접속한 시간과 기간, 컴퓨터를 켜고 끈 시간 등 가장 정확한 통신사실 확인자료를 손쉽게 덤으로 얻을 수 있다. 즉 통신사실 확인자료의 요청을 위한 별도의 허가서는 필요 없다. 피의자가 만약 요즘 유행하고 있는 인터넷 전화를 사용하고 있다면 허가서에 없는 전화통화까지 들어볼 수 있다. 나아가 피의자가 패킷화된 데이터를 사용한 IPTV 서비스를 이용하고 있다면, 수사기관은 피의자가 보오 있는 TV프로그램을 동시에 볼 수 있다.

따라서 수사기관은 피의자가 사용한 컴퓨터와 관련된 모든 정보와 내용은 기본이고, 피의자가 좋아하는 음악과 드라마, 최근 구입한 인터넷 쇼핑의 품목과 가격, 거실에서 받은 친구와의 전화통화 내용은 물론, 문을 걸어 혼자 몰래 감상한 야한 동영상까지, 피의자가 모든 통신 정보를 단 한 장의 허가서에 의해 몽땅 취합하게 된다. 수사기관은 허가서에 특정된 정보만을 볼 방도가 없다.¹⁸⁾ 패킷감청에 대한 법원의 허가는 사실상 ‘포괄적 백지 허가서’를 발부하는 것이다. 피고인 및 그와 통신을 한 사람들의 통신의 자유 및 사생활의 비밀 자유는 유명 무실하게 된다.

16) 패킷감청 방법에 대하여는 오길영, 앞의 글, 418 아래.

17) 진보네트워크센터, 2009.10.29.; 권정호, “의견서”, 2009고합731 국가보안법위반, 제출처: 서울중앙지방법원 제25형사부, 2009.11. 상세한 것은 오길영, 앞의 글, 410 아래.

18) 오길영, 앞의 글, 420-1.

결국 패킷감청은 감청대상자와 무관한 제3자를 포함하여 일반적으로 감청하는 결과를 낼 수 있으며, 수사목적과 무관한 통신내용까지 무제한적으로 포괄적으로 감청하는 문제점을 안고 있다. 따라서 패킷감청은 헌법상 포괄영장금지 원칙에 위반됨은 물론이고 심각한 프라이버시 침해에 대한 사법적 통제가능성을 유명무실하게 만든다. 이러한 점 때문에 패킷감청은 헌법 제37조 제2항의 본질적 내용 침해에 해당하지 않는지가 문제된다.

III. 패킷감청 및 그 허가의 헌법적 문제점

1. 패킷감청에 대한 ‘헌법적 접근’

헌법규범적 가치가 높은 것일수록 약방의 감초처럼 나타나 구체적인 헌법적 쟁점에 대한 해결의 향도 구실을 하는 것이 순리이다. 그렇지 않다면 그것은 헌법규범이 헌법현실에 착종되지 못한 까닭이다. 이런 지경에서 헌법규범은 단지 규범일 뿐 위헌적 관행과 현실이 우위를 점하며, 원칙은 원칙일 뿐 현실적 규정력을 발휘하는 것은 예외이다.¹⁹⁾

헌법은 “국가의 조직·구조·체제”²⁰⁾에 대한 법이다. 근대입헌주의의 핵심원리는 권력분립원칙이다. 권력분립원칙은 국민의 자유와 권리를 보장하기 위하여 국가권력을 입법·관·집행·사법권으로 분할하고, 이들 권력을 각각 분리·독립된 별개의 국가기관들에 분산·시킴으로써, 특정의 개인이나 집단에게 국가권력이 집중되지 아니하도록 함은 물론 권력상호간에 권력적 균형관계가 유지되도록 하는 통치구조의 구성원리이다.²¹⁾ 그 개념적 요소는 국가작용의 구분이고, 별개 기관에 그것을 귀속시키는 것이다. 이때 각 기관은 자신에게 귀속된 통치작용만을 행사하고 다른 기관에게 귀속된 통치작용은 행사할 수 없다.²²⁾

그런데 권력분립원칙이 내포한 억제와 균형 관계는 의회 중심으로 형성된다. 즉 “오늘날 법률유보원칙은 단순히 행정작용이 법률에 근거를 두기만 하면 충분한 것이 아니라, 국가공동체와 그 구성원에게 기본적인고도 중요한 의미를 갖는 영역, 특히 국민의 기본권실현과 관련된 영역에 있어서는 국민의 대표자인 입법자가 그 본질적 사항에 대해서 스스로 결정하여야

19) 법적·정치적 질서로서의 규칙이 배제된 것으로서 예외를 포함하는 구조를 가진다는 지적은 종종 있었다. 즉 예외가 규칙에서 벗어나는 것이 아니라 오히려 규칙이 스스로의 효력을 정지시킴으로써 예외를 창출한다는 것이다. 아감벤은 “오늘날 예외 상태 자체가 바로 근본적인 정치 구조로서 점점 더 전면에서 떠오르고 있으며, 궁극적으로 규칙이 되어가고 있다”고 지적한다(Agamben, Giorgio, 박진우 옮김, 호모사케르: 주권 권력과 별거벗은 생명, 새물결, 2008, 63). 그러나 내가 보기엔 그것이 한국 사회의 현실에서는 이미 고착화되었다.

20) 권영성, 헌법학원론, 법문사, 2008, 3.

21) 권영성, 앞의 책, 739.

22) 권영성, 앞의 책, 739.

한다는 요구까지 내포하고 있다”(의회유보원칙).²³⁾

국회를 중심으로 이루어지는 입법작용은 일반적이고 추상적인 성문의 법규범을 정리하는 국가작용이며, 행정작용은 입법의 하위작용으로서 법규범에 따라 법을 구체화하고 집행함으로써 현실적으로 국가목적 실현하는 작용이다.²⁴⁾ 헌법은 현대에 이르러 행정부 중심의 국가 운용 경향에 따라 집행부에 광범위한 행정입법권을 인정하고 있다. 그렇지만 헌법은 “법률에서 구체적으로 범위를 정하여 위임받은 사항”에 관해서만 행정입법을 허용한다(헌법 제 75조).

“법률의 위임은 반드시 구체적이고 개별적으로 한정된 사항에 대하여 행해져야 한다. 그렇지 아니하고 일반적으로 포괄적인 위임을 한다면 이는 사실상 입법권을 백지위임하는 것이나 다름없어 의회입법의 원칙이나 법치주의를 부인하는 것이 되고 행정권의 부당한 자의와 기본권행사에 대한 무제한적 침해의 초래할 위험이 있기 때문이다”.²⁵⁾

권력분립원칙은 입법·사법·행정기관이 적절하게 권한을 나누어 가지기만 하면 충족되는 헌법원칙이 아니다. 그것은 단지 필요조건일 뿐이다. 그것의 충분조건은 각 작용이 가지고 있는 본질적 특성을 유지하는 것이다. 그 본질적 특성이 기본권 보장에 결부된 한에서 권력분립원칙은 매우 엄정하게 관철되어야 한다.

그러므로 개별적이지만 포괄적인 피의자의 통신행위와 그와 관련된 일반적이고 포괄적인 통신 상대방의 통신행위를 일반적이고 포괄적으로 침해하는 패킷감청은 검열 또는 허가처럼 헌법의 금지사항에 해당한다. 따라서 패킷감청에 대한 법원의 허가 또한 헌법상 허용되지 않는다. 패킷감청에 대한 법원의 허가는 법의 적용으로서의 집행작용이 아닌, 법의 해석을 넘어서는 입법작용의 성질을 띠고 있을 뿐 아니라 헌법이 허용하는 영장주의의 본질에서 벗어나기 때문이다.

2. 패킷감청과 영장주의

감청에 대하여 통신비밀보호법은 영장이 아닌 법관의 허가를 얻도록 하고 있다. 허가는 성질상 영장 발부와 동일한 것으로 본다.²⁶⁾ 그것은 수사기관이 법원이 한정한 대상과 방식에 따라야 함을 의미하는 것이다. 이때 법원은 대상과 방식을 개별적·구체적으로 한정하여야 한

23) 헌재 1999.5.27. 선고 98헌바70 결정.

24) 권영성, 앞의 책, 812.

25) 헌재 1991.7.8. 선고 91헌가4 결정; 1998.5.28. 선고 96헌가1 결정.

26) 정종섭, 헌법학원론, 박영사, 2009. 다만 그는 감청은 헌법 제12조 제3항에서 정하는 체포·구속·압수·수색에 해당하지 않으므로 헌법 제12조 제3항이 적용되지 않는다고 본다. 그렇지만 일반영장의 금지 등 영장주의의 핵심은 감청허가에도 그대로 타당한 것으로 보아야 할 것이다.

다. 그것은 통신의 자유에 대한 “적절한 사회적 기대”²⁷⁾를 보장하는 것이어야 한다. 헌법에서 규정한 영장은 범죄의 내용, 구금할 장소, 압수수색의 목적물과 범위가 특정되지 않은 일반 영장은 금지된다. 따라서 압수의 목적물과 수색의 대상과 범위가 모호하거나 포괄적인 일반 영장(general warrant)은 허용되지 않는다.²⁸⁾

여기에서 ‘일반’이란 단어와 ‘포괄’이란 단어를 법적으로 구별해야 한다. 엄밀하게 말하면 일반영장은 그 용어 자체가 성립할 수 없다. 영장은 개인별로 발급되는 것이어야 하므로²⁹⁾ 불특정 다수에 대하여 발해질 수 없는 까닭이다. 헌법상 금지되는 영장을 정확하게 표현하면, 그것은 포괄영장(또는 백지영장이나 추상적 영장)이다. 왜냐하면 영장은 구체적이어야 하기 때문이다. 따라서 명확하게 그 대상이 한정되어 있어야 한다.

반면 패킷감청은 “말 그대로 데이터가 움직이는 도로를 통째로 감청하도록 허가해 준 것이다. 대상도 없고 범위도 없이, 도로에 움직이는 모든 것을 다 감청하도록 진정한 ‘포괄 허가서’를 발부해 준 셈이다.”³⁰⁾

그런데 감청을 비롯한 통신제한조치를 허용하는 법원의 결정에 대하여 통신비밀보호법은 왜 영장이 아니라 허가라는 표현을 사용한 것일까. 내 생각엔 감청에는 신체의 자유에 대한 체포·구속영장 또는 물건에 대한 압수수색영장과 다른 본질적 차이가 있다. 영장은 한 사람의 인신만이 또는 범위를 확정할 수 있는 피의자의 물건만을 그 대상으로 한다.

그러나 통신제한조치에는 피의자 외에 또 다른 상대방이 관여되어 있다. 전화인 경우 통화의 상대방, 우편의 경우 송신인 또는 이메일의 경우 송수신인 등이 그 상대방이다. 피의자 관점에서 보면 그 상대방은 한 두 사람으로 특정될 수 없다. 그런 점에서 감청 허가란 피의자를 대상으로 발부되지만, 불가피하게 통신의 속성상 불특정 다수의 상대방이 관계될 수밖에 없는 구조이다. 그렇기 때문에 통신제한조치는 “다른 방법으로는 그 범죄의 실행을 저지하거나 범인의 체포 또는 증거의 수집이 어려운 경우에 한하여 허가할 수 있”(통신비밀보호법 제5조 제1항)음이 내재되어 있다고 말할 수 있다.

그러므로 법원이 피의자와 특정 통신매체를 대상으로 하여 통신제한조치를 허가하는 것은 그 허가 자체에 있어서도 신중해야 하며, 허가하는 경우에도 구체적 범위를 확정하기 위하여 최선의 노력을 다하여야 한다. 그렇지 않다면 피의자의 통신상대방은 통신의 자유 또는 사생

27) Crocker, Thomas P., FROM PRIVACY TO LIBERTY: THE FOURTH AMENDMENT AFTER LAWRENCE, UCLA law review 제57권 제1호, 2009, 3.

28) 정종섭, 앞의 책, 514.

29) 영국의 수사권규율법(Regulation of Investigatory Powers Act 2000) 제8조 제1항은 “한 명의 감청대상자” 또는 “영장이 관련되는 감청이 이루어지는 시설물과 관련된 경우에는 한 세트의 시설물” 중 하나가 기재되어야 함을 명시하고 있다.

30) 오길영, 앞의 글, 411.

활의 비밀 등을 침해당하기 때문이다. 따라서 피의자의 통신상대방 중 피의자의 범죄행위와 상당 정도 연관성이 있는 통신상대방과의 통신만이 감청대상으로 되어야 된다. 그렇지 않다면 법원은 통신비밀보호법상의 허가주의를 위반한 것이 된다. 왜냐하면 피의자만을 특정하여 그의 모든 통신상대방과의 통신을 감청하도록 허가하는 것은 통신상대방의 관점에서 보면 불특정 다수에 대한 허가라는 점에서 일반허가이기 때문이다.

따라서 패킷감청은 헌법적으로 성립할 수 없는 일반허가이면서 동시에 헌법적으로 금지되고 있는 포괄허가이다. ‘패킷’이란 말을 ‘패키지(package)’로 오해하는 경우가 있는데, 패킷감청은 ‘불특정인을 포괄적 통신수단에 의해 포괄적 사항의 묶음’(패키지) 채로 감청함으로써 ‘위헌 요소의 패키지감청’이라 부를 만하다. 감청대상자와 상당관계에 있는 통신상대방과의 통신내용만을 그 내용 자체를 들여다보지 않고 구체적으로 선별하여 감청할 수 있는 패킷감청 기술이 등장하지 않는 한, 패킷감청은 헌법상 절대적으로 금지되어야 한다. 수사기관이 패킷감청 기술의 혜택을 누리려면, 기본권의 최대한 보장을 실현하기 위하여 그 침해 방지책이 충분히 마련될 때까지 기다려야 한다. 법적으로 그렇게 하지 않는다면 헌법상 통신의 자유는 유명무실해질 것이며, 통신비밀보호법에 따른 법관에 의한 감청허가제 또한 무용지물이 될 것이기 때문이다.

3. 패킷감청의 위헌성

첫째, 패킷감청은 헌법의 기본원칙으로서 권력분립원칙에 위배된다. 국가작용의 측면에서 권력분립원칙은 집행행위에 대하여 개별성 및 구체성을 엄격하게 요한다. 그것이 완화되는 현상이 일어나고 있지만, 그것은 적어도 기본권 제한의 영역은 아니다. 그런 점에서 보면, 패킷감청은 행정작용과 사법작용의 본질적 한계범위를 넘어선 것이다. 그것은 단순히 법률의 제정 또는 개정으로 해결될 수 있는 사안이 아니다.

둘째, 패킷감청은 헌법 제37조 제2항으로부터 도출되는 과잉금지원칙에 위배된다. “기본권의 최대보장의 원칙과 최소제한의 원칙은 기본권보장의 2대원칙이며, 이 원칙은 헌법이 기본권제한의 방법으로 규정하고 있는 일반적 법률유보에 의한 제한방법(헌법 제37조 제2항)이나 헌법의 직접규정에 의한 제한방법의 해석에 있어서도 존중되어야 한다.”³¹⁾ 과잉금지원칙은 국민의 기본권을 제한하는 경우 국가작용의 한계를 명시한 원칙으로서 목적정당성³²⁾·수단적정성³³⁾·피해최소성³⁴⁾·법익균형성³⁵⁾ 원칙을 그 내용으로 하며, 그 어느 하나에라도 저촉되면

31) 현재 1991.7.22 선고 89헌가106 결정.

32) 목적의 정당성은 국민의 기본권을 제한하는 의회의 입법은 그 입법목적이 헌법과 법률의 체계 내에서 정당성을 인정받을 수 있어야 함을 의미한다.

33) 수단적정성이란 법률에 규정된 처분이 제한 목적을 달성하는 데 유용할 뿐 아니라 적정한 수단인가의 여부에 따른 판단 기준을 말한다.

위헌이 된다는 헌법원칙이다.

통신의 자유에 대한 제한으로서 패킷감청은 과잉금지원칙이 엄격하게 적용되어야 한다. 범죄 수사의 목적이 정당하다고 하더라도 그 수단으로서 패킷감청은 불특정인에 대한 포괄적 감청이기 때문에 그 수단으로서 적정하지 않다. 뿐만 아니라 피해최소성원칙에도 부합하지 않는다. 왜냐하면 회선감청에 의하지 아니하고도 특정 계정의 이메일에 대하여 감청할 수 있기 때문이다.

셋째, 패킷감청은 헌법상 적법절차에 위배된다. 적법절차는 입법·집행·사법 등 모든 국가작용은 정당한 법률을 근거로 하고 정당한 절차에 따라 발동되어야 한다는 헌법원리이다. 이때 ‘due process of law’의 실질적 의미는 ‘적법절차’가 아니라 ‘법의 적정한 절차’³⁶⁾이다. 헌법재판소도 “적법절차를 절차의 적법성 뿐만 아니라 절차의 적정성까지 보장하는 것”으로 풀이하고 있다.³⁷⁾ 즉 적법절차는 모든 공권력 행사는 절차상의 적법성뿐만 아니라 공권력 행사의 근거가 되는 법률의 실체적 내용도 합리성과 정당성을 갖춘 실체적인 적법성이 있어야 한다는 법리이다.³⁸⁾

적법절차의 핵심내용은 ① 개인의 자유와 권리에 영향을 미치는 국가적 행위에 대하여 관계국가기관이 정당한 권한을 가질 것, ② 입법의 절차는 물론이고 법률의 내용도 구체적이고 명확할 것, ③ 상대방에게 고지·청문의 기회가 제공될 것, ④ 변호인의 조력을 받을 권리와 유리한 증인의 강제소환 등이 보장될 것, ⑤ 관정기관이 공정하게 구성될 것, ⑥ 권리의무의 판정은 정의의 원칙과 헌법의 기본이념에 합치하고 자의적인 것이 아닐 것 등이다. 패킷감청은 적어도 ①, ②, ③, ⑥에 위배된다. 수사기관의 패킷감청은 물론 그에 대한 법원의 허가도 헌법상 허용되지 않기 때문이며, 패킷감청은 감청의 성질상 당사자에게 통지되지 않음은 물론 그 자체가 구체적이고 명확하지 않기 때문이다.

넷째, 패킷감청은 헌법이 금지하고 있는 연좌제에 위배된다. 헌법상 “모든 국민은 자기의 행위가 아닌 친족의 행위로 인하여 불이익한 처우를 받지 아니한다.”(헌법 제13조 제3항). 자신의 행위가 아닌 친족의 행위를 이유로 형사처벌 등 불이익한 처우를 받는 것은 헌법의 자기책임원칙 또는 개인책임원칙에 위배되기 때문이다. 이 조항은 민법상의 친족인 배우자·혈

34) 피해최소성원칙은 입법자가 강도가 낮은 침해의 단계로는 입법목적을 달성할 수 없는 경우에만 비로소 더 강한 침해의 단계에 발을 들여 놓을 수 있다는 것을 요청한다.

35) 법익균형성원칙은 “기본권의 제한이 위의 여러 원칙들에 적합한 경우에도 기본권 제한이 의도하는 정치·경제·사회적 유용성과 그 제한에 의하여 야기되는 국민적·사회적 손실을 비교형량하여 양자간에 합리적인 균형관계가 사해야 함”(권영성, 앞의 책, 353)을 말한다. 목적과 수단의 비교형량에서 지향해야 할 지침은 ① 침해의 강도(Intensität), ② 공공복리의 비중 및 긴급성, ③ 기본권보장에서 보호되는 개별이익 그 자체 등이다.

36) 김승환, “헌법과 민주주의,” 민주법학 제31호, 2006, 356.

37) 헌재 1993.7.29. 선고 90헌바35 결정.

38) 헌재 1992.12.24. 선고 92헌마8 결정.

죽인척(민법 제767조)의 행위뿐 아니라 그 밖의 모든 타인의 행위로 인한 불이익한 처우를 금하는 취지이다.³⁹⁾ 그리고 불이익한 처우는 예를 들어 해외여행의 제한이나 공무담임권의 제한 기타 모든 영역에서 국가기관에 의한 모든 불이익한 대우를 포함한다. 그런데 패킷감청은 그 대상자와 인터넷회선을 함께 사용한다는 이유로 불특정의 사람들의 통신의 자유를 중대하게 침해할 수 있어서 연좌제에도 위배되는 것이다.

다섯째, 패킷감청은 헌법 위반일 뿐 아니라 통신 감청이 최소한·보충적으로 이루어져야 한다는 통신비밀보호법상의 감청 범위를 벗어난 위법한 감청이다. 구체적으로는 통신비밀보호법 제3조 제2항과 제5조 제1항 위반일 가능성이 매우 크다. 왜냐하면 전기통신의 감청은 “범죄수사 또는 국가안전보장을 위하여 보충적인 수단으로 이용되어야 하며, 국민의 통신비밀에 대한 침해가 최소한에 그치도록 노력하여야”하며, “통신제한조치는 … 범죄를 계획 또는 실행하고 있거나 실행하였다고 의심할만한 충분한 이유가 있고 다른 방법으로는 그 범죄의 실행을 저지하거나 범인의 체포 또는 증거의 수집이 어려운 경우에 한하여 허가할 수 있”기 때문이다.

패킷감청은 보충성의 원칙에 충실해야 할 수사과정에서 감청원칙을 벗어나기 십상이다. 왜냐하면 감청 대상자의 인터넷 통신내용은 대상자의 서버에 그대로 저장되기 때문에 수사기관은 필요한 내용을 사후에 얼마든지 압수수색영장을 받아 이를 취득할 수가 있기 때문이다. 따라서 패킷감청으로 취득한 증거자료는 얼마든지 사생활 침해가 덜한 포딩 방식의 감청으로 획득할 수 있을 것이다. 패킷감청이 문제가 된 사건에서 국가정보원이 패킷감청에 의해 획득된 증거를 제출하지 못한 것은 바로 이 점을 증명하고 있다.

결론적으로 패킷감청은 헌법 제37조 제2항 단서의 본질적 내용 침해에 해당하는 기본권 침해이다. 헌법 제18조 “모든 국민은 통신의 비밀을 침해받지 아니한다.”는 규정은 해석상 ‘통신에 대한 패킷감청과 그에 대한 허가는 인정되지 아니한다’는 내용을 포함하고 있다. 이미 패킷감청이 행해지고 있으며 이것이 통신비밀보호법상 허용되는 것이라는 의견과 판단은⁴⁰⁾ 위헌적인 해석으로서 이러한 해석은 허용되어서는 안된다. 패킷감청의 적법성을 전화감청으로부터 유추하기도 하지만, 휴대폰을 비롯한 전화 통화 내용과 인터넷 활동 내용은 그 범위에 있어서 엄청난 차이가 있다.

39) 김철수, 헌법학개론, 박영사, 2007, 643.

40) 예를 들면, 서울중앙지방검찰청 윤상호검사가 작성한 “검찰 의견서”(2009.10.14). “○ 일부 감청허가서에 허가된 인터넷 회선 감청의 경우 기술적으로 변호인 주장과 같은 패킷감청이 가능한 것은 사실입니다.” “○ 하지만, 인터넷 회선 감청은 통신비밀보호법상 적법한 감청입니다. ※ 집행과정에서 수사대상자 외의 자가 송·수신하는 전기통신이 지득·채록될 가능성을 배제할 수 없으나, 이는 전화회선에 대한 감청의 경우와 다르지 않고 집행상 유의할 부분이라고 할 것입니다. - 즉 본건의 경우 설사 인터넷 회선 감청을 하였다고 하더라도 통신비밀보호법의 허가요건, 집행절차에 따른 것으로 적법합니다.”

IV. 통신비밀보호법의 개정방향

패킷감청은 헌법상으로는 물론 통신비밀보호법상으로도 허용될 수 없다. 그런데 마치 패킷 감청이 통신비밀보호법상 허용될 수 있는 것처럼 오해하는 것은 통신비밀보호법 자체가 모호하게 규정되어 있기 때문이다.

패킷감청에 대한 논란이 제기된 후 통신비밀보호법 개정안이 제출되었다. 이정현의원안⁴¹⁾은 제6조 제6항⁴²⁾에 후단을 신설하고 있다. 즉 “이 경우 인터넷 회선에 대한 감청의 허가서에는 전자우편의 내용, 접속한 인터넷홈페이지의 주소, 인터넷홈페이지의 게시판 또는 대화방 등에서 게시한 의재지의검색한 정보목록 등 대통령령으로 정하는 바에 따라 그 대상과 범위 등을 구체적으로 특정하여 기재하여야 한다.”는 것이다. 그러나 이 법안은 패킷감청에 대한 제한이 법률 문언상으로는 존재하지만 현실적으로는 존재할 수 없는 것이어서 사실상 패킷감청의 법적 근거를 마련한 것으로 귀결될 뿐이다.

따라서 헌법적 관점에서는 패킷감청이 절대적으로 금지되어야 한다는 규범기준으로 접근해야 한다. 그것은 통신비밀보호법상의 감청허가 절차 자체를 엄격하게 제한하는 내용을 담는 것이다.

첫째, 통신비밀보호법의 감청허가 절차는 감청에 대한 정의부터 법원의 허가에 이르기까지 구체화되어 있지 않은 헌법적 문제를 안고 있다. 먼저 감청이 “전기통신에 대하여 당사자의 동의 없이 전자장치·기계장치등을 사용하여 통신의 음향·문언·부호·영상을 청취·공독하여 그 내용을 지득 또는 채록하거나 전기통신의 송·수신을 방해하는 것”(법 제2조 제7호)으로 포괄적으로 정의되어 있다. 이것이 허가의 전제 개념이어서 법이 허용하는 감청의 범위를 명확하게 제한하고 있지 못하다.

참고로 일본의 ‘범죄수사를 위한 통신감청에 관한 법률’ 제3조는 “판사가 발부하는 감청영장에 의하여 전화번호 기타 発信元 또는 발신처를 식별하기 위한 번호 또는 부호(이하 “전화번호 등”이라 한다)에 의하여 특정된 통신의 수단(이하 “통신수단”이라 한다)으로서 피의자가 통신사업자 등과 맺은 계약에 의거하여 사용하고 있는 것(범인에 의한 범죄관련통신에 사용된다고 의심할 수 없다고 인정되는 것을 제외한다) 또는 범인에 의한 범죄관련통신에 사용된다고 의심할만한 것에 대하여 이를 사용하여 행하여진 범죄관련통신의 감청을 할 수 있다.”(밑줄은 인용자)고 규정하고 있다.

41) 2009.12.11.

42) 제5항의 허가서에는 통신제한조치의 종류·그 목적·대상·범위·기간 및 집행장소와 방법을 특정하여 기재하여야 한다.

이러한 입법태도는 패킷감청이 허용되는지 여부를 고려할 여지를 남기고 있지 않다. 따라서 감청의 개념 자체를 특정 번호 등에 의해 특정된 통신수단에 대하여만 할 수 있는 것으로 명확히 함으로써 패킷감청을 불법적인 것으로 명시해야 한다. 그리 되면 통신비밀보호법 제 16조 제1항 제1호에 따라 패킷감청을 한 자는 10년 이하의 징역과 5년 이하의 자격정지에 처해질 것이다.

둘째, 법관에게 청구되는 허가신청서의 정보가 상세하게 규정되어야 한다. 참고로 미국 연방법전 제18편 범죄 및 형사소송 절차는 감청 허가를 신청함에 있어 다음과 같은 정보가 포함될 것을 요청하고 있다.

- “(a) 신청서를 작성하는 수사관 또는 법 집행관과 신청을 인가하는 공무원의 신원
- (b) 다음 사항을 포함하여 명령서 발부가 필요하다는 믿음을 정당화하기 위하여 신청자가 의지하고 있는 사실과 정황에 대한 충분하고 완전한 기술
 - (i) 이미 실행되었거나 현재 실행 또는 계획되고 있는 특정 범죄에 관한 상세한 설명
 - (ii) 제11항⁴³⁾에 규정된 것을 제외하고, 감청설비의 특성과 위치 또는 통신이 감청되는 장소에 관한 특별한 기술
 - (iii) 통신이 감청되는 방식에 관한 특별한 설명
 - (iv) 신원이 파악되었을 경우, 범죄 행위자와 감청대상자의 신원
- (c) 다른 수사 절차가 시도되어 실패한 적이 있는지 여부와 그러한 절차가 시도되더라도 성공하기 어렵다든지 또는 너무 위험한 것으로 판단하는 이유에 관한 충분하고 완전한 기술
- (d) 감청이 필요한 기간에 관한 기술. 수사의 성질상 기술된 유형의 통신이 최초 획득될

43) 통신이 감청되는 설비에 관한 세부 설명이나 그 장소에 관련되는 본 조의 제1항(b)(ii)와 제3항(d)의 요건은 다음과 같은 경우 적용하지 아니한다.

- (a) 대화감청에 관한 신청에 있어서
 - (i) 신청이 연방수사관이나 법 집행관에 의하여 이루어져 법무장관, 법무부장관, 법무차관, 법무차관보나 법무차관보 대리가 인가하고
 - (ii) 신청서가 위와 같은 세부설명이 실현가능하지 않다는 완전하고 충분한 해명을 포함하고 있고 범죄 혐의자에 대한 신원과 그 혐의자의 통신이 감청된다는 사실을 소명하고 있으며
 - (iii) 판사가 위와 같은 세부설명이 실현가능하지 않다고 판단하는 경우
- (b) 유선 또는 전자통신 감청에 관한 신청에 있어서
 - (i) 신청이 연방 수사관이나 법 집행관에 의하여 이루어져 법무장관, 법무부장관, 법무차관, 법무차관보 또는 법무차관보 대리가 인가하고
 - (ii) 신청서가 범죄 혐의자에 대한 신원과 그 혐의자의 통신이 감청된다는 사실을 소명하고 있고, 그 혐의자의 행동이 특정한 설비로부터의 감청을 방해할 소지가 있다고 믿을만한 상당한 이유가 있다는 사실을 제시하고 있으며
 - (iii) 판사가 위와 같은 소명이 적절하게 되었다고 인정하고 있고
 - (iv) 신청서에 소명된 사람이 감청대상 통신이 전송되거나 전송된 기기에 근접하여 있거나 근접하고 있었다고 추정할 만한 상당한 이유가 있는 때에만 감청허가 또는 승인명령이 감청을 허용하는 경우

때 감청허가가 자동적으로 종료되어서는 아니 되는 경우, 동일한 유형의 통신이 추가 발생하리라 믿을만한 사유에 대한 특별한 기술

- (e) 신청서에 명기된 동일 인물, 감청설비 또는 장소와 관련되는 유선통신, 대화 또는 전자 통신의 감청허가를 신청한 자가 알고 있는 과거의 모든 신청에 관한 사실과 위와 같은 각각의 신청에 대하여 판사가 취한 조치에 관한 충분하고 완전한 기술
- (f) 연장을 신청하는 경우, 감청으로 그때까지 입수된 결과에 대한 상세한 설명과 그러한 결과의 입수에 실패한 경우 그에 대한 합당한 설명”

이러한 규정은 통신비밀보호법이 천명하고 있는 보충성원칙과 최소성원칙이 당연히 내포하고 있는 구체화 내용이라 할 것이다. 그런 점에서 감청 허가 신청의 남용을 막고 그에 대한 법원의 통제를 강화하기 위해서 이러한 내용을 통신비밀보호법에 추가해야 할 것이다.

또한 감청을 허가하는 판사가 감청의 필요성을 실질적으로 심사할 수 있는 권한을 부여해야 할 것이다. 참고로 미국에서 “판사는 신청자에게 신청 사유를 뒷받침할 수 있는 추가증언이나 서면 증거의 제출을 요구할 수 있다.”

셋째, 통신비밀보호법은 감청의 허가를 피의자 관점에서만 규정함으로써 그 통신상대방의 통신의 자유와 사생활의 비밀과 자유를 무시하고 있다. 보충성원칙을 적용한다면, 감청허가의 경우 법관으로 하여금 상당관계에 있는 통신상대방과의 통신에 대하여만 한정적으로 적시를 해야 할 것이다.

참고로 미국 제2518조 제3항은 감청의 허가요건으로서 ① 범죄 실행의 개연성 ② 증거획득의 개연성 ③ 보충성 ④ 해당 감청설비의 수사대상과의 관련성을 요구하고 있다.

“(3) 신청서를 제출 받은 판사는 신청자가 제출한 사실들을 토대로 다음과 같이 결정하는 경우 판사가 재직하고 있는 법원의 영토관할권 내(그리고 같은 관할권 내의 연방법원에 의하여 허가된 이동감청장비의 경우 연방내에서는 그 관할권 밖이라고 해당됨)에서 유선통신, 대화 또는 전자통신의 감청을 요청한 대로 또는 수정하여 허가하거나 승인하는 명령서를 발부할 수 있다.

- (a) 어떤 개인이 본 장의 제2516조에서 열거한 범죄를 실행하였거나 실행 또는 계획하고 있다고 믿을 만한 상당한 이유가 있다고 결정하는 경우
- (b) 그러한 범죄와 관련된 특정한 통신이 감청을 통하여 수집될 것이라고 믿을 만한 상당한 이유가 있다고 결정하는 경우
- (c) 통상적인 수사절차가 이미 시도되어 실패하였거나 시도하더라도 합리적으로는 성

공하기 어렵거나 너무 위험한 것이라고 판단된다고 결정하는 경우

- (d) 제11항에 제시된 것을 제외하고, 유선통신, 대화 또는 전자통신이 감청되는 설비 또는 장소가 그 같은 범죄와 관련하여 사용 또는 사용될 예정이거나 이러한 범죄 혐의자에 의하여 임차 또는 일반적으로 사용되고 있다고 믿을만한 상당한 이유가 있다고 결정하는 경우”

이렇게 통신비밀보호법이 개정되어야 통신비밀보호법상 패킷감청이 가능하다는 해석을 불식시킬 수 있을 것이다. 또 그래야만 그동안 제대로 드러나지는 않았지만 공공연한 비밀처럼 인정되었던 패킷감청의 관행이 형사 처벌을 통해서 사라질 수 있을 것이다.

덧붙여 통신비밀보호법이 규정하고 있는 통신수단을 그 성질에 따라 구분하여 규정할 필요가 있다. 통신비밀보호법상 통신은 ‘우편물 및 전기통신’을 의미하고(동법 제2조 제1호), ‘이메일 등의 저장 데이터’와 관련하여 문제가 되는 ‘전기통신’에 대하여는 ‘전화·전자우편·회원제정보서비스·모사전송·무선호출 등과 같이 유선·무선·광선 및 기타의 전자적 방식에 의하여 모든 종류의 음성·문언·부호 또는 영상을 송신하거나 수신하는 것’이라고 규정하고 있다(동법 제2조 제3호). 일반적인 대화를 시작으로 유선전화·팩스·무전기는 물론 휴대전화·인터넷으로 전달되는 각종의 정보(인터넷 전화를 통한 대화나 채팅)와 전자적 우편물(문자메시지나 이메일) 등 현재 존재하는 모든 통신매체들을 망라하여 무작위로 포섭하고 있는 이러한 입법태도는 적절하지 않기 때문이다.⁴⁴⁾

V. KT의 '맞춤광고'와 패킷감청⁴⁵⁾

KT는 이른바 '맞춤광고'에 패킷감청을 상업적으로 이용하려고 한다. '쿡 스마트웹(Qook Smartweb)'이 그것이다. 이것은 영국의 폼(Phorm)사가 개발한 'Webwise'라는 맞춤형 광고시스템의 수입품이다. 그 내용은 이용자가 현재 보는 이메일과 사이트 내용에 맞추어 광고를 내보내겠다는 것이다.

본격적인 DPI 논란은 미국 인터넷 광고업체인 네부에드(NebuAd)가 '행동기반 맞춤형 광고 시스템(behavioral targeting advertising systems)'을 개발하여 이를 세인트루이스주의 ISP인

44) 이에 대하여는 오길영, “통신비밀보호법 개정안 비판,” 민주법학 제34호, 민주주의법학연구회, 2007.9, 378-381.

45) 오길영, 앞의 글, 415-417에서 원래의 각주를 제외하고 발췌하여 전재한 것임.

‘차터 커뮤니케이션즈(Charter Communications)’에 판매한 것에서 시작되었다. 당해 광고시스템은 ISP 가입자들의 인터넷 사이트 방문내역을 추적해 개별 관심사에 부합하는 맞춤형 광고를 제공하는 한편, ISP로 하여금 온라인 광고 수익을 누릴 수 있도록 하는 일종의 지능형·맞춤형 광고시스템이다.

그러나 시민단체들은 이러한 광고서비스가 인터넷 사용자들의 웹서핑 내역을 추적·수집·분석한다는 점, 그리고 그러한 사실을 정확히 알리지도 않거나 제대로 된 동의를 받지도 않았다는 점 등을 이유로 프라이버시 문제를 제기하였다. 이러한 사실이 이슈가 되자 ISP인 차터 커뮤니케이션즈는 내부에드의 사용을 무기한 연기하였다.

이렇게 DPI 기술로 인해 프라이버시 침해의 논의가 부각되자 이것은 주로 ECPA 위반으로 논의되었다. 그러나 맞춤형 광고시스템의 경우에는 이를 적용하기가 쉽지 않았다. 왜냐하면 ECPA상의 예외규정에 해당하기 때문인데, 특히 ‘인터넷 사용자의 동의’가 있었다는 것이 핵심적 이유이다. 상황이 이러하자 입법의 필요성이 부각되어, 결국 의회에서 법안 작업에 착수하기에 이르렀다. 에너지 및 상업위원회(Committee on Energy & Commerce) 차원에서 DPI 관련업체에 대한 실태조사 증언이 있었으며, 법안의 주요내용으로는 ‘정보 수집에 대한 동의 요건’, ‘정보의 수집방법과 수집된 정보의 활용상황에 대한 공개’ 등이 논의되고 있다.

그러나 맞춤형 광고시스템에 대한 영국의 입장은 달랐다. 영국의 정보위원회(The Information Commissioner's Office, ICO)가 폼(Phorm)사의 DPI기술에 대하여 ‘사용자의 선택권이 있는 한 DPI는 위법이 아니다’라는 공식 입장을 내놓은 것이다. 상황이 이렇게 되자, 이번에는 유럽위원회(European Commission, EC) 차원에서 이러한 영국정부의 대응을 문제 삼고 나왔다. ‘EU 데이터 보호규약(1995 EU Directive concerning Data Protection)’과 ‘EU 전자통신규약(2002 EU Directive concerning Electronic Communication)’의 위반이라는 것이다.

일반적인 DPI에 대한 실정법적 해석은 자명하다. 그것은 감청법 위반이다. 우리나라의 경우 통신비밀보호법 제3조 1항의 위반이 되고, 미국의 경우에는 ECPA § 2511(a)(1)의 위반이 된다. ‘DPI형 맞춤 광고 시스템’은 표면상의 형태에 있어서는 사용자 친화적인 색채를 띠는 혼한 상업프로그램인 것처럼 보인다. 그러나 그 실체에 있어서는 감청회선의 제공자와 감청수단의 개발자가 결탁한 형태이다. 그것은 제3자인 KT가 통신의 송신자와 수신자 양당사자의 동의를 모두 구하지 않은 채 이용자의 통신내용을 감청하는 것으로서, 엄연히 현행 통신비밀보호법 위반이다.

그러나 미국의 사례에서 보듯 DPI는 일반적인 도청이나 데이터 리텐션(Data Retention)과는 달리 서비스나 프로그램 등의 수많은 형태로 변모할 수 있는 디지털 기술이다. 그렇기 때

문에 이것에 대하여 기존의 감청법 체계로 규제하기란 불가능에 가깝다. 디지털 매체에 관하여 우리나라보다 훨씬 더 정교한 체계를 가지고 있는 미국에서조차 새로운 입법을 준비하고 있다는 점이 그것을 증명한다.

설령 새로운 입법을 시도하는 경우에도 패킷감청 기법을 이용한 ‘맞춤광고’에 대하여 헌법에 합치되는 방식으로 법률적 규제를 하기란 불가능해 보인다. 그때그때 양당사자의 동의가 모두 있는 경우에만 관련 정보를 수집할 수 있을 것인데, 이것은 현실적으로 가능하지 않기 때문이다. 사실상 양자 모두 포괄적 정보에 대해 동의를 하지 않는 이상 개별적인 구체적 정보마다 동의하는 키를 누르느라 인터넷을 이용할 수 없게 될 것이기 때문이다. 사업자가 서비스 제공을 미끼로 포괄적 정보에 대한 동의를 사실상 강요한다면 그것은 기본권 침해이기 때문에 헌법적으로 허용될 수 없다.

따라서 통신비밀보호법 제3조에 제4항을 신설하여 “전기통신에 의한 정보수집에 대하여 당사자의 동의가 있다고 하더라도 일방당사자의 포괄적 동의에 근거한 정보수집 활동은 불법감청으로 본다.”고 명확하게 규정할 필요가 있다.

VI. 나오는 글

결론적으로 패킷감청은 헌법적으로 절대 허용될 수 없는 절대금지의 영역이다. 즉 그것은 헌법 제37조 제2항 단서의 본질적 내용 침해에 해당하는 것이어서 금지된다. 따라서 헌법 제18조 “모든 국민은 통신의 비밀을 침해받지 아니한다.”는 규정은 해석상 ‘통신에 대한 패킷감청의 허가는 인정되지 아니한다’는 내용을 포함하고 있다.

국가권력과 개인의 기본권의 역전현상은 헌법의 근간을 흔든다. 헌법재판소는 국가안보에 대하여 한 치의 빈틈도 없게 하려 하지만, 그 때문에 국민의 기본권은 숨 쉴 수가 없다. 개인의 사생활의 비밀과 자유의 영역이 줄어들고 있지만, 국가의 비밀의 영역은 날로 팽창일로에 있다. 통신의 자유도 마찬가지이다. 근본적인 대책이 필요하다.

헌법 제37조 제2항은 기본권을 제한하는 입법을 옹호하는 이들의 금과옥조이다. 그 때문에 단서인 본질적 내용 침해 금지 원칙은 거의 죽어 있다. 반면 집회·시위의 자유를 제한하기 위하여 법원 담장의 경계지점으로부터 100m 이내에서 절대적 시위금지 구역은 살아 있다. 그만큼 집회·시위의 자유는 질식 상태이다.

기본권 문제에 있어서 우리는 늘 타협을 강요당한다. 기본권의 절대적 보호영역은 늘 내심

의 영역에만 머물러 있다. 그 내심의 확장된 공간으로서 통신은 철저히 상대화될 것을 강요당한다. 과학기술의 발전이 오히려 인간의 자유 공간을 위축시키고 있는 셈이다. 그것은 필연적이거나 숙명적인 것이 아니다. 오히려 우리의 자유 공간을 절대적 침해금지 구역으로 확보하는 것은 인권의 관점에서 민주주의적으로 방어해야 할 정당한 몫이다. 패킷감청이 바로 그러한 절대적 금지구역이어야 한다. 어떠한 방식으로든 패킷감청을 법적으로 정당화하는 것은 결국 헌법의 근간을 부정하는 셈이다. 국민투표를 거쳐 헌법을 개정하여 그 근거를 마련한다고 하더라도 패킷감청은 정당성 부재를 넘어 ‘헌법적 불법’⁴⁶⁾일 뿐이다.

46) 라드브루흐가 사용한 ‘법률적 불법’(Radbruch, Gustav, 이재승 옮김, “역주: 법률적 불법과 초법률적 법,” 법철학연구 제 12권 제1호, 한국법철학회, 2009, 1-26)으로부터 차용한 변형어이다. 특정 헌법조항 또한 헌법 자체가 불법성을 띠는 경우이다. 대표적으로는 1972년의 이른바 ‘유신헌법’을 그 예로 들 수 있을 것이다.



- 권영성, 헌법학원론, 법문사, 2008.
- 권정호, “2009고합731 국가보안법위반 사건 의견서,” 제출처: 서울중앙지방법원 제25 형사부, 2009.11, 총 8쪽.
- 김승환, “헌법과 민주주의,” 민주법학 제31호, 2006.
- 김철수, 헌법학개론, 박영사, 2007.
- 오길영, “통신비밀보호법 개정안 비판,” 민주법학 제34호, 민주주의법학연구회, 2007.9.
- 오길영, “인터넷 감청과 DPI(Deep Packet Inspection),” 민주법학 제41호, 민주주의법학연구회, 2009.12, 391-426.
- 정종섭, 헌법학원론, 박영사, 2009.
- 진보네트워크센터, “패킷 감청 의견,” 2009.10.29
- 선진한국을 위한 통신비밀보호법 개정방향, 주최: 국가안보전략연구소, 2009.12.1.
- Agamben, Giorgio, 박진우 옮김, 호모사케르: 주권 권력과 벌거벗은 생명, 새물결, 2008.
- Crocker, Thomas P., FROM PRIVACY TO LIBERTY: THE FOURTH AMENDMENT AFTER LAWRENCE, UCLA law review 제57권 제1호, 2009, 1-70.
- Michelman, Scott, WHO CAN SUE OVER GOVERNMENT SURVEILLANCE?, Michelman, Scott ; UCLA law review 제57권 제1호, 2009, 71-114.
- Ohm, Paul, “The Rise and Fall of Invasive ISP Surveillance,” Working Paper Number 08-22, Legal Studies Research Paper Series, 2008.9.9, 1-82.
- Radbruch, Gustav, 이재승 옮김, “역주: 법률적 불법과 초법률적 법,” 법철학연구 제12권 제1호, 한국법철학회, 2009, 1-26.
- Wong, Thomas, Regulation of Interception of Communications in Selected Jurisdictions, research and Library Services Division, Legislative Council Secretariat, 2005.2.2, <http://www.legco.gov.hk/yr04-05/english/sec/library/0405rp02e.pdf>, 검색일: 2009.12.3.

.....패킷감청의 문제점과 개선방안에 대한 토론회

02

DPPI 기술 활용 민간 관심기반 광고서비스의 문제점 검토

임 종 인

(고려대 정보보호대학원 교수)

DPI 기술 활용 민간 관심기반 광고서비스의 문제점 검토 : KT Qook Smartweb을 중심으로

고려대학교
정보경영공학전문대학원/정보보호연구원
임 종 인

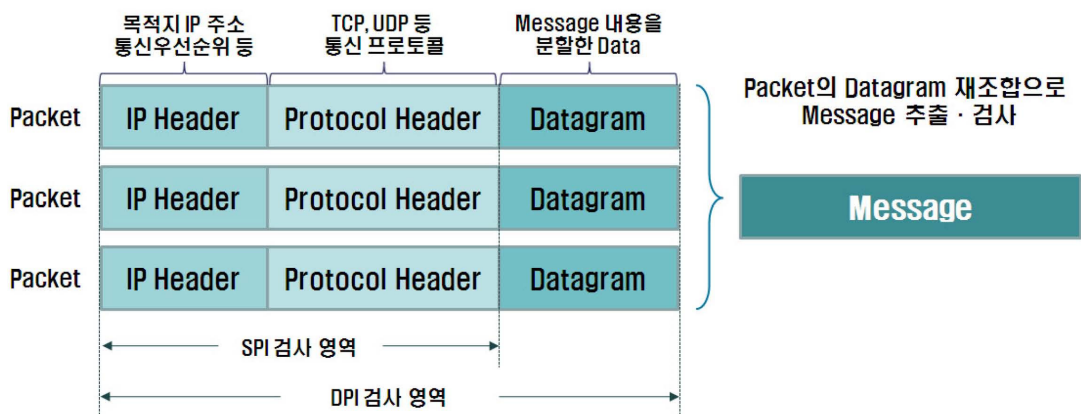
- 1 DPI의 기술 개요
- 2 Qook SmartWeb Service
- 3 예상 문제점
- 4 대응책

DPI (Deep Packet Inspection) 기술 개요

Deep Packet Inspection 기술 개요

기존 네트워킹이나 방화벽이 사용하는 SPI (Shallow Packet Inspection)
기술은 패킷의 IP Header, Protocol Header만 검사

DPI (Deep Packet Inspection) 기술의 경우
패킷의 Datagram을 재조합하여 Message 추출 · 검사

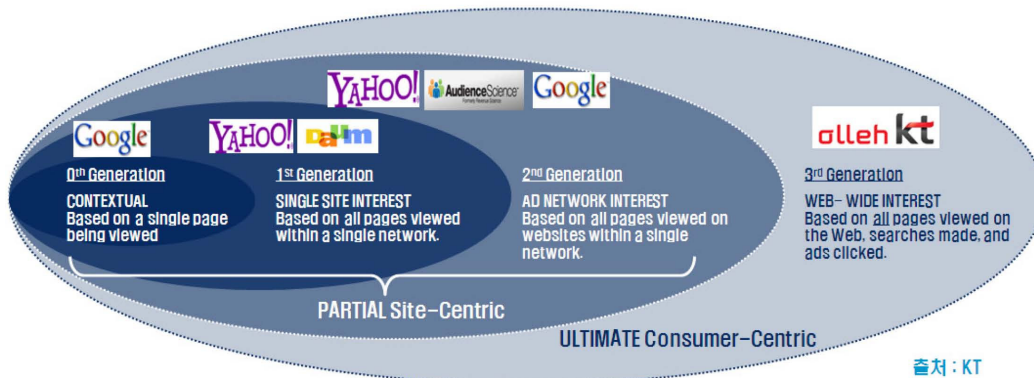


DPI 기술의 다양한 용도



Qook SmartWeb Service

KT SmartWeb의 특징과 차별점

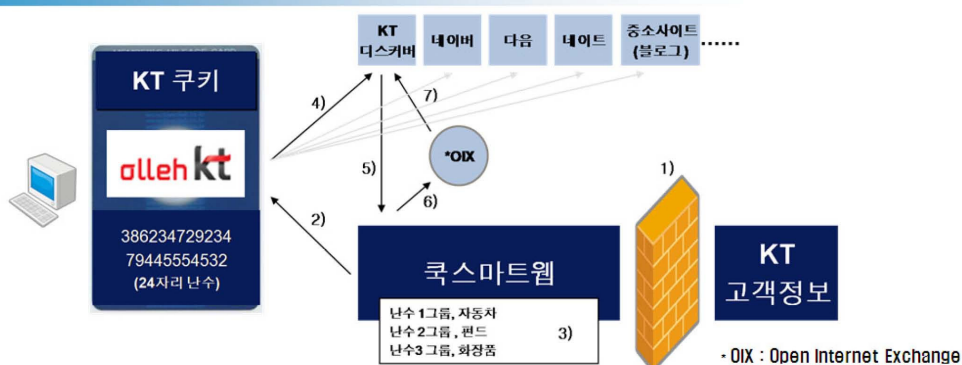


인터넷 서비스 사업자가 아닌 망사업자에 의한 DPI 기술의 활용

기존의 특정 페이지, 특정 웹사이트, 특정 네트워크 기반의 기존 방식과 달리 개인의 웹에서의 모든 행위를 대상으로 하는 관심기반 광고서비스임

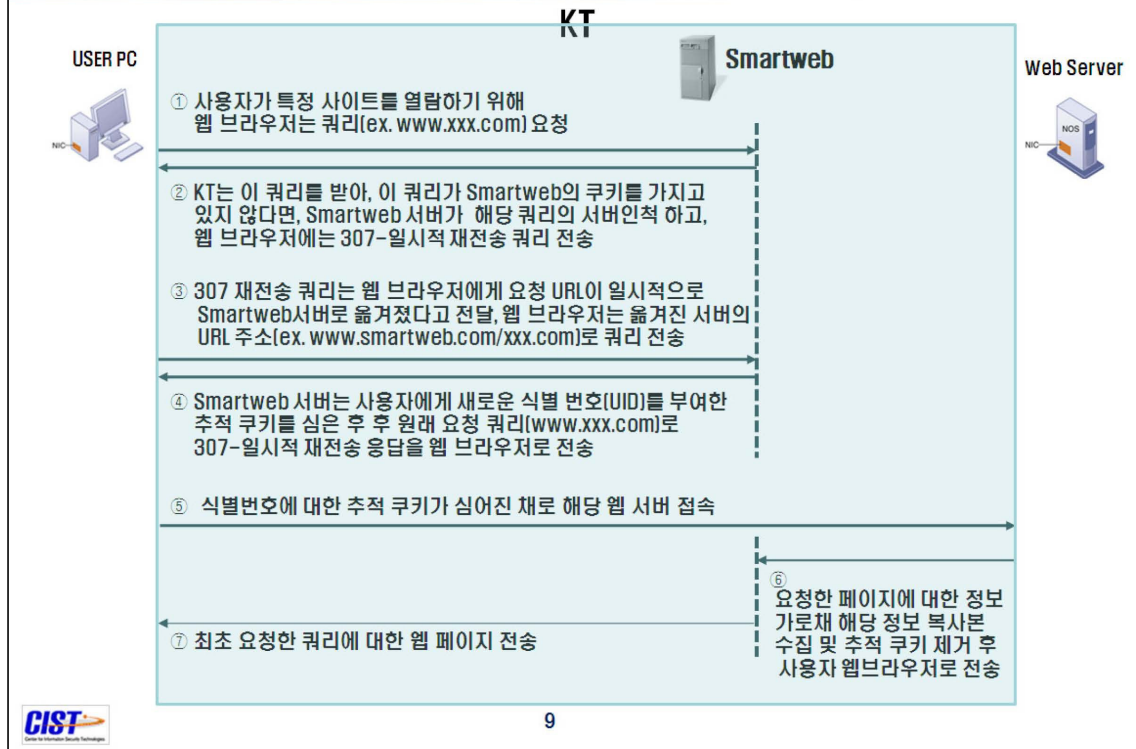
다른 서비스에 비해 잠재적 프라이버시 침해 위험이 광범위할 가능성이 존재함

KT SmartWeb 서비스 개요



- 1) KT고객정보와 차단
- 2) 24자리 난수를 쿠키에 담아 동의한 고객의 PC에 전송 : 코스마트웹 상에는 난수 번호로만 식별
- 3) 네트워크 단에서 난수를 기준으로 사전에 정의된 관심표에 따라 난수를 관심표 별로 그룹핑
- 4) PC(이용자)가 제휴된 사이트를 방문하면 PC(브라우저)가 난수를 사이트로 전달
- 5) 제휴된 사이트의 코스마트웹 경로를 통해 난수가 코스마트웹에 전달
- 6) 난수가 어떤 관심표 그룹에 속하는지 확인 후, 관련 콘텐츠 혹은 광고를 보내도록 명령
- 7) 사이트의 지정된 위치에 맞춤 콘텐츠 및 광고 전송

KT SmartWeb 서비스 원리



DPI 기술의 예상 문제점

민간의 DPI 기술 사용의 법적 문제

미국의 DPI 관련 법률적 논의

민간의 DPI 기술 사용에 대한
ECPA
(Electronic Communication Privacy Act)
적용 여부 논란

잠재적 프라이버시 침해 위험 높음에도
ECPA의 동의의 예외 규정으로 규제 불가

민간의 DPI 마케팅 기술 규제를 위한
법안 입법 필요성 대두됨에 따라
의회의 전담입법 법안 제정 논의 착수

영국 및 EU의 DPI 관련 법률적 논의

영국 ICO는
ISP의 DPI 기술 사용은 Opt-in 제공 시
불법 아니라는 입장 발표

EC (European Commission)의 지적
· 영국 실정법 사용자중심 재편해야 함
· 영국에는 사용자들이 데이터가
유출되거나 오남용 되기 전 동의서를
받을 수 있는 법제도적 장치가
마련되어 있지 않음
· EU 데이터보호지침(1995) 및
EU 전자통신지침(2002) 위반 지적

국내에서도 법률상 · 헌법상 유사한 논란

KT Qook SmartWeb 서비스 동의방식의 문제점

취급되는 정보의 항목 및 이용 기간은 어떻게 됩니까?

주키를 기반으로 웹 이용정보를 공간적으로 집중하여 과실방지, 관심 기반 서비스 및 광고를 제공 합니다.

위 사항을 유념하여 동의해 주시기 바랍니다.

* 웹 이용정보란 키워드, URL, 이용 사이트, 쿠키, 방문 횟수, 10개 이내, 랜덤번호, 쿠키고, 쿠키고, 리 분류시간 생성(생성된 정보는 6개월 저장 및 관심 서비스 및 광고 제공 시 사용) 후 실시간으로 삭제됩니다.

위 서비스 제공을 위하여 KT가 보유하는 기계적 데이터 과정에서 웹 이용 정보가 아닌 트래픽 정보의 일부가 포함될 수 있으나 모든 트래픽은 쿠키고, 시간 기록으로만 데이터 된 후 바로 삭제 됩니다.

☐ 동의

현존 고객 동의서

목적, 취급 정보항목, 이용기간 등 명시

동의버튼

간단한 경고 웹 이용정보 이외 정보 포함가능

고객 동의서 추가사항

잠재적위험의 심각성 명시적 고지 후 동의절차

오용 및 사고에 의한 침해 발생 시 배상책임 명시

웹 이용 정보 수집에 대한 안내의 강조 필요

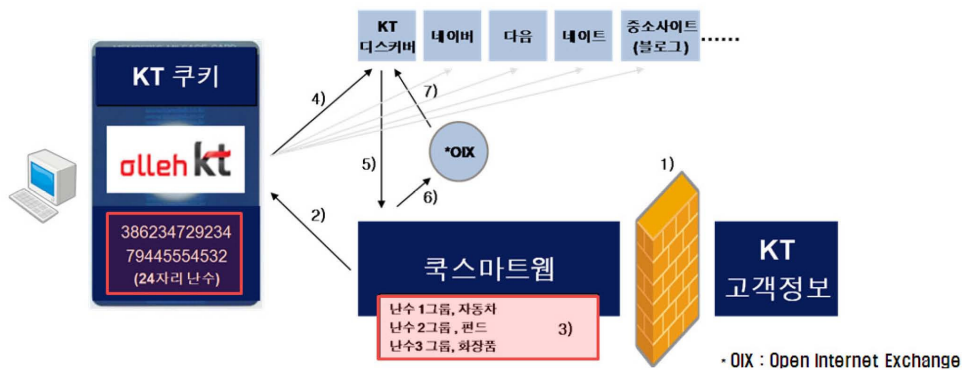
오용 및 사고에 의한 침해 발생 시 배상책임 명시

KT의 프라이버시 비침해 주장

- 서비스는 이용자의 동의를 전제로 함
- 언제든지 원하면 서비스 해지 가능
- 랜덤값/익명화 조치를 통한 개인 식별 정보 제거
- 활용데이터는 키워드/URL/페이지 키워드 뿐임
- 데이터들은 필터링 될 뿐 수집/저장 안 되고 삭제됨
- 서버에 저장되는 정보는 랜덤값/광고카테고리/시간값에 한정
- 해당 정보는 암호화되어 저장됨
- 공개되어 있는 http(80포트) 프로토콜만을 이용
- https 등 암호화된 금융정보, 메신저, 이메일은 대상이 아님
- 의료정보 등 민감 정보는 처리 대상이 아님

위의 이유로 감청이나 프라이버시 침해가 아니라고 주장함

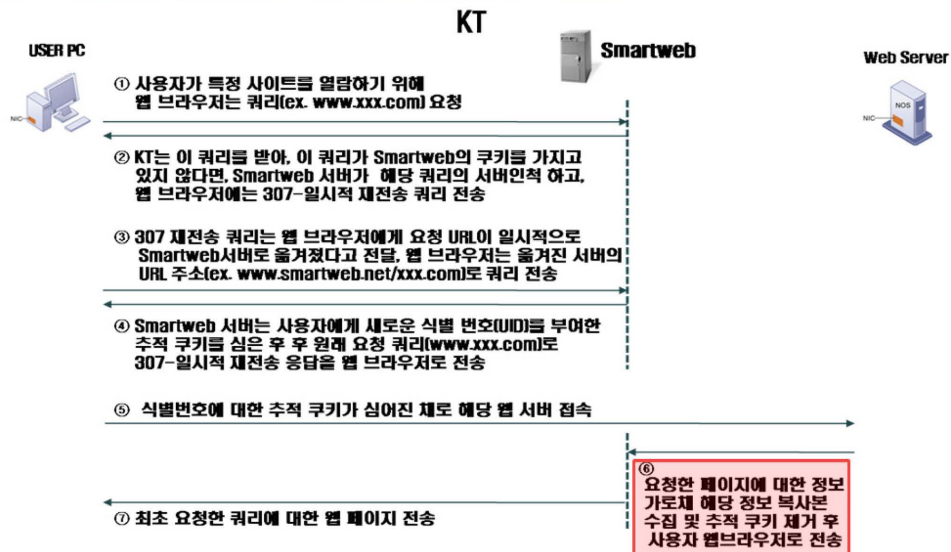
KT SmartWeb 기술의 문제점



내부적으로 특정 IP에 대한 난수값 추적 가능
→ IP와 성향정보 결합에 따른 오용 가능성

ISP의 DPI기술 설정에 따라 수집 범위 확대 가능 → 모든 패킷 수집 가능

KT SmartWeb 기술의 문제점



사용자의 인터넷 사용 기록 복사의 문제

KT 서비스의 잠재적 프라이버시 위험

KT의 주장이 성립하려면 선량한(Good-will) 기업을 상정해야 함

소비자 성향정보와 IP정보의 결합에 따른 프라이버시 침해 가능성

기술적으로는 ISP의 해당 기술 설정여부에 따라 모든 패킷 수집 가능

향후 수집 범위 및 관련 정책 변화 가능성

적법한 권한 없는 불법도청에 이용될 가능성

사전에 선의의 기업을 상정하는 것은 매우 위험함

해당 기업에 내부통제와 외부감사를 의무화하는 강력한 규제가 필요함

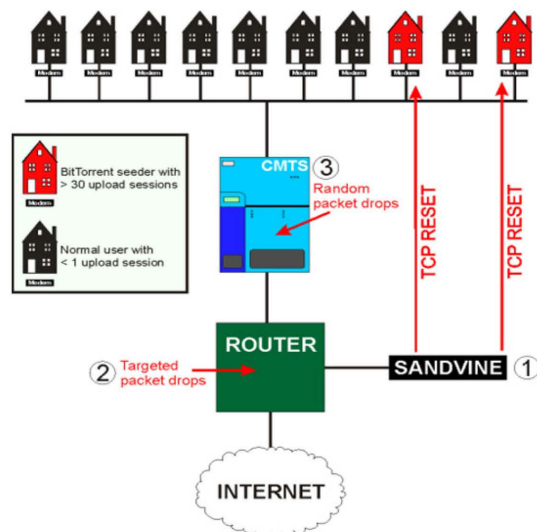
민간기관의 DPI 기술 사용 논란 사례

미국	Comcast사의 P2P 프로토콜 제한에 따른 망 중립성 논란
	NebuAd사의 <행동기반 맞춤형 광고시스템> ISP 판매 논란
영국	Phorm사의 <맞춤형 광고시스템> BT 도입 논란 (Webwise)
한국	Phorm사의 <맞춤형 광고시스템> KT 도입 논란 (Qook Smartweb)



미국 Comcast 사의 DPI 활용 P2P 프로토콜 제한

- 미국의 최대 케이블(네트워크)사업자인 컴캐스트(Comcast Corporation)가 자사의 인터넷 서비스 가입자들 중 BitTorrent라는 P2P 프로그램을 사용하는 가입자에 한해 당해 P2P 프로토콜을 제한하여 '망 중립성(Net Neutrality)' 논란
- P2P 프로그램으로 인해 전체 네트워크 정체가 빚어진다는 판단 하에, P2P 사용자들에 한해 인터넷 속도를 낮추는 기술적 제약을 가했는데, P2P 사용자를 구분하기 위해 DPI 기술 사용



미국 NebuAd 사의 행동기반 맞춤형 광고시스템



- 인터넷 광고 업체인 NebuAd는 <행동기반 맞춤형 광고시스템(Behavioral Targeting Advertising Systems)>을 개발하여 지역 ISP인 Charter Communications에 판매함
- Behavioral Targeting Advertising Systems은 ISP 가입자들의 인터넷 사이트 방문내역을 추적해 개별 관심사에 부합하는 맞춤형 광고를 제공하는 한편, ISP로 하여금 온라인 광고수익을 보장해주는 지능형 · 맞춤형 광고시스템임
- 시민단체들은 해당 광고서비스가 사실 고지 및 동의 없이 인터넷 사용자의 웹서핑 내역을 추적, 수집, 분석했다는 프라이버시 이슈를 제기하였고, 이와 관련한 의회 청문회까지 열림
- Charter Communications는 NebuAd사의 Behavioral Targeting Advertising Systems 사용을 무기한 연기했음



19

영국 BT사의 Phorm 서비스 논의 과정



2006	BT(British Telecom)사, 고객 동의 없이 Phorm 서비스 시험 실시
2006	영국정부, 사용자동의 획득 후 Phorm 서비스 실시를 결정
2008	Phorm사, BT 등 ISP 협력에 의해 OX 광고시스템 출시
2008	영국 공정거래위원회와 왕립검찰청의 BT 조사
2008.7	EU, Phorm사기술의 개인사생활 침해 가능성 경고
2009.7	BT, Phorm사의 타겟 광고 기술 도입 포기



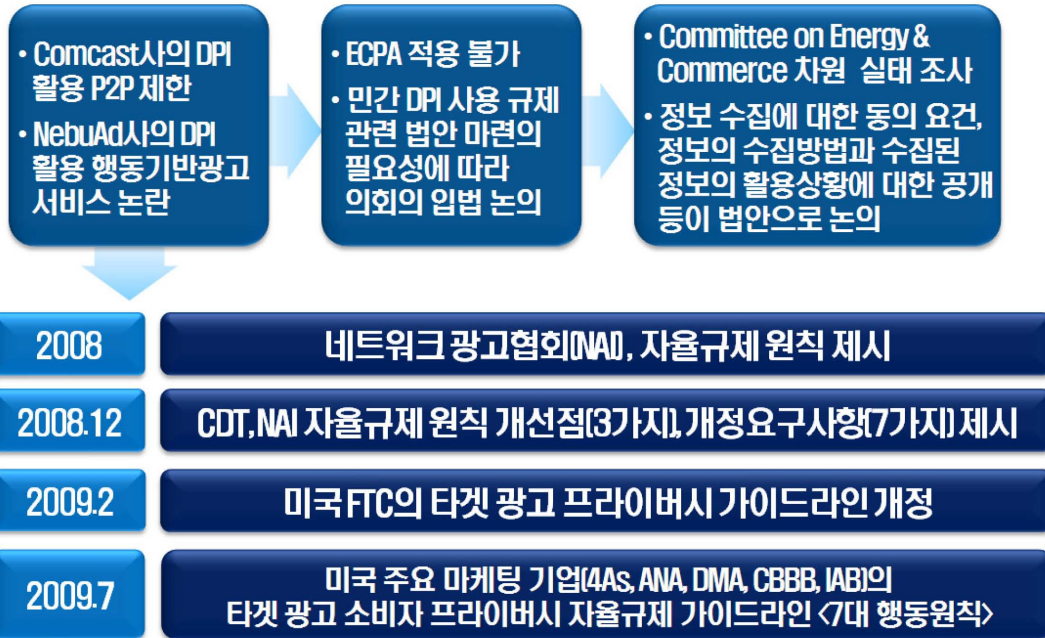
20

DPI 기술의 예상 문제점에 대한 해결 방안

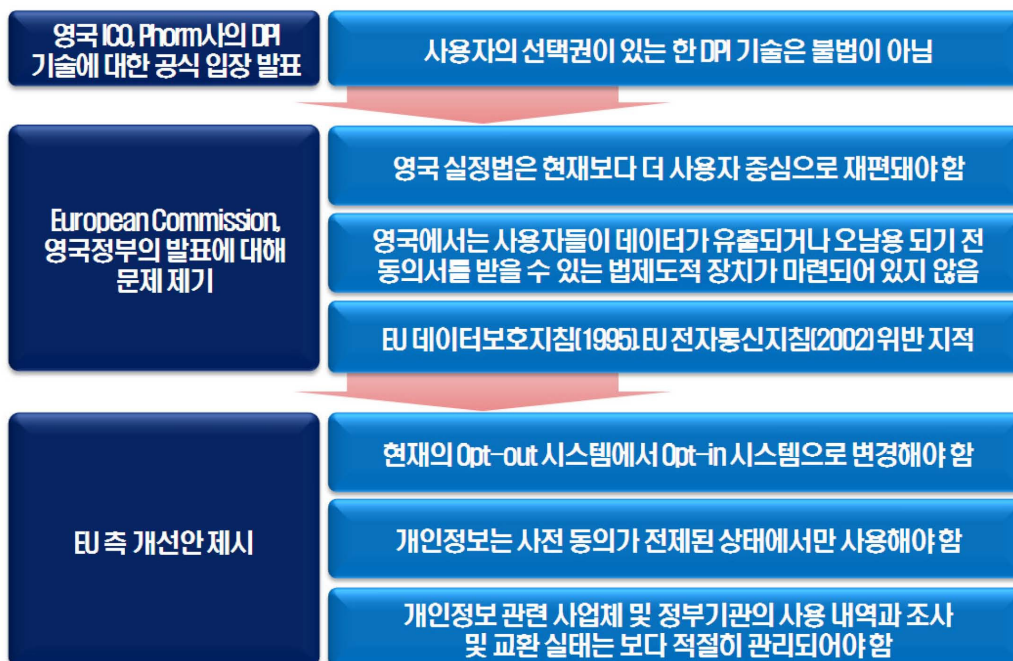
현대 마케팅 기술과 개인정보보호



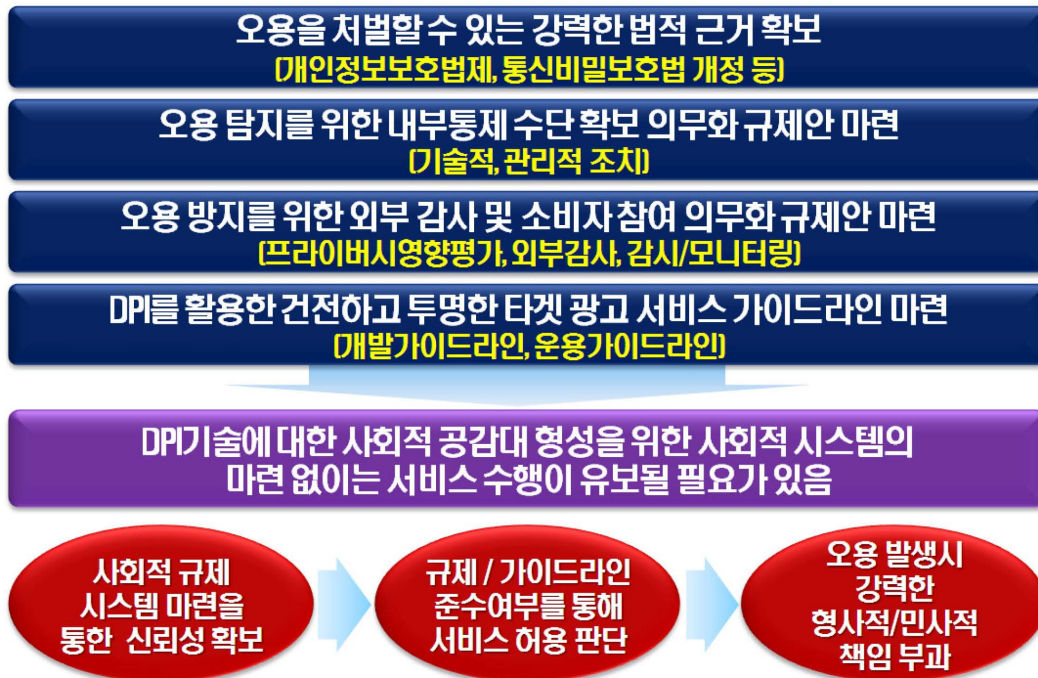
미국의 민간 DPI 기술 사용 관련 규제 사례



영국 및 EU의 민간 DPI 기술 사용 관련 규제 사례



KT SmartWeb 서비스에 대한 대응 방안



소비자 신뢰성 확대 및 사회적 합의 절차 개발

개인정보를 포함한 소비자데이터 통제권을 심각하게 위협할 수 있는 기술 및 서비스의 경우
의무적으로 통제권을 보장할 수 있는 기술적/절차적 장치를 마련하는 규제를 둘 필요가 있음





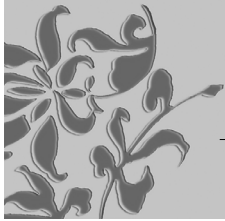
감사합니다

.....패킷감청의 문제점과 개선방안에 대한 토론회

03

토론문

권정호
(민주사회를 위한 변호사 모임)



1. 패킷감청의 실태

가. 패킷감청의 허용여부와 법적 규제를 둘러싸고 최근 전세계적인 논쟁이 일고 있는데, 한국에서는 2008년 남북공동선언실천연대 사건의 재판과정에서 국가정보원이 패킷감청을 실시한 사실이 최초로 드러난 이후, 2009년 범민련 사건에서는 검찰의 공소가 제기되기 6년 전인 2003. 7. 30.부터 2009. 5. 7. 구속시까지 단 하루도 빠지 않고 국가정보원이 관련 피고인들의 모든 통신내용을 감청하였는바, 검찰이 제출한 증거에 의하여도 국정원은 적어도 2004. 7. 30. 이후부터 범민련 남측본부 사무실 및 피고인 이경원의 자택에서 이용한 인터넷 통신내용을 패킷감청한 것으로 드러났다.

나. 범민련 사건의 경우 국정원이 법원의 통신제한조치허가서를 발부받아 피고인들(특히 피고인 이경원)에게 취한 통신제한조치는 크게 나누어 전기통신 감청, 우편물 검열, 대화녹음 청취 등이 있는바, 그 중 전기통신 감청의 경우 피고인들의 이메일은 다음, 네이버 등 해당 포털사업자들에 대한 압수수색영장에 의하는 이외에 위 포털사업자들이 피고인들의 특정계정을 그대로 복사하여 국정원에 제공하는 포워딩(forwarding) 방식에 의하여 취득한 것들이 대부분이지만, 범민련 남측본부 사무실에 설치된 (주)KT 인터넷 전용선에 대한 감청 및 IP 추적을 포함한 착발신지 추적은 회선사업자인 KT 등의 협조를 얻어 전부 패킷감청의 방식으로 이루어진 것이다.

다. 국정원은 2004. 10. 7. 범민련 남측본부가 사무실 인터넷 전용선을 기 사용중이던 '비대칭디지털가입자회선'(ADSL, 로그인 ID : bum615)에서 고속 데이터 전송이 가능한 '초고속디지털가입자회선'(VDSL, 로그인 ID : bum615)으로 변경하자 기존 ADSL에 대한 통신제한조치 집행을 중지하고 위 VDSL에 대한 통신제한조치가 필요하다고 사유를 내세

위 별도로 15일 기간의 통신제한조치허가서를 재신청까지 하여 2004. 11. 15.자로 발부 받았는바, 이는 범민련 사무실이 인터넷 회선방식을 변경함에 따라 국정원이 패킷감청의 기존 방식을 바꾸기 위하여 단기간의 허가서를 신청하여 발부받은 것으로, 범민련 사건에서 국정원이 패킷감청을 했다는 것에 대한 의문의 여지가 없는 명백한 증거이다.

2. 패킷감청의 기술적 특성

가. 전기통신기술의 발전은 감청기술 발전의 역사와 맥을 같이 할 정도로 정보수사기관에서는 새로운 전기통신기술이 출현하는 경우 그에 대한 감청설비까지 개발이 완료되어야 사업등록을 허가한다는 견해가 유력합니다. 아직도 국정원, 경찰청, 기무사 등 정보수사기관에서 사용하고 있는 인터넷 패킷감청 설비의 정확한 수량 및 종류는 베일에 가려져 있는 실정이다.

나. 인터넷 감청은 기술적으로 1) 백도어(back door) 방식 2) 포워딩(forwarding) 방식 3) 패킷감청(Packet Inspection) 등 3가지 방식이 있는데, 백도어 방식은 감청 대상자의 PC에 감청 프로그램을 심어서 원격에서 대상자가 PC를 작동하는 모습을 감청하는 것이고, 포워딩 방식은 포털이나 IPTV 등 플랫폼 사업자가 정보수사기관에 대상자의 복제계정을 제공하거나 실시간 데이터 전달을 통해 이루어지는바, 이런 경우는 보통 이메일이나 메신저의 통신내용을 감청할 때 많이 사용되고, 당연히 집행장소는 포털사업체가 됩니다. 반면에 패킷감청은 PC나 사업자를 통하지 않고 인터넷망을 직접 감청하는 방식으로 인터넷망을 이용하는 암호화되지 않은 모든 통신내용을 감청할 수 있는바, 일상적인 이메일, 메신저, 웹서핑, 블로그, 게시물 읽기쓰기는 물론 온라인 음악감상, 온라인 계좌이체, P2P 다운로드, 인터넷전화, IPTV 등 모든 인터넷 활동이 감청대상이 되고, 집행장소는 회선사업체가 된다.

3. 패킷감청의 위헌, 위법성

가. 통신제한조치는 통신의 속성상 불특정 다수의 상대방이 관계될 수밖에 없는 구조상 피의자의 통신상대방 중 피의자의 범죄행위와 상당정도 연관성이 있는 통신상대방과의 통신만이 감청대상으로 되어야 하고, 그것도 수사목적과 관련성이 있는 통신내용으로

범위가 명확히 한정되어야 하는 것이 헌법의 영장주의와 침해의 최소성·보충성을 규정하고 있는 통신비밀보호법의 취지에 부합한다. 따라서 패킷감청은 허가서 하나만으로 피의자만을 특정하여 그의 모든 통신상대방과의 통신을 감청할 수 있으므로 기본적으로 헌법적으로 성립할 수 없는 일반허가이면서, 동시에 수사목적과 무관한 모든 통신내용까지 무제한적 감청이 가능하여 헌법적으로 금지되고 있는 포괄허가이므로, 패킷감청은 헌법상 절대적으로 금지되어야 한다는 발제자의 주장에 전적으로 동의한다.

나. 패킷감청의 가장 큰 문제점은 감청 대상을 특정화하기 쉽지 않다는 점이다. 첫째, 보통의 가정이나 직장에서는 공유기 등을 통해 다수의 PC와 다수인이 해당 네트워크 서비스를 공동이용하므로 대상자의 PC를 임시적으로 다른 이가 사용할 수도 있다. 따라서 현재의 패킷 감청은 감청 대상자가 아닌 타인의 인터넷 통신 내용을 감청하게 되는 경우가 다수 있을 것이다. 그러나 외부에서 감청을 집행하는 입장에서는 지금 전송되는 패킷이 감청 대상자의 행위에 의해 송수신되는 것인지 알 수 없다. 따라서 감청 대상자를 특정할 수 없는 패킷감청은 각 피의자별로 감청이 이루어지도록 한 현행 「통신비밀보호법」에 위배되고(동법 제6조 제1항), 법정증거로서의 효력도 없다.

다. 둘째, 패킷 감청의 경우 특정 이메일이나 메신저에 대한 감청과 달리 서버로부터 대상자에게 전달되는 모든 통신내용을 대상으로 한다. 이 가운데에는 공개된 통신내용도 있을 수 있지만 비공개 통신내용도 있을 수 있는데, 비공개 통신내용은 단지 대상자가 이용하였다는 이유만으로 정보수사기관에 제공된다. 이 과정에서 이용자의 비밀번호 등이 제공될 가능성도 있는데, 이는 감청을 집행하는 과정에서 비밀번호가 누설되어서는 안된다는 통신비밀보호법의 취지에 위배된다(동법 제9조 제4호). 결국 패킷감청은 감청대상자와 무관한 제3자를 감청하는 결과를 낳을 수 있으며, 수사목적과 무관한 통신내용까지 무제한적으로 포괄감청한다는 것이 가장 큰 문제점인바, 포괄영장금지 원칙에 위반됨은 물론이고 심각한 프라이버시 침해에 대한 사법적 통제가능성이 전무한 상황이다.

라. 더구나 패킷이란 목적을 가지고 이동하는 통신 과정상의 자료로서 수사에 필요한 자료는 해당 패킷이 목적지에 도달한 후 기존의 포워딩 방식의 감청이나 압수수색으로도 충분히 입수가 가능하다. 여러 가지 통비법에 규정된 감청방식으로 위법한 패킷감청이 굳이 인정될 필요가 없는 것이다. 범민련 사건에서 국정원이 명백히 피고인들의 인터넷 활동을 패킷감청했음에도 그로 획득된 증거를 전혀 제출하지 않은 것은 바로 이 점을

말해주고 있는 것이다. 따라서 패킷감청은 정보수사기관이 달성하고자 하는 수사목적은 미미한데 비하여 그 기본권 침해의 정도가 너무 심각하여 현저하게 목적과 수단 간의 균형을 잃은 수사방법으로 비례원칙에 위반되는바, 헌법상 기본권제한의 본질적 한계를 넘어 위헌, 위법한 것이다.

이상과 같이 패킷감청은 그 대상자의 불특정성, 대상 통신내용의 포괄성 때문에 통신 감청이 최소한보충적으로 이루어져야 한다는 통신비밀보호법의 제정취지에 비추어 통비법이 허용하는 감청의 범위를 벗어난 위헌, 위법한 감청이므로, 향후 통비법을 개정하여 패킷감청의 절대적 금지를 명문화하고 이에 대한 위반행위를 처벌하는 규정을 신설하여야 한다는 발제자의 결론에 전적으로 동감한다.

4. 통비법 일부개정안의 문제점

가. 이정현 의원의 통신비밀보호법 개정안(2009. 12. 11.)은 패킷감청의 허가서 내용 구체화, 통신제한조치 기간 및 연장횟수 제한, 통신제한조치로 알게 된 내용의 열람 또는 복사 및 통신제한조치 허가범위 외의 내용이나 불필요한 내용의 폐기의무 등을 담고 있는데, 그 중 감청허가서 내용의 구체화로서 인터넷 회선에 대한 감청허가서에는 전자우편의 내용, 접속한 인터넷홈페이지의 주소, 홈페이지의 게시판 또는 대화방 등에서 게시한 의견, 검색한 정보목록 등 대통령령으로 정하는 바에 따라 그 대상과 범위 등을 구체적으로 특정하여 기재하도록 하고 있다.

나. 그러나 개정안은 패킷감청의 요건을 엄격하게 한다는 명분을 내세우고 있지만 현행법에 의하여 금지되는 패킷감청을 허용하고 이를 더욱 용이하게 하는 부작용이 훨씬 크다. 기술적으로 패킷 상태로 전송되는 데이터 가운데 전자우편 내용 또는 게시판에 올린 의견 등만 따로 걸러 가로채는 기술은 아직 개발되지 않았다는 것이 전문가들의 설명이기 때문이다. 따라서 패킷감청을 엄격히 제한한다는 명분하에 오히려 패킷감청에 대하여 법적으로 면죄부만 마련해 줄 가능성이 큰 개정안에 반대한다.¹⁾ 지금 필요한 것은 패킷감청의 법적 근거를 마련하는 것이 아니라 패킷감청의 가능성을 법적으로 차단하는 것이다. 이를 위하여 현행 통비법의 통신제한조치에 대한 허가절차를 세밀하게 규정할 필요가 있다.

1) “통신비밀보호법 일부개정법률안(의안번호 제6976호)”에 관한 민변 의견서(2010. 1. 22.)

..... 패킷감청의 문제점과 개선방안에 대한 토론회

04

온라인 맞춤형 광고 가이드라인 제정 추진 현황

이 강 신
(한국인터넷진흥회 단장)

온라인 맞춤형 광고 가이드라인 제정 추진 현황

2010. 2. 1

이강신 인터넷기반·개인정보보호단 단장



발 표 순 서

I. 가이드라인 제정 추진 배경

II. 가이드라인 추진 경과

III. 온라인 맞춤형 광고 주요 이슈

IV. 향 후 일 정

1/6

I. 가이드라인 제정 추진 배경

가이드라인의 필요성

- 온라인 이용 행태(방문사이트, 방문 시 행동 등)를 분석하여 이용자 관심에 맞추어진 광고를 제공하는 차세대 광고 기술 등장
- 이용자 입장에서는 온라인상에서의 개인 행태 및 성향에 대한 파악으로 개인 프라이버시 침해 우려
- 온라인 맞춤형 광고 이용자의 자기정보통제권을 보장할 수 있는 가이드라인 제정 필요

가이드라인 성격

- 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 등 관계 법령의 개인정보 보호 원칙을 토대로
- 온라인 맞춤형광고 제공자가 맞춤형 광고 제공 시 이용자의 프라이버시를 자율적으로 보호할 수 있도록 개발

2/6

II. 가이드라인 제정 추진 경과

추진 경과

- '09. 10. 15 : Kick off 미팅
 - '09. 10. 19 : 제 1차 회의 (국외 온라인 맞춤형 광고 서비스 검토)
 - '09. 10. 29 : 제 2차 회의 (국내 온라인 맞춤형 광고 서비스 검토)
 - '09. 12. 29 : 제 3차 회의 (온라인 맞춤형 광고의 사회·심리적 영향 및 정보통신망 법상 개인정보 정의에 대한 법률 검토)
 - '10. 1. 14 : 제 4차 회의 (온라인 맞춤형 광고 유형 분류 검토 등)
- ※ 연구반 구성 : 업계(한국인터넷기업협회, 포털 등), 학계(소비자, 사회학, 심리학, 정보보호, 경영정보), 법조계, 시민단체(한국소비자 연맹, 소비자시민의 모임, 바른사회 시민회의), 기타(한국인터넷광고심의 기구) 등 총 19명으로 구성

3/6

III. 온라인 맞춤형 광고 주요 이슈[1/2]

분류 기준

- 맞춤형 광고를 위해 활용되는 정보 및 활용 횟수에 따른 이용자 프라이버시 침해 위험도를 기준으로 분류

기 준	유 형 분 류	동 의 방 식
프라이버시 침해 위험도	① 개인을 식별 또는 식별 가능성이 있는 경우	Opt-in
	② 개인 식별 가능성은 없으나 행태정보가 축적·분석·저장되는 경우	Opt-out
	③ 행태정보가 1회적으로 활용되는 경우	적용 없음

4/6

III. 온라인 맞춤형 광고 주요 이슈[2/2]

주요 이슈

- “특정한 개인을 알아볼 수 있는”의 범위
- “다른 정보와 쉽게 결합하여 알아볼 수 있는”의 범위

〈정통방법상 개인정보의 정의〉

[제2조제1항제6호] 생존하는 개인에 관한 정보로서 성명·주민등록번호 등에 의하여 **특정한 개인을 알아볼 수 있는** 부호·문자·음성·음향 및 영상 등의 정보(해당 정보만으로는 특정 개인을 알아볼 수 없어도 **다른 정보와 쉽게 결합하여 알아볼 수 있는** 경우에는 그 정보 포함)

- 유형분류 별 동의 방식

5/6

IV. 향후 일정

향후 일정

- 7월까지 약 7~8회의 연구반 회의 개최 및 8월말 공청회를 통한 최종 의견 수렴 후, 9월말 가이드라인 마련 예정



6/6

감사합니다

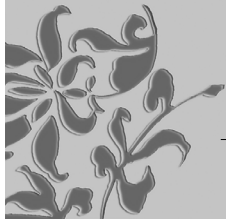
한국인터넷진흥원
Korea Internet & Security Agency

.....패킷감청의 문제점과 개선방안에 대한 토론회

05

‘패킷감청의 헌법적 문제점’에 대한 토론문

오길영
(민주주의 법학 연구회 박사)



‘패킷감청의 헌법적 문제점’에 대한 토론문

▶ 오길영(민주주의 법학 연구회 박사)

오동석 교수님의 옥고, 잘 읽었습니다. 헌법적 시각에서 패킷감청에 대한 주요쟁점을 면밀하게 검토해 주셨습니다. 저는 오교수님의 발제에 공감하면서, 보충하는 의미에서 몇 가지 말씀을 덧붙이고자 합니다.

1. 패킷감청은 위헌이다.

오교수님은 발제에서 3가지 측면으로 패킷감청의 위헌성에 대하여 말씀하여 주셨습니다. 특히 패킷감청은 행정작용과 사법작용의 본질적 한계를 넘어선 것으로서 이는 단순의 법률의 제정 또는 개정으로 해결될 수 없는 사안이라는 지적에 대하여 전적으로 공감하는 바입니다.

저는 현행 통신비밀보호법이 아날로그 시대의 기술을 상정한 법체계로써 새로운 디지털 기술특성을 제대로 반영할 수 없는 본연적 한계를 가지고 있다는 점을 몇 편의 글을 통해 지적해 왔습니다.

즉 현행 통신비밀보호법은 아날로그 기술과 디지털 기술의 차이를 제대로 극복하지 못하고 있어, 아날로그 감청에 있어서의 합리적 요리법을 디지털 재료에서는 제대로 구현해내고 있지 못하다는 것입니다. 따라서 기본권 침해의 위험에 노출되어 있으며 이의 보완을 위한 새로운 레시피를 마련해야 한다는 것이 그것입니다.

그러나 DPI의 경우 그 제한법규의 모호성과 감청대상의 포괄성으로 인해 현행 통신비밀보호법의 규제대상이 될 수 없음을 최근의 줄고에서 밝힌 바 있습니다. 즉 DPI의 경우 레시피를 마련하는 차원이 아니라 요리가 불가능한 재료이라는 것입니다. DPI는 마치 독극물과 같아서 이러한 재료를 가지고 요리를 하고자 하는 것 자체가 현재의 기술로서는 불가능함은 물론 고도의 위험성을 가지고 있다는 것입니다.

물론 독이 있는 재료를 굳이 요리할 경우도 있습니다. 복어요리의 경우 ‘테트로도톡신(Tetrodotoxin)’이라는 맹독성이 있으나, 오늘날 훌륭한 요리재료로써 각광을 받고 있습니다.

그러나 우리는, 복어의 간과 알 그리고 혈액 속에 존재하는 독성을 제거할 수 있는 명확한 기술이 존재한 이후에나 복어요리가 허가되었다는 역사를 잊지 말아야 합니다.

다시 말해 DPI의 독성을 제거하는 기술이 없는 현재에 있어서는, 패킷감청은 엄연한 위험적 대상일 뿐입니다.

2. 개정안은 폐기되어야 한다.

지난 12월 11일, 이정현의원이 대표발의한 바 있는 통신비밀보호법 개정안에 ‘DPI-레시피’가 새로이 등장하였다고 하여 살펴보았습니다. 동 개정안은 “인터넷 회선에 대한 감청의 허가서에는 전자우편의 내용, 접속한 인터넷홈페이지의 주소, 인터넷홈페이지의 게시판 또는 대화방 등에서 게시한 의견, 검색한 정보목록 등 대통령령으로 정하는 바에 따라 그 대상과 범위 등을 구체적으로 특정하여 기재하도록” 한다는 규정을 신설하고 있습니다.

이는 마치 ‘DPI의 주요 독성을 제거하고 요리하도록 하라’는 것과 같은 ‘원칙적 제안’에 불과한 입법입니다. 그러나 구체적으로 ‘어떠한 방법으로 그러한 독성을 제거하는 지’에 대하여는 대통령령으로 정한다는 ‘모르쇠’ 입법태도를 보이고 있습니다.

그렇다면, 왜?!.. 동 개정안은 구체적인 방법을 제안하지 않고 ‘모르쇠’ 방식을 채택하고 있는 것일까요? 말그대로, 그 독성을 제거하는 방법을 모르기 때문입니다. 좀 더 정확히 말하자면, 아직 그 누구도 제대로 된 DPI-독성제거법을 찾아내지 못했기 때문입니다.

따라서 동개정안은, 일단 ‘DPI의 주요 독성을 제거하고 요리하도록 하라’는 원칙적인 입장을 제안하면서 그 구체적인 독성제거법에 대하여는 대통령령으로 정하도록 하였으니, ‘입법부가 모르는 독성제거법에 대하여는 행정부가 알아서 찾아내라’고 위임해 버린 것과 마찬가지로입니다.

입법부가 모르는 독성제거법을 행정부라고 하여 도대체 무슨 수로 찾아낸다는 것입니까? 또한, 앞서 밝힌 바와 같이 현실적으로 그러한 독성 제거방법은 기술적으로 존재하지조차 않습니다.

나아가 오교수님께서 발제문에서 밝히신 바와 같이, 법률의 차원에서 기본권제한의 본질적 사항에 대하여 함구하면서 그 구체적 사항을 하위입법에 위임하는 동 개정안의 입법태도는 위임입법의 한계를 넘은 의회유보원칙 위반으로써 위헌법률의 대표적 유형에 속하기도 합니다.

따라서 동 개정안의 해당내용은 폐기되어야 합니다.

3. 패킷감청의 상업화는 금지되어야 한다.

DPI 기술의 위험성은 비단 감청의 영역으로만 제한되는 것은 아닙니다. 이번 정권에서 도입하여 사회적 문제가 되고 있는 서른 대가 넘는 패킷감청 장비도 문제이지만, 최근 국내 IT 기업에서 그 도입을 의욕하고 있는 ‘맞춤형 광고시스템’의 경우가 실제로 야기할 사회적 파장에 있어서는 오히려 더 큰 부작용을 가져올 것으로 예상됩니다.

맞춤형 광고시스템을 감청에 비추어 이야기하자면, 감청회선 제공자와 감청수단의 개발자가 결탁하여 감청기반형-광고기술을 개발하고, 이를 상업화하여 이익창출의 새로운 수단으로써 활용하고자 하는 사안이기 때문입니다.

오늘날 상업화의 무대에 있어서는 오로지 ‘이익’만이 고려될 뿐, 그 어떤 가치도 제대로 보호받을 수 없다는 사실은 이미 주지의 사실입니다. 또한 예상되는 부작용의 내용과 정도에 있어서도, 지금까지 경험해온 IT환경하에서의 개인정보 유출과 이로 인해 회복할 수 없는 피해의 기억들과는 그 차원을 달리합니다.

이미 말씀드린 바와 같이, DPI 기술의 본질적 위험성은 그의 활용처가 감청이라는 소화불량한 수단으로 활용된다는 점만이 아닙니다. DPI 자체가 맹독성 재료이라는 것이 핵심입니다.

마치 환각의 소재로 사용되는 마약류가 다이어트약품의 명목으로 판매된다고 하여 정당화될 수 없듯이, DPI의 독성을 제거하지 못한 채로 이를 단지 상업화로 재포장한다고 하여 그 본질적 위험성이 사라질 수는 없습니다. 오히려 상업화의 대상으로 변모하는 순간, 그 어떤 수단으로도 통제할 수 없는 난공불락의 기본권 침해수단으로서 기능하게 될 것입니다.

따라서 패킷감청의 상업화는 전면적으로 금지되어야 합니다.

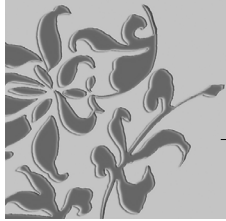
- 경청해 주셔서, 대단히 감사합니다.

.....패킷감청의 문제점과 개선방안에 대한 토론회

06

패킷 감청과 통신의 비밀

장 여 경
(진보네트워크센터 활동가)



1. 기술 발달과 통신의 비밀

1993년 통신비밀보호법이 처음 제정되었을 때 이 법이 보호하는 ‘통신’으로 주로 간주되었던 것은 우편물과 유선전화였다. 그러나 기술이 발달하면서 통신매체의 종류와 가지수가 계속 늘어났고 그에 대한 규제 입법의 속도는 뒤쳐진 듯이 보였다. 정보·수사기관들은 이 ‘지연’을 자의적이고 편의적으로 활용해 왔다.

예컨대 음성사서함, 문자메시지, 이메일 등 모든 통신매체에 부대하는 저장매체가 오늘날처럼 발달하기 전에 입법화한 통신비밀보호법은 ‘송수신이 완료되어 저장된 통신내용’에 대해서 그 보호 대상으로 삼기 애매한 부분이 있었다. 이에 대한 정보·수사기관들의 반응은 일반 물건의 압수수색 절차를 따라 무려 7년치의 통신 내용을 지득 및 채록하면서도, 그 압수수색에 있어 형사소송법에서 일반적으로 보장하고 있는 당사자의 참여권이나 통보의 권리를 무시해 왔다. 무선호출기가 등장했을 때는 사업자로부터 비밀번호를 통째로 제공받기도 하였다. 또한 ‘통신사실 확인자료’에 대한 규정이 신설되었던 2001년 통신비밀보호법 개정 당시 이는 명백히 ‘자료제공요청서 접수시점 이전의 자료에 한정’되는 의미였지만, 휴대전화 이용자가 증가하자 ‘장래의 위치추적’을 슬쩍 통신사실 확인자료에 포함시켜 손쉽게 제공받기 시작했다.

기술은 계속 빠른 속도로 발달할 것이고 법은 끊임없이 이를 뒤쫓아가는 입장일 것이다. 기술 발달과 보호 규범의 지연 현상이 발생할 때 우리는 어떠한 선택을 해야 할까?

답은 명백하다. 오동석 발제자의 지적처럼 헌법적 원칙에 충실해야 하는 것이다. 권리주체의 기본적 권리에 미치는 영향에 대하여 엄격하게 평가하고, 이를 위축시킬 가능성이 있는 자의적인 해석이나 불법을 행해서는 안 된다. 우리 헌법 제18조와 통신비밀보호법의 취지는 통신의 비밀과 자유에 대한 제한은 최후적 수단이자 최소한으로 이루어져야 한다는 것이다. 더구나 오늘날처럼 일상생활의 영위에 있어 통신의 비중이 높아진 상황에서 통신의 비밀에 대한 보호 수준은 표현의 자유와 정치적 자유는 물론 다른 모든 기본권에 연쇄적으로 영향을 끼친다.

2. 정보기관의 감청

우리 현실은 비관적이다. 감청에 있어서 범죄 수사와 직접 관련이 없는 정보기관의 비중이 압도적이다. 정보기관의 감청은 정치적인 반대자들을 감시하고 억압하는 목적으로 사용될 수 있다는 점에서 매우 심각한 문제이다. 실제로 국가정보원은 그 전신인 국가안전기획부 당시 부터 직접 개발한 휴대전화 감청장비를 동원하여 방대한 규모로 정치적이고 불법적인 감청을 해왔음이 2005년 드러나 사회적으로 큰 충격을 주었다.

<표 1> 기관별 통신 감청 건수

(단위 : 전화번호 혹은 아이디 건수)

	검찰	경찰	국정원	군수사기관	합계
2000	386	1,320	1,575	261	3,542
2001	362	1,289	2,412	308	4,371
2002	208	627	2,234	187	3,256
2003	165	648	5,424	203	6,440
2004	106	554	8,201	289	9,150
2005	100	241	8,082	112	8,535
2006	43	131	8,440	51	8,665
2007	41	95	8,628	39	8,803
2008	24	94	8,867	19	9,004

자료: (구)정보통신부와 방송통신위원회의 반기별 발표자료를 취합함.

지난 국정감사 때는 31대의 패킷 감청 장비를 직접 보유하고 사용해 왔음이 알려지기도 하였다. 더욱 큰 문제는 이렇게 최첨단 감청 장비를 다수 보유하고 있는 정보기관의 감청에 영장주의의 예외가 인정된다는 사실이다. 외국인을 감청할 때는 법원의 허가가 아닌 대통령 승인만으로 가능하고 긴급한 감청 때는 국가정보원장의 승인만으로 감청할 수 있다. 그러나 외국인을 언제 어떻게 얼마나 감청하고 있는지 그것이 정말 외국인에 대한 감청인지 여부는 정보기관만이 알고 있다. 통계조차 비밀이다. 현재 ‘사업자를 통한 간접 감청 제도의 도입’이라는 명분으로 추진되고 있는 이한성 의원의 개정안에서는 같은 사유 하에서만 ‘직접’ 감청 장비를 운용할 수 있도록 하여 정보기관의 비밀 감청 권한을 확대하였다. 이러한 규정들은 정보기관이 영장주의를 우회할 수 있는 길을 제공함으로써 통신비밀보호법의 입법 취지를 완전히 무너뜨릴 수 있다.

여기서 법원의 통제는 미미하다. 심지어 법원은 허가서 한 장으로 우편물 검열과, 유선전

화·휴대전화·인터넷 메일에 대한 감청은 물론 인터넷 회선 전체와 대화에 대한 감청까지 한번에 모두 실시하는 저인망식 감청을 허용해 왔다(<그림 1>).

우리는 이러한 총체적 문제들이 집약된 최악의 사례로써 패킷 감청을 접하게 되었다.

- 가. 대상자 명의로 사용 중인 휴대폰()의 음성사서함 감청·문자메시지 열람, 위치·착발신지 추적 및 국내·국제 통신사실 확인자료
- 나. 대상자가 근무처인 연구소(서울특별시 성북구)에 자신의 명의로 설치, 사용 중인 초고속인터넷회선에 대한 전기통신내용의 지목·채록 및 실시간 착·발신 IP추적
- 다. 대상자 주거지(서울특별시 성북구)에 妻 (31세) 명의로 설치한 초고속 인터넷회선(ID:)에 대한 전기통신 내용의 지목·채록 및 실시간 착·발신 IP추적
- 라. 대상자 명의 이메일 계정(@ , @ , 등 2개)에 대한 전기통신내용의 지목·채록 및 착·발신 내역
- 마. 대상자 주거지(서울 성북구) 및 사무실(연구소, 서울 성북구)에 대상자 명의로 착·발신된 우편물 검열·복사·인도
- 바. 대상자와 대화를 나누는 상대방 사이의 법 위반 피의사실을 내용으로 하는 대화 녹음·청취

<그림 1> 감청 허가서 (일부 예시)

3. 패킷 감청

인터넷 회선을 오가는 신호 전체에 대한 패킷 감청은 그 사생활 침해 정도가 매우 심각하다(<그림 1>의 ‘나’항과 ‘다’항). 인터넷 초창기에는 컴퓨터 속도와 자원의 한계 때문에 규모가 큰 패킷 감청은 효과적으로 이루어질 수 없었다. 최근의 기술적 진보로 인하여 ISP와 정보수사기관들이 큰 규모로 패킷 감청을 하는 것이 가능해졌다.

한국에서는 남북공동선언실천연대 사건에 대한 재판과정에서 국가정보원이 패킷 감청을 실시한 사실이 드러났고, 지난 8월 31일 인권단체들이 이를 비판하는 기자회견을 개최함으로써

패킷 감청 문제가 처음 알려졌다. 그러나 실제로 정보기관이 언제부터 얼마나 큰 규모로 패킷 감청을 실시해 왔는지는 아직까지 전혀 알려지지 않고 있다.

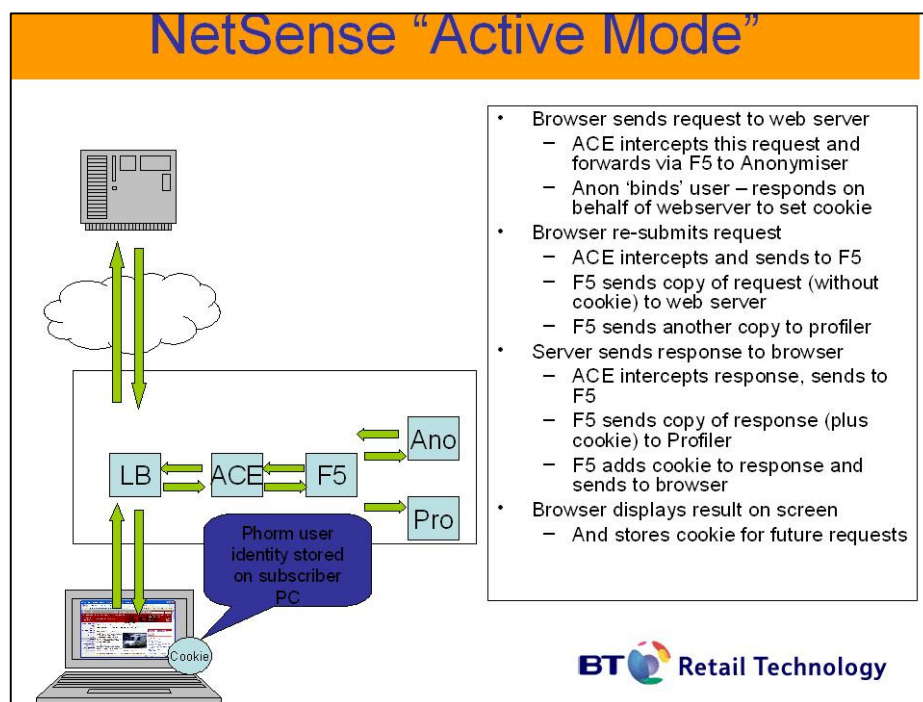
패킷 감청의 가장 큰 문제점은 감청 대상을 특정할 수 없다는 점이다. 첫째, 보통의 가정이나 직장에서는 공유기 등을 통해 다수의 PC와 다수인이 해당 네트워크 서비스를 공동이용한다. 대상자의 PC를 임시적으로 다른 이가 사용할 수도 있다. 따라서 현재의 패킷 감청은 감청 대상자가 아닌 타인의 인터넷 통신 내용을 감청하게 되는 경우가 다수 있을 것이다. 그러나 외부에서 감청을 집행하는 입장에서는 지금 전송되는 패킷이 감청 대상자의 행위에 의해 송수신되는 것인지 알 수 없다. 따라서 패킷 감청은 각 대상자별로 감청이 이루어지도록 한 현행 「통신비밀보호법」에 위배되고(동법 제6조 제1항), 문제의 패킷을 대상자가 송수신하였다는 점이 별도로 입증되지 않는 한 법정 증거로서의 효력도 없다. 결국 패킷 감청은 정보기관의 은밀한 정보수집욕구만을 충족시켜 줄 뿐이다.

둘째, 패킷 감청의 경우 특정 이메일이나 메신저에 대한 감청과 달리 서버로부터 대상자에게 전달되는 모든 통신내용을 대상으로 한다. 이 가운데에는 공개된 통신내용도 있을 수 있지만 비공개 통신내용도 있을 수 있는데, 비공개 통신내용은 단지 대상자가 이용하였다는 이유만으로 정보수사기관에게 제공된다. 이 과정에서 이용자의 비밀번호 등이 제공될 가능성도 있는데, 이는 감청을 집행하는 과정에서 비밀번호가 누설되어서는 안된다는 「통신비밀보호법」의 취지에 위배된다(동법 제9조 제4호).

결국 패킷 감청은 그 범위가 너무 광범위하여 대상자와 대상 통신내용을 특정할 수 없다는 점에서 우리 「통신비밀보호법」이 허용하는 감청의 범위를 벗어난 위법한 감청이다. 더구나 패킷이란 목적을 가지고 이동하는 통신 과정상의 자료로서 수사에 필요한 자료는 해당 패킷이 목적지에 도달한 후 기존의 이메일 전달(forwarding) 방식의 감청이나 압수·수색으로도 충분히 입수가능하다. 여러모로 통신비밀보호법에 규정된 감청 방식으로 부적합한 패킷 감청이 굳이 인정될 필요가 없는 것이다.

결론적으로 오동석 발제자의 지적대로 인터넷 회선 감청은 ‘헌법적 불법’으로서 중단되어야 한다. 더 나아가 차제에 법을 정비하여 감청이 허가된 대상 피의자가 발송·수취하거나 송·수신하는 것임이 분명하지 않은 통신에 대해서는 감청하지 못하도록 명확히 적시할 필요가 있다.

4. 패킷 감청의 상업화¹⁾



<그림 2> KT와 같은 기술을 채택한 영국 BT사의 경우

패킷 감청에 대한 또다른 논란은 그 상업적 이용이다.

KT에서 도입하려는 DPI 메카니즘에 따르면 KT 이용자의 모든 인터넷 통신내용은 품사의 패킷 감청 장비를 거친다. (KT는 '동의'한 '일부' 이용자에 한하여 '서비스'한다고 하지만 '동의 이용자 확인'이 정확히 어떤 단계에서 이루어지는지 명확해질 필요가 있다. 동의한 '일부' 이용자의 패킷 만이 품사의 장비에서 처리된다고 간주하더라도) 문제는 이용자의 관심사가 DPI를 통해 분석된다는 것이고, 그 분석 결과로써 그룹화된 관심사에 맞춘 광고가 웹사이트 특정 위치에 뜨는 것이다.

품사는 '맞춤' 서비스를 신청하지 않은 어떤 사용자들의 정보는 '그냥 흘러가고', https 등 보안 프로토콜을 이용하는 통신내용들도 '그냥 흘러간다'고 주장한다. 더불어 흘러가는 통신내용들 가운데 '주민등록번호'나 '전화번호'로 인식될 수 있는 '일련 숫자'들은 '버린다'고 주장한다. (여기서도 '흘러가는 것'이 어떤 수준인지 확인될 필요가 있다.) 어찌되었건 https 등으로 암호화되어 있지 않은 KT의 (모든 혹은 일부) 이용자의 통신 내용이 '일단' 품사의 장비를 거친다는 점은 확실하다. 그렇지 않으면 어떻게 그것이 숫자라는 것을 알겠는가?

1) 보다 정확한 기술적 표현은 DPI(Deep Packet Inspection)이겠지만 맥락상 앞서 정보수사기관의 패킷 감청과 함께 '패킷 감청'으로 표현한다.

그렇다면 폼사는 이용자가 방문하는 모든 페이지의 URL만을 읽을 뿐 아니라, 모든 웹페이지의 내용을 보는 것이다. 이용자의 이메일 이용, 비공개된 게시물이나 대화 등의 통신내용도 암호화되어 있지 않은 한 폼사의 장비가 읽는다. 폼사의 장비로써는 이것이 이메일인지 비공개된 카페 게시물인지 알 도리가 없으니 무조건 읽는다. 이것은 분명 통신비밀보호법에서 보호하고 있는 통신 내용이고, 폼사의 장비는 제3자이며, 여기서 일어나는 DPI 행위는 제3자 감청인데, 우리 통신비밀보호법에서는 양당사자의 동의나 영장이 없는 제3자의 감청은 허용하지 않는다.

KT와 폼사는 ‘자발적으로 동의한’ 이용자를 대상으로 한다고 주장한다. 그러나 우리 대법원에 따르면 이 때 동의는 통신 송신자와 수신자 모두로부터 받아야 한다. 제3자가 전화통화자 중 일방만의 동의를 얻어 통화내용을 녹음한 경우, 통신비밀보호법에 위반한다고 본 것이다 (대법원 2002. 10. 8. 선고 2002도123 판결). 그러나 KT가 DPI 과정에서 읽어내는 이메일 모든 당사자들로부터 적법한 동의를 획득하는 것이 과연 가능한 일인가?

무엇보다 기술 환경이 허용한다고 하여 사생활의 가장 은밀한 내용까지 무차별적으로 파헤쳐 영업 대상으로 삼는 비즈니스 모델은 허용되지 않는 것이 바람직하다. 지금은 이메일 뿐인지 모르겠으나 앞으로는 그 어떤 것이라도 될 수 있다. 물론 임종인 발제자가 지적하였듯이 적법한 권한 없는 불법도청에 이용될 수 있다는 우려도 빼놓을 수 없다.

.....패킷감청의 문제점과 개선방안에 대한 토론회

07

온라인 맞춤형광고(OBA)에 대한 입장

구 태 언
(김앤장 법률사무소 변호사)

온라인 맞춤형광고(OBA)에 대한 입장

2010.2.1

변호사 구태언

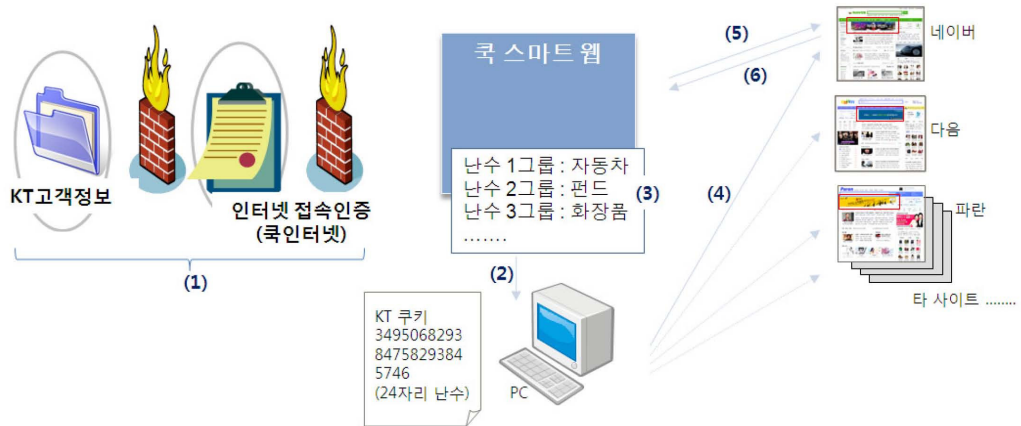
I. 서비스의 개요

본건 온라인 맞춤형 광고는 인터넷서비스제공자(Internet Service Provider, "ISP")의 네트워크 상에서 수집된 특정 키워드 데이터를 처리하여 인터넷 이용자의 관심사에 부합하는 온라인 맞춤형 광고를 제공하는 비즈니스 모델임

본건 모델을 통해 기존에 무차별적으로 보여지던 광고 및 콘텐츠 대신 기호에 맞는 맞춤형 광고 및 콘텐츠를 제공함으로써, 광고 및 콘텐츠의 정보로서의 가치가 상승하게 되고, 이용자에게도 이익이 되는 방식으로 광고의 가치를 제고함으로써 사회 전반적인 효용 상승 효과 및 비용 절감 효과가 있음

시스템 상 개인식별정보의 제거, 타 정보와의 결합가능성 제거, 수집정보의 최소화, 암호화, 익명성 보장 등 기술적·관리적 조치를 통하여 이용자의 Privacy를 최대한 보호할 수 있도록 구현

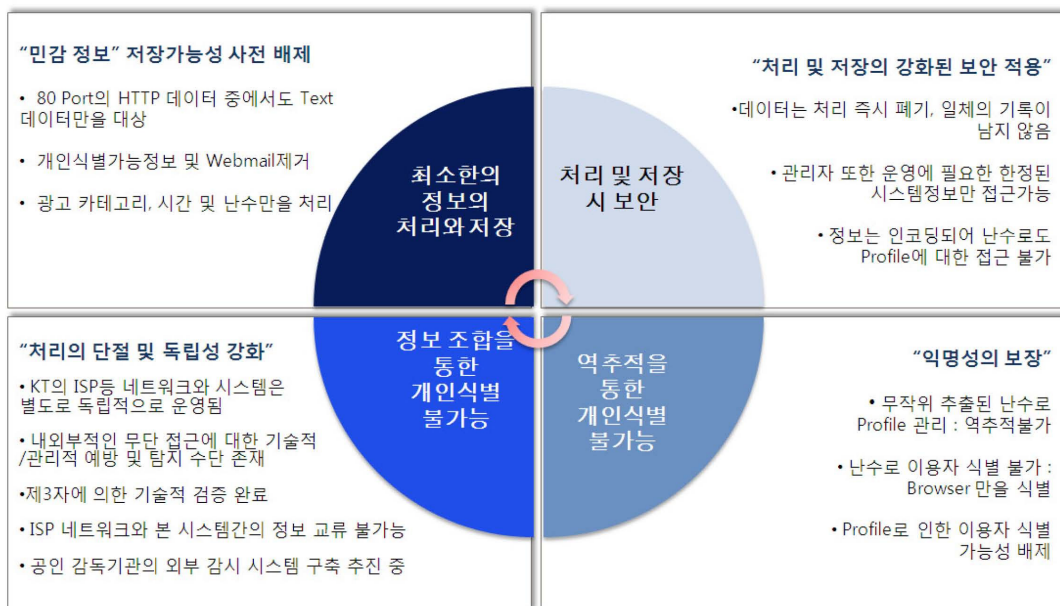
II. 시스템 구성 및 정보처리 과정



- 1) 쿱스마트웹을 고객정보와 원천차단
- 2) 24자리 난수를 쿱에 담아 동의한 고객 PC 로 보냄 > 쿱스마트웹 상에는 난수 번호로만 식별 : **개인식별불가**
- 3) 네트워크 단에서 사전에 정의된 관심표에 따라 난수를 그룹 분류 > 난수/관심그룹/분류된 시간)으로 보관 : **개인식별불가**
- 4) PC(난수)가 제휴된 사이트에 방문
- 5) 제휴된 사이트를 통해 쿱스마트웹에 난수 전달 : **3자 정보제공 없음**
- 6) 쿱스마트웹은 난수가 어떤 관심표 그룹에 속하는지 확인 후, 관련 콘텐츠 혹은 광고를 사이트 지정된 위치에 전송

3

III. 서비스의 특징



4

IV. 감청 해당 여부

1. 지득 또는 채록 여부

감청은 통신의 내용의 지득 또는 채록이 요건임. 본건 서비스는 통신의 내용을 지득 또는 채록하지 아니하고 이를 의도하고 있지도 아니함

지득 여부

- 지득: 깨달아 얻음 내지 알게 됨
- 통신내용은 전혀 저장됨 없이 최종적으로 (1) 광고 카테고리, (2) 매칭시간, (3) 난수만 남게 되므로 통신의 내용을 알 수 없음

채록 여부

- 채록: 채집하여 기록함
- 이용자의 통신내용은 전혀 기록 내지 저장되지 아니함

고의 부재

- 지득 내지 채록을 의도하지 아니함
- 시스템적으로 통신내용은 제거되도록 구현

5

IV. 감청 해당 여부

2. 당사자 특정성

감청의 대상은 특정 당사자간의 통신. 본건 서비스에 있어서는 당사자가 특정되지 아니하여 Privacy 보호됨

비밀성에 대한 보호

- 통신의 자유: 통신의 비밀에 대한 보호
- 개인이 특정되지 아니하면 "비밀성" 보장됨
→ 통신의 자유 보호됨

개인식별성 배제

- 개인식별정보 제거
- (1) 광고 카테고리, (2) 매칭시간, (3) 난수만 저장
- 익명화 / 역추적 불가
- 네트워크의 물리적 차단 · 독립운영 / 기술적 · 관리적 보호조치를 통한 타 정보와의 교류가능성 · 결합가능성 배제
- 이를 통하여 당사자 특정가능성 배제

6

IV. 감청 해당 여부

3. 동의

형식에 구매되지 아니하고 실질적인 동의 여부에 따라 판단되어야 함. Privacy에 대한 실질적인 통제권을 행사하였는지 여부에 따라 판단

통비법상 동의

- 동의 방식 규정되지 아니함
- 묵시적인 동의도 가능

동의 여부 판단 기준

- 통비법의 목적은 Privacy 보호
- Privacy에 대한 통제권 여부에 따라 판단
- 이용자의 상황에 대한 인식 + 통제권 행사가능성

이용자의 동의 획득

- 서비스의 내용 및 탈퇴방식을 명시적으로 고지
- 이를 통한 이용자의 상황에 대한 인식 + 통제권 행사가능성 확보

7

V. 결론

본건 서비스와 방식이 유사한 인터넷 쿠키 및 온라인 맞춤형 광고 서비스는 다수의 포털, 전자상거래 웹사이트 등에서 이미 일반화·상용화 되어 있음

본건 서비스는 감청이나 사생활(Privacy) 침해 우려를 원천적으로 배제하도록 설계되었으며, 오히려 사생활 보호에 부합하면서도, 인터넷 이용자들의 관심과 선호를 반영하여 이용자에게 맞춤형 광고 제공이 가능함.

본건 서비스에 있어서는 통신의 내용에 대한 지득 또는 채록이 일어나지 아니하고, 이를 의도하고 있지도 아니하며, 당사자가 특정되지 아니하여 통신의 비밀성이 보장되고, 이용자의 동의권이 확보되어 있으므로 감청에 해당하지 아니함

8