【논문】

감청의 상업화와 그 위법성*

오길영
서강대 강사, 전자상거래법
eclaw@daum.net

<국문초록>

이 글은 현재 KT가 그 도입을 추진하고 있는 것으로 판단되는 DPI형 인터넷 맞춤광고의 위법성을 논증하기 위하여 작성되었다.

먼저 개인정보보호를 위한 두터운 안전장치를 마련하고 감청이나 사생활 침해의 우려를 원칙적으로 배제하도록 설계하였다는 KT의 주장에 대하여, DPI행위의 구조적인 분석과 쿠키의 유인·변조행위 등 구체적인 기술요소에 대한 검토를 통하여 DPI형 맞춤광고의 기술적 함정과 허위성을 밝힌다. 또한 1·2세대 인터넷 맞춤광고와의 기술적·구조적 차별성에 대한 검토를 통하여 "이미 상용화되어 있는 인터넷 맞춤형 광고서비스의 일환일 뿐"이라는 KT측 주장의 허구성을 입증한다.

다음으로 DPI형 맞춤광고에 대한 법리적 검토 부분에서는 DPI형 맞춤광고로 인해 야기되는 위법적 요소들에 관하여, 기술적 분석의 기반위에서 개별적·구체적인 검토를 진행하였다.

KT의 주장과는 달리 DPI형 맞춤광고 기술은 인터넷 사용자에 대한 특정가능성이 엄연히 존재한다는 점, DPI행위 자체가 통신비밀보호법상의 감청에 해당하여 통신비밀보호법 위반이라는 점, 쿠키의 변조행위 또한 통신비밀보호법상의 감청에 해당한다는 점, 나아가 저작권법 위반임은 물론 정보통신망법 위반에 해당하여 결국 DPI형 맞춤광고 기술이 우리 현행법상 명백한 위법행위임을 논증하는 것이 이 글의 결론이다.

주제어: 인터넷 맞춤광고, DPI형 맞춤광고, 패킷감청, 쿡 스마트웹, Phorm

---

* 심사위원: 김종서, 오동석, 윤영철
투고일 2010. 5. 31. 심사개시: 2010. 5. 31. 게재확정: 2010. 6. 8.

< 차 례 >

Ⅰ. 시작하며

지난 2월 1일, '패킷감청[1]의 문제점'에 대한 토론회[2]가 국회의원회관 소회의실에서 열렸다. 국회방송을 통해 생방송된 본 토론회에 필자는 토론자로 참여하게 되었는데, 열심히 통역을 받으며 토론을 경청하고 있던 한 외국인을 토론회가 진행되는 내내 응시하고 있었다. 한 나라의 국회에서 열리는 토론회에 외국인이 참여하는 것도 이례적인 일이지만, 단순한 구경정도가 아니라 열심히 통역을 받으며 토론회의 시작부터 끝까지 진지한 표정으로 자리를 지키고 있는 사람이라면, 그는 분명 패킷감청과 밀접한 관련이 있는 사람일 것이기 때문이었다. 후에 확인한 바에 의하면, 그는 역시나 그 토론회가 무척이나 중요한 사람이었다. 그는 패킷감청[3]

---

1) 패킷감청과 DPI(Deep Packet Inspection, 이하 DPI), 그리고 DPI형 인터넷 맞춤형 광고에 대한 전반적인 이해와 그 문제점에 대해서는 미흡하나마 필자의 지난 논문을 참고하면 좋을 것이다. 오길영, "인터넷 감청과 DPI(Deep Packet Inspection)", 민주법학 제41호(2009).

2) 민주당 우윤근, 박영선, 변재일 의원이 주최하여 <패킷감청의 문제점과 개선방안에 대한 토론회>라는 제목으로 2시간 남짓 진행된 토론회는 패킷감청 시연을 필두로 국정원이 실시하여 논란이 된 바 있는 패킷감청의 위헌성과 패킷감청 기술을 활용한 인터넷 맞춤광고의 문제점 등을 주요한 내용으로 진행되었다. 2명의 발제자와 5명의 토론자, 그리고 1명의 사회자로 진행된 본 토론회의 영상은 <http://www.assembly.go.kr/renew09/brd/formation/last_pro_vw_detail.jsp?programId=86&infoId=7304&index=769&gotopage=1>, 검색일: 2010.4.1.에서 다시 볼 수 있다.

3) 본고에서 검토하는 DPI형 인터넷 맞춤광고에서의 DPI 기술에 대한 적절한 표현

기술을 인터넷 광고수단으로 개발한 영국 Phorm사의 최고정보책임자(CPO, Chief Privacy Officer)였고, Phorm사는 바로 우리나라의 KT에게 '쿡 스마트웹(Qook Smartweb)'이라는 DPI형 인터넷 맞춤광고의 원천기술을 제공한 장본인이기 때문이다.[4]

필자는 당시 KT가 도입하고자 하였던 '쿡 스마트웹'에 대하여 반대의사를 분명히 하면서 그 치명적 위험성을 '독극물'에 비유하기까지 하였는데, 필자의 이러한 발언에 그 외국인의 표정이 심히 일그러지는 것을 수차 확인할 수 있었다. 토론회를 마치고 나오면서, 우연히 그를 다시금 로비에서 마주치게 되었다. 그의 동료에게 이해할 수 없다는 표정으로 고개를 설레설레 흔들기도 하다가, 무언가 억울함을 토로하듯 열띤 손동작과 함께 다소 격앙된 목소리로 자신의 주장에 힘을 더하고 있는 그의 모습을 먼발치에서 바라봤던 기억이 지금까지도 생생하다.

이 글은, 그러한 그를 위하여 작성되었다. KT에게 판매할 Phorm사의 DPI형 인터넷 맞춤광고 기술이 왜 우리나라에서 사용될 수 없는지를 면밀하게 검토하여, 억울해 하던 그를 위해 뒤늦게 글로나마 설득하고자 함이 본 논문의 취지이다.

본격적인 검토에 앞서 미리 밝혀 두고자 하는 몇 가지가 있다.

먼저, 토론회 이후에 KT는 시험운용한 바 있는 '쿡 스마트웹' 서비스를 상용화할 계획이 없다며 갑작스레 입장을 선회한 바 있다[5]는 점이다. 언론을 통해 밝혀진 이러한 KT의 변화가 사실인지, 아니면 당시 패킷감청에 대한 뜨거운 논란을 피하고자 한 미봉책으로서 대언론용 입장을 표

은 '패킷감청'이 아니라 '패킷도청'이 될 것이다. 통신비밀보호법에 의한 '법원의 허가서'가 없는 상태로 진행되는 사적인 '도청'에 해당하기 때문이다. 그러나 본고에서는 지난 논문과의 융통성 있는 연계를 위하여, 편의상 이를 '패킷감청'으로 표현하기로 함을 미리 밝혀 둔다.

4) 토론회 영상에서도 수차 등장하게 되는 그에 대한 이력과 정보는 <http://www.linkedin.com/in/jbrooksdobbs>, <http://www.linkedin.com/pub/brooks-dobbs/a/292/3bb>, 검색일: 2010.4.1.에서 확인할 수 있다.

5) "KT, 개인형 맞춤 광고 서비스 논란 - 거센 풍랑에 고개 숙인 신 사업", 디시뉴스(DCNEWS.IN), 2010.3.11자, <http://www.dcnews.in/news_list.php?code=economy&id=518113>, 검색일: 2010.4.1.

명한 것에 불과한 것인지를 필자는 반드시 알아내어야만 했다. 왜냐하면 기사의 내용처럼 KT가 당해 서비스를 상용화[6]하지 않는다면, 굳이 이러한 글을 작성할 필요가 없기 때문이다.

그러나 의아하게도 이 의문은 KT의 파트너인 Phorm사가 산통을 깨는 바람에 너무나 쉽게 해결되었다. 상용화 계획이 없다는 KT의 보도로부터 보름 뒤에 보도된 몇몇 기사[7]에서 Phorm사의 CEO는 "한국에서 두 가지의 시도를 성공적으로 완수했으며, 적절한 시점에 상용화할 것"[8]이라고 밝혀 KT의 위장술을 속시원히 밝혀 주었다. 이러한 이유로 KT측의 보도를 신뢰할 수 없음을 밝힌다.

다음으로, Phorm사의 기술이 브라질에서 상용화되었음을 언급하고 싶다. 많은 논란 속에서 그동안 사업을 진행할 수 없었던 Phorm사는, 드디어 올해 3월 26일 브라질에서 'Navegador'로 명명된 그들의 서비스를 개시할 수 있었다.[9] 이러한 Phorm사의 파트너로는 브라질의 선도 ISP업체(우리나라의 예를 들자면 KT)인 'Oi'가 손을 잡았고, 인터넷 사용자에게 선별된 맞춤형 광고를 공급하게 되는 포털(Potal)업체(우리나라의 예를 들자면 Naver, Daum 등)로는 'Estadão', 'iG', 'Terra', 'UOL' 등이 파트너로 나섰다. 그러나 브라질에서도 Phorm사의 항해가 그리 순조롭지만은

---

6) 전기통신사업법상 기간통신사업자에 해당(동법 제5조 제1항)하는 KT가 '쿡 스마트웹' 서비스를 어떠한 형태로 상용화할지는 구체적으로 알려져 있지 않다. '쿡 스마트웹'과 같은 내용의 사업은 기간통신사업에 포함되기가 곤란하므로, KT와 Phorm의 합작회사 형태의 새로운 법인이 사업주체로 등장하지 않을까 추론해 본다.

7) The Register, "Phorm turns up in Brazil", 2010.3.26자, <http://www.theregister.co.uk/2010/03/26/phorm_brazil/>, 검색일: 2010.4.1; London Stock Exchange Market News, "Phorm, Inc. Commercial Deployment in Brazil", 2010.3.26자, <http://www.londonstockexchange.com/exchange/prices-and-news/news/market-news/market-news-detail.html?announcementId=10427027>, 검색일: 2010.4.1.

8) Chief executive Kent Ertugrul said today: "Beyond Brazil, we have successfully completed two trials in Korea, about which we will update the market in due course, and we are now active in almost every other major internet market worldwide."

9) 앞서 주 7에서 밝힌 기사가 바로 Phorm사의 브라질 진출을 보도한 기사들이다.

않은 것으로 보인다. 출항과 더불어 우려의 목소리가 나오고 있고,[10] 최근 들어서는 브라질 경쟁당국의 혐의를 받고 있다는 소식 또한 나오고 있기 때문이다.[11]

이 지점에서 언급하고 싶은 점은, 왜 유럽이나 북미가 아닌 브라질이고 그 다음이 우리나라인가 하는 점이다. 아마도 Phorm사는 IT 기반시설의 수준과 인터넷 보급률이 높은 나라 중에서 관련입법이 허술하고 프라이버시 보호 수준이 낮은 국가를 지목한 것이라 생각된다. 이러한 불쾌한 판단이 이 글을 쓰는 또 하나의 동기가 되었음을 밝힌다.

마지막으로 DPI형 인터넷 맞춤광고의 문제가 우리 앞에 새롭게 떨어진 우리나라만의 문제가 아니라, 이미 수년전부터 국제적으로 공유되어 온 제법 익숙한 쟁점이라는 것을 밝히고 싶다. 이는 본 논문이 'NoDPI.org', 'EthicalNetworks.org' 등 DPI기술을 반대하는 프라이버시 관련 국제단체의 지지와 연대에 의해 작성되었다는 점에서 쉽게 이해할 수 있다. 특히 'NoDPI.org'의 활동가인 Mr. Keith. Mallen은 방대한 정보제공과 끊임없는 열정으로 이 글의 작성에 있어 많은 영감을 불어넣어 주었다. 한국에 대한 그의 관심과 열정에 크나큰 감사의 말씀을 드리면서, 본격적인 검토를 시작하고자 한다.

---

10) Gaspari, Elio, "A trapaça do rastreador da Oi no Velox", 2010.3.31자, <http://www.linearclipping.com.br/MEC/m_stca_detalhe_noticia.asp?cd_sistema=55&cd_noticia=1093446>; <http://www.linearclipping.com.br/MEC/m_stca_detalhe_noticia.asp?cd_sistema=55&cd_noticia=1093388>, 검색일: 2010.4.1.

11) 우리의 공정거래위원회에 해당하는 브라질의 경쟁당국인 '경제보호행정위원회(Conselho Administrativo de Defesa Econômica)'로부터 불공정거래 혐의를 받고 있다. 이 사건의 진행에 관하여는 <http://www.cade.gov.br/Default.aspx?d95aad7ab86e80946fa06cce61>, 검색일: 2010.4.1.의 화면에 등장하는 링크를 클릭하면 확인할 수 있고, <http://www.cade.gov.br/temp/t245201019008085.pdf>, 검색일: 2010.4.1. 및 <http://habeasdata.doneda.net/2010/05/06/a-cartada-final-da-phorm-no-brasil-parceria-com-empresa-do-grupo-oi-retirada-da-pauta-do-cade/>, 검색일: 2010.4.1. 등을 통해서도 이러한 상황을 파악할 수 있다.

Ⅱ. DPI형 맞춤광고의 기술적 분석

맞춤광고는 말 그대로 특정 개인에게 최적화된 광고를 하는 방식을 말한다. 불특정다수를 상대로 일방적인 홍보를 하던 종래의 광고형태와는 달리, 광고의 대상이 되는 개인에 대해 수집된 정보를 바탕으로 그의 관심분야와 예측가능한 수요를 미리 분석하고 이를 광고마케팅의 수단으로 활용하는 적극적인 형태의 광고방식이다.

1. 인터넷 맞춤광고 개관

일반 오프라인 매체를 통한 광고, 예를 들어 전단지 광고, 신문이나 잡지 등 인쇄매체상의 광고, 길거리의 광고판이나 TV·라디오 등의 방송매체를 통한 광고는 그 대상을 특정하지 않은 채 진행되는 광고라는 점에서 광범위한 노력에 비해 효율이 높을 수는 없다. 이에 반하여, 인터넷을 통한 맞춤형 광고는 인터넷 이용자의 개인정보(성별, 연령, 지역 등)와 인터넷 이용습관(주이용 웹사이트 및 서비스 유형, 이용 빈도, 관심 검색어 등)에 관한 정보를 수집하여 해당 이용자의 관심이나 필요, 취미 등을 분석·분류하여 특정 개인에게 최적화된 광고를 선별하여 제공하는 방식[12] 이므로 그 효율을 극대화시킬 수 있다는 장점이 있다.

그렇다면 인터넷 이용자가 인터넷 서핑을 할 동안, 누가 어떠한 방식으로 어떤 정보를 취합할 수 있기에 이렇듯 사람을 알아보는 용한 광고가 가능한 것인가?

1.1. 인터넷 맞춤광고의 당사자

인터넷 맞춤광고 시장에는 제품홍보를 원하는 광고주, 인터넷 사이트를 운영하면서 광고를 게재할 수 있는 공간을 가지고 있는 광고사업자(흔히 ‘Media’, ‘Publishers’ 등으로 칭해지나, 본고에서는 편의상 ‘광고사

12) 한국인터넷진흥원, “온라인 맞춤형 광고에 대한 인식조사”, 2009년 하반기 인터넷이슈 기획조사(한국인터넷진흥원, 2009), 1쪽.

업자'라 칭하기로 함), 그리고 양자를 매개하는 대행사, 이렇게 세 명의 주체가 있다.[13]

광고사업자는 'naver.com', 'daum.net' 등과 같은 포털사이트는 물론 인터넷 신문이나 인터넷 쇼핑몰 등 광고를 게재할 수 있는 공간을 가지고 있는 사이트의 운영자로, 각 사이트가 가지고 있는 '사용자 교통량'에 따라 광고가격을 정해 광고주에게 광고 공간을 제공하는 사업자이다.

대행사는 각 나라마다 그 형태가 상이하긴 하나, 미국의 상황을 기준으로 하자면 사용자의 접속이 가장 많은 사이트(우리의 예를 들자면 naver.com의 메인 화면)인 '프리미엄 광고공간(Premium Space)'의 대행을 담당하는 '광고 에이전시(Ad Agency)'와, 메인화면상에서 클릭을 통해 이동하게 될 때 만나는 사이트나 이메일 접속 사이트 등의 '2차적 시장(Secondary Market)' 광고공간의 대행을 전담하는 '제3자 광고네트워크사(3rd Party Ad Networks)'[14]로 구분할 수 있다. 쉽게 생각하자면 광고상품의 판매를 중개하거나 주선하는 회사 정도로 생각해 볼 수 있겠으나, 실제로는 이들 또한 독립된 서버(Sever)를 가지고 있는 네트워크 사업자이다.

예를 들어, 인터넷 사용자가 포털사이트에 접속하여 로그인(Login)을 한 경우를 생각해 보자. 가장 잘 보이는 중앙 상단부나 좌우측 공간에 각종 광고배너가 화려하게 사이트를 장식하고 있는 화면을 쉽게 떠올릴 수 있다. 이 장면을 기술적으로 표현해 보면 이러하다.

먼저, 인터넷 접속을 위해 사용자가 웹-브라우저를 가동하고 주소란에 기억하고 있는 주소를 기입한다(예를 들어 'www.naver.com'). 웹-브라우저는 해당 주소를 이해하고는 곧장 '네이버 서버'에다 해당사이트의 화면

---

13) 양지연, "온라인 맞춤형 광고: 개인정보보호와 정보이용의 균형점을 찾아서, 미국 FTC와 EU의 가이드라인에 비추어", LAW & TECHNOLOGY 제5권 제2호(서울대학교 기술과법센터, 2009), 2-3쪽의 내용을 필자의 시각에서 재구성하였음.

14) 국내에는 아직 널리 보급된 형태는 아니지만, 구글, 야후, 마이크로소프트사 등 외국계 인터넷 기업의 경우에는 모두 제3자 광고네트워크사를 자회사의 형태로 보유하고 있으며, 이들은 주로 프리미엄 광고공간(Premium Space)에 비해 판매력이 떨어지는 2차적 시장(Secondary Market)에 해당하는 광고 공간을 효율적으로 판매하기 위해 특성화된 대행사이다.

송출을 요청하게 된다. 네이버 서버는 준비된 화면을 송출하게 되는데, 페이지의 구성형태(프레임)와 각종의 구성요소(그림이나 문자 등)는 물론 준비된 광고의 내용도 동시에 송출할 것이다. 이렇게 받은 내용물들을 웹-브라우저가 다시금 잘 정리하여 우리에게 보여 주게 된다.

여기서 광고 부분을 좀 더 자세하게 살펴보자. 사이트의 다른 구성요소처럼 네이버가 준비하여 네이버 서버에서 직접 송출하는 광고도 있을 수 있지만, 반드시 그래야만 하는 것은 아니다. 만약, 네이버가 최근 제3자 광고네트워크사와 광고계약을 체결한 바가 있다면, 해당 광고 부분만은 네이버 서버가 아니라 제3자 광고네트워크사의 서버에서 따로 송출해 줄 수 있다. 우리가 사용하는 웹-브라우저가 이렇듯 여러 서버에서 송출받은 내용을 한 페이지에 동시에 보여줄 수 있는 기능이 있기 때문이다.[15][16]

1.2. 사용자에 대한 특정방법

맞춤광고의 가장 큰 특징은 사람을 알아본다는 것이다. 어떤 사이트를 방문할 경우 그 사이트에서 그 방문자에게 가장 적합한 광고를 한다는 것은, 광고를 하는 해당 사이트의 입장에서는 그 방문자가 누구인지를 특정할 수 있어야만 한다.

1.2.1. 로그인(Login) 정보

가장 쉬운 특정방법은 로그인 정보이다. 우리가 어떠한 사이트에 회원가입을 하게 되면 각종 신상정보를 제공하게 된다. 성명, 주민등록번호, 생년월일, 주소와 성별 등은 기본이고, 때로는 기호나 취미 및 관심분야, 심지어 결혼여부나 종교까지도 기입하게 되면서, 마지막에 개인정보 보호

---

15) 사용자의 입장에서는 그 송출자가 네이버 서버이건 제3자 광고네트워크사의 서버이건 상관없이, 그냥 한 페이지의 일면에서 화려한 광고배너가 열심히 움직이고 있다는 상황만을 목격할 뿐이다.

16) 따라서 오프라인 광고매체와는 달리 인터넷상의 광고는 이들 양자, 즉 광고사업자와 대행사가 함께 광고 업무를 수행하게 된다고 표현하는 것이 좀 더 정확하다.

정책이나 약관사항에 동의해야만 가입이 완료된다. 이러한 정보를 이미 축적하고 있는 사이트의 입장에서는 해당 가입자가 로그인을 할 경우 조금만 노력하면 쉽게 광고의 효과를 높일 수 있다. 예를 들어 남자회원에게는 면도기 광고를, 여자회원에게는 화장품 광고를 부각시키는 것이, 남녀를 구별하지 않고 하는 광고보다 훨씬 효과적일 것이다.

이러한 로그인 정보는 개인 신상에 관하여 정확한[17] 1차 정보이긴 하나, 광고를 위한 분석대상으로서는 너무 간단한[18] 정보이기 때문에 인터넷 맞춤광고를 위한 주요정보로까지는 활용되지는 않는다. 또한 대부분의 국가에서 그 유출로 인한 심각한 부작용을 경험하여 이에 관한 규제를 마련해 두고 있다는 점도, 사이트의 입장에서는 광고용으로의 자유로운 사용을 망설이게 하는 요소가 되기도 한다.

1.2.2. IP주소(IP address)

IP주소는 패킷(Packet)화하여 데이터를 주고받도록 되어 있는 현재의 네트워크방식에 있어, 인터넷에 연결되어 있는 각 컴퓨터마다 하나씩 부여받게 되는 고유한 주소이다. 따라서 사용자를 특정하기 위한 훌륭한 식별자가 될 수 있으나, 정확히 말하자면 사용자를 특정한다고 표현하기보다는 사용자가 사용한 컴퓨터를 특정한다고 보는 것이 맞다.

그러나 통상적으로 동일한 컴퓨터에서 인터넷 접속을 반복하게 되는 우리의 일상을 고려해 본다면, 사이트의 입장에서는 이러한 차이가 큰 문

17) 국제적으로 보면 인터넷상에서도 실명을 요구하는 우리나라와 같은 경우는 희박하므로, 다른 나라의 경우에는 정확성에 대해서도 단정할 수 없다.

18) 예를 들어 '30세인 여성'이라는 정보는, 최적화된 광고를 하기에는 너무 간단하다는 것이다. 물론 30세인 여성이라는 정보가 전혀 무의미한 것은 아니지만(무턱대고 주름방지 화장품 광고를 해보는 것이 가능은 하겠지만), 광고주의 입장에서는 광고효과의 극대화를 위해서는 좀 더 정확하고 자세한 정보가 필요하다는 것이다. 즉, 30세인 여성이 올 여름휴가철의 유럽행 비행기편과 지중해 여행에 관련한 정보를 검색했다는 사실을 알게 된다면, 광고주는 어떠할까? 지중해의 햇살에 대비한 자외선 차단력이 있는 화장품들과 여행용으로 알맞은 휴대용 화장품 세트를 집중적으로 광고한다면, 아마 훨씬 정확하고 능동적인 광고가 될 것이다.

제가 되지는 않을 것이다. 흔히 사이버 범죄의 수사실무에 있어서 IP주소 추적이 주요한 수사기법으로 등장하는 것을 보아도, 사용자의 특정가능성을 충분히 신뢰할 수 있을 것이다. 또한 사이트의 입장에서는 사용자의 접속과 동시에 저절로 알게 되는 정보이기 때문에, IP주소에 대한 지득과 취합에 대하여 별다른 부담이 없다는 장점이 있다.

1.2.3. 쿠키(Cookie)

네이버(naver)사이트에 로그인을 해서 메일을 확인한 사용자가, 어제 밤에 옥션(auction)사이트에서 구매했던 물건의 배송상태를 확인하기 위해 동일한 브라우저상에서 그 주소를 바꾸어 옥션으로 접속했다고 가정하자. 그리고는 방금 전에 확인했던 메일의 답신을 작성하기 위해 다시금 네이버사이트로 주소를 바꾼다면, 이번에는 별도의 로그인 없이 바로 네이버의 메일사이트로 들어갈 수 있게 된다. 똑똑한 브라우저는 사용자가 다른 곳을 다녀와도 이미 네이버사이트에 로그인을 했었다는 사실을 기억하고 있는 것이다.

이렇듯 브라우저는 매번 접속할 때마다 로그인을 해야 하는 불편을 덜어주기 위해, 접속정보 등의 방문흔적을 기록한 작은 사이즈의 파일을 사용자가 접속한 해당 사이트와 주고받게 된다.[19] 이 파일을 '쿠키'라고 한다.[20] 쿠키에 기록되는 내용은 딱히 정해진 바가 없으므로 해당 사이트 측에서 임의적으로 결정하게 된다. 즉 접속을 위한 기본정보(사이트의 도

19) 앞의 예를 빌어 좀더 정확히 말하자면, 처음 네이버에 로그인을 한 당시에 사용자의 브라우저에는 이미 'naver'라는 도메인 이름이 새겨진 쿠키가 심어지고, 옥션(auction)에 접속을 한 때에도 마찬가지로 옥션이 발행한 쿠키가 사용자의 컴퓨터에 심어지게 된다. 다시금 네이버에 접속을 하게 된 때에는 사용자의 브라우저가 네이버가 발행했던 쿠키를 네이버 서버에 확인시킴으로써 로그인 절차가 생략될 수 있는 것이다.

20) 쿠키는 해당 서버와의 재접속에 대비하여 '사용자의 컴퓨터'에 서버와의 연결고리가 되는 내용을 기록한 작은 흔적을 남겨두는 것이고, 이와 반대로 '해당 서버'쪽에 재접속에 대비한 흔적을 남기는 기술을 '세션(Session)'이라고 한다. 이렇듯 사용자의 공간에 과자 부스러기처럼 흔적이 남게 된다는 의미에서, 그 이름을 '쿠키'라고 부르게 되었다고 한다.

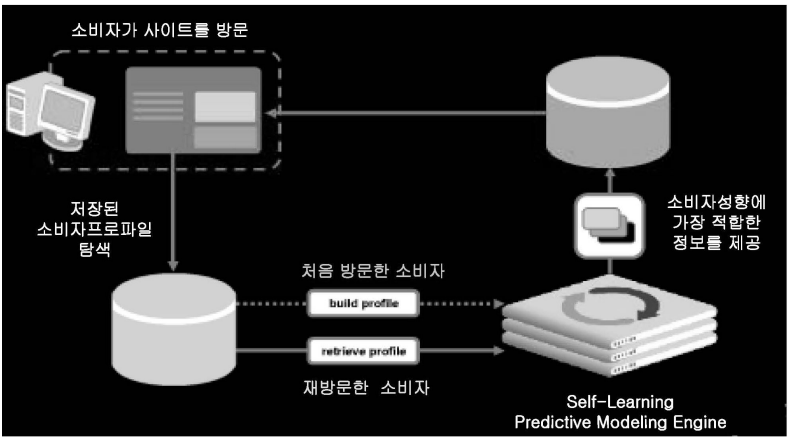
메인네임, 그 사이트를 구분하는 숫자 등)뿐만이 아니라, 접속시간이나 방문한 사이트의 주소는 물론 사용자의 주민등록번호나 로그인정보(ID와 Password)까지도 기록하도록 설정할 수도 있다. 따라서 사이트 측이 원하는 정보를 기록하게끔 자유로이 설정할 수 있으므로 매우 요긴한 정보수집 수단이 되는 동시에, 사용자의 정보가 별다른 통제 없이 유출될 우려가 있기 때문에 개인정보 보호의 문제[21]가 발생한다.

맞춤광고에 있어서도 쿠키의 정보가 가장 핵심적인 사용자 특정방법으로 활용된다. 일단 한번 접속한 바 있는 사용자가 재접속해올 경우, 사용자의 정보를 가득히 담아오도록 미리 심어놓았던 쿠키를 열어보기만 하면 사용자의 특정이 쉽게 가능해지기 때문이다.

1.3. 인터넷 맞춤광고의 운영구조

이러한 정보들을 가지고 광고사업자나 대행사의 맞춤광고가 시작된다.

<그림 1: 인터넷 맞춤광고의 운영구조>[22]



21) 이에 관한 전반적인 내용은 김민중/안종근/육희숙, "인터넷상 쿠키를 통한 개인정보침해의 법적 문제", 법학연구 제24집(전북대학교 법학연구소, 2006) 참조.

22) 나종연, "온라인 타겟 마케팅과 소비자 프라이버시 보호", 한국 CPO 포럼 2009년도 제5차 Privacy Round Up 발표자료(2009), 3쪽의 도안을 인용.

물론 단순히 이러한 정보들의 분류나 조합들만으로 맞춤광고를 하는 것은 아니고, 이들을 기초적인 식별자로 활용하여 인터넷 사용자의 각종 행위유형(기입한 검색어와 이를 통해 이동한 링크의 주소, 자주 접속하는 사이트의 주소와 그 유형, 열람한 페이지의 내용과 구매한 상품의 종류 등)을 다시금 추가분석하여 이에 더하게 된다.[23] 자료들의 축적과 정확한 분석을 위하여 보통 광고사업자나 대행사는 그 업무를 전담하는 별도의 시스템(자기학습형 예측모델링 엔진, Self-Learning Predictive Modeling Engine)을 보유하고 있다. 이러한 복합적인 과정을 거쳐 세밀하게 조정된 광고가 해당 사용자에게 송출되는 것이다.

구체적으로는, ① 인터넷 사용자가 하나의 사이트와의 상호작용을 통해 얻게 된 정보만을 이용해서 이루어지는 광고유형으로서 '사이트 맞춤형 광고(Site Targeting)'[24]나 '컨텍스추얼 맞춤형 광고(Contextual Targeting)',[25] ② 인터넷 사용자가 찾은 검색어, 방문한 웹페이지, 클릭한 링크, 사용자가 본 내용 등 사용자의 행동 양태에 대한 정보가 일정기간동안 수집·저장·축적·분석되어 구축된 광고용 데이터(Ad Profile Data)를 기반으로 이루어지는 광고유형으로서 '행동양태 맞춤형 광고(Behavioral Targeting)', ③ 구축된 광고용 데이터와 함께 사용자의 등록정보나 공개된 정보를 동시에 이용하는 '프로파일 맞춤형 광고(Profile Targeting)' 등으로 크게 구분[26]해 볼 수 있다.[27]

---

23) 이렇듯 분석대상이 되는 사이트들은, 모두 맞춤광고의 주체들(광고사업자나 대행사)과 사전계약을 통해 이러한 분석에 동의한 자들이다.

24) 각종의 사이트를 미리 여러 가지의 범주(금융, 경제, 건강, 미용, 여행, 자동차 등)로 분류해놓고 있는 상황에서, 만약 여성인 인터넷 사용자가 여행관련 범주의 사이트를 방문하게 되면 이 페이지 상단의 배너에 여성용 여행용품의 광고를 송출하는 형태임.

25) 인터넷 사용자가 읽은 페이지의 제목이나 검색한 내용 등을 즉각적으로 수집하여 이에 부합하는 광고를 바로 송출하는 형태임.

26) 이러한 구분은 양지연, 앞의 글, 5-6쪽과 나종연, 앞의 글, 4-9쪽의 내용을 필자의 시각에서 재구성하였음. ①의 경우를 1세대 맞춤광고 유형으로 ②와 ③의 경우를 2세대 맞춤광고 유형으로 구분하는 견해로는 임종인, "DPI 기술 활용 민간 관심기반 광고서비스의 문제점 검토", 패킷감청의 문제점과 개선방안에 대한 토론회 자료집(2010), 38쪽.

2. DPI형 맞춤광고의 차별성

소위 3세대라 불리우는 DPI형 맞춤광고[28]는, DPI라는 패킷감청 기술을 정보수집의 방식으로 활용한다는 대표적인 차이점과 함께 광고시스템의 운영주체와 참가자, 그리고 수집하는 정보의 종류와 분량에 있어 지금까지 설명한 1세대 또는 2세대 맞춤광고의 형태와 뚜렷한 차이가 있다.

2.1. DPI형 맞춤광고의 구조

DPI형 맞춤광고가 사용하는 DPI기술은 사용자의 컴퓨터와 연결되어 있는 인터넷 회선에다 직접 패킷감청 장치를 설치하게 된다. 따라서 1·2세대 인터넷 맞춤광고에서는 등장하지 않던 인터넷 회선회사(즉 ISP)가 새로운 주체로 등장하게 된다.

그 운용구조를 간략하게 살펴보자.[29] 먼저 ① DPI형 맞춤광고사(우리나라의 경우 Phorm, 이하 Phorm)가 ISP(우리나라의 경우 KT, 이하 KT)

---

27) 이에 더하여 '광고 선호 관리자(Ad preference Manager)'라는 관심분야 설정 시스템을 활용하여 키워드나 콘텐츠 외에 추가적인 정보를 활용하여 고객의 관심에 부합하는 광고를 제공하는 형태로, 현재 Google이 운용중인 '인터넷 기반 광고(Internet Based Advertising)'를 또 하나의 유형으로 추가할 수 있다. 이에 관한 간략한 소개는 <http://www.freepatentsonline.com/7319975.html>, <https://www.google.com/accounts/ServiceLogin?service=adwords&hl=en_KR&ltmpl=adwords&passive=true&ifr=false&alwf=true&continue=https%3A%2F%2Fadwords.google.com%2Fum%2Fgaiaauth%3Fapt%3DNone%26ugl%3Dtrue&sourceid=awo&subid=il-iw-ha-EN_GLBL_SKWS-AWFEEN&gsessionid=G9_gInx4moJikdBnZ9CUDg>, 검색일: 2010.4.1. 등에서 확인할 수 있다.

28) 이러한 유형의 광고기술을 상업화한 경우로는 미국에서의 NebuAd, 영국에서의 Phorm 등의 사례가 있으며(오길영, 앞의 글, 414-417쪽), 인터넷 상에서의 채팅내용을 패킷감청하여 맞춤광고를 하는 EchoMetrix사가 개발한 'Sentry and Family Safe'라는 소프트웨어가 최근 논란이 되고 있다.

29) 이는 Phorm사의 기술시연에 직접 참가하여 그 메커니즘을 기술적으로 분석한 Cambridge대학 Computer Laboratory의 Richard Clayton교수의 보고서[Clayton, Richard, "The Phorm 'Webwise' System"(2008), <http://www.cl.cam.ac.uk/~rnc1/080518-phorm.pdf>, 검색일: 2010.4.1]의 내용을 필자의 시각에서 재구성한 것임.

와 계약을 체결하여 KT의 인터넷 회선에다 패킷감청장비[30](이하 DPI 장치)를 설치한다. ② KT 회선가입자(즉 쿡[31]인터넷서비스 가입자)가 웹-브라우저를 작동해 특정 사이트의 주소(예를 들어 'www.cnn.com')를 주소창에 기입한다. ③ 브라우저의 접속요청을 담은 데이터(쿠키)를 Phorm의 DPI 장치가 가로채 여기에다 사용자 식별을 위한 Phorm의 꼬리표(Unique Identifier, UID[32])를 달도록 변조한 다음 사용자의 브라우저가 원래 입력했던 사이트로 변조된 쿠키를 재전송하게끔 시킨다. ④ 사용자의 브라우저가 꼬리표가 달린 쿠키를 가지고 해당 사이트(www.cnn.com)에 접속하면, 사이트는 화면을 구성하는 각종 데이터들을 사용자의 컴퓨터로 송출한다. ⑤ Phorm의 DPI 장치가, 회선을 오가는 수많은 데이터 가운데 사용자를 향해 송출되어 오는 데이터(즉 꼬리표가 달린 데이터)를 선별하여 가로챈다. ⑥ 가로챈 데이터를 복사하는 동시에 꼬리표를 떼어내고 사용자의 컴퓨터로 보낸다. ⑦ 데이터 복사본을 Phorm의 분석시스템(Open Internet Exchange, OIX)에 따로 보내어 이를 분석·분류하고 사용자에 최적화된 광고정보를 도출한다. ⑧ 분석·도출된 광고정보를 제휴된 사이트에 알려주고, 추후 사용자가 제휴사이트를 방문할 때에 맞춤광고를 하게끔 한다.

이를 KT가 제공한 도안을 통해 살펴보면 다음과 같다.[33]

---

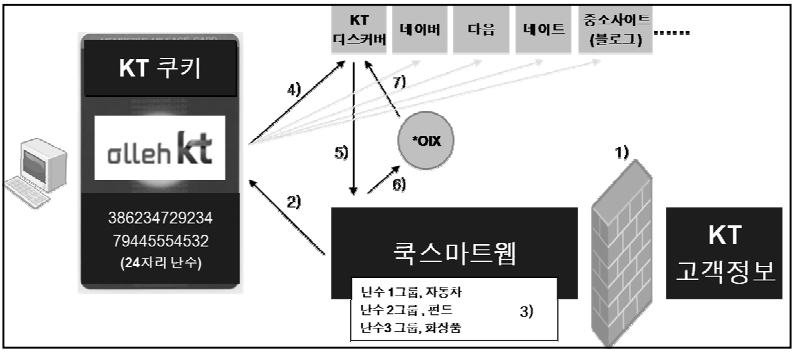
30) Phorm사의 장비가 정확히 어떠한 것인지는 아직 국내에는 알려진 바가 없다. 그러나 Clayton 교수는 이를 전형적인 DPI용 네크워크 장비인 'Layer 7 switch'로 표현하고 있다(Clayton, 앞의 글, 2쪽). 원래 'Layer 7 switch' 장비는 회선을 오가는 패킷의 내용을 분석하여 이를 바탕으로 패킷에 대한 부하분산, 리디렉션, 필터링 등을 통해 지능적으로 트래픽을 관리하는 고성능 네트워크 스위치 장비로 개발되었다.

31) 종전에는 '메가패스(Megapass)'라는 브랜드를 사용하였으나, 최근 이를 쿡(Qook)으로 변경하였다.

32) KT가 제공한 도안에 따르면, 이러한 UID로 24자리의 난수를 사용한다고 한다.

33) <그림 2>의 도안은 토론회의 발제를 맡은 임종인, 앞의 글, 38쪽에서 인용. 토론회 당시 토론자로 참여하였던 KT측 대리인도 토론문을 통해 본 도안과 대동소이한 도안을 제공한 바 있다. 그러나 ① 도안의 짜임새가 발제자가 제공한 본 도안보다 떨어지는 점, ② 그 내용과 설명에 있어 차이점이 전혀 없다는 점, ③ 발제자가 본 도안의 출처를 'KT'로 명기하고 있어 위 도안 또한 KT측

<그림 2: DPI형 맞춤광고의 운영구조>



1) KT고객정보와 차단
2) 24자리 난수를 쿠키에 담아 동의한 고객의 PC에 전송 : 쿡스마트웹 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 쿡스마트웹 경로를 통해 난수가 쿡스마트웹에 전달
6) 난수가 어떤 관심표 그룹에 속하는지 확인 후, 관련 콘텐츠 혹은 광고를 보내도록 명령
7) 사이트의 지정된 위치에 맞춤 콘텐츠 및 광고 전송
* OIX: Open Internet Exchange

위 도안에서 볼 수 있듯이 DPI형 맞춤광고 기술을 통해 발생하는 가장 큰 변화는, 종래의 인터넷 맞춤광고에서 광고사업자로서 주도적 당사자의 역할을 하던 포털업체(도안에서는 네이버, 다음, 네이트 등)가 여기서는 평범한 '제휴된 사이트'로 취급된다는 점이다. 즉 DPI형 맞춤광고의 핵심기술은 '인터넷 회선'에다 '패킷감청 설비'를 설치·운영하는 것이고, 따라서 인터넷 회선을 가지고 있는 KT와 패킷감청 설비를 운영하게 되는 Phorm이 주도적 당사자가 된다. 이는 곧 광고이익의 귀속처가 대전환

의 자료를 바탕으로 작성되었음을 확인할 수 있다는 점 등의 이유로 KT측 대리인의 도안을 채택하지 않았음을 밝힌다. KT측 대리인의 도안은 구태언, "온라인 맞춤광고(OBA)에 대한 입장", 패킷감청의 문제점과 개선방안에 대한 토론회 자료집(2010), 78쪽에서 확인할 수 있다.

됨을 의미하며, 나아가 종래의 인터넷 광고시장 붕괴와 재편을 예고하는 것이다.

인터넷 산업을 이끄는 가장 큰 수익인 광고수익을 포털업체가 독식하다시피 하는 현실에서, 그저 인터넷 회선 사용료로만 만족해야 했던 각국의 ISP 업체들에게는 DPI형 인터넷 맞춤광고야말로 정말이지 포기할 수 없는 장미빛 미래가 될 것이다.

2.2. DPI형 맞춤광고 기술의 함정

KT가 제공한 도안 하단의 설명부분을 보면, 방화벽을 사용해 고객정보와 차단을 시키고(설명 1) 24자리의 난수를 사용하여 익명화를 실시(설명 2)하는 등 개인정보 보호를 위해 두터운 안전장치를 마련하고 있고,[34] 나아가 사용자 분석을 위해 수집되는 사이트는 '제휴된 사이트'에 한정됨(설명 4와 5)을 밝히고 있다. 또한 그 어디를 살펴보아도 패킷감청이 실시된다거나 쿠키의 변조가 시행된다고 설명되어 있지 않다.

물론 Phorm사의 입장에서는 이러한 메커니즘이 상당 부분 중요한 영업비밀에 속할 수 있을 것이고 KT의 입장에서는 기술의 우수성과 안전성을 홍보하기 위해 가급적 불리한 부분을 감추는 것이 당연하겠으나, 이러한 설명이 소극적으로 함구하는 정도인지 아니면 적극적으로 허위의 설명을 하고 있는 것인지는 분명히 해야 할 것이다.

위 도안에서 생략된 부분들을 중심으로 기술적인 맹점을 짚어보기로 하자.

2.2.1. DPI와 그 대상

도안에 있어 DPI는 어느 지점에서 실시되는가? 인터넷 주소(예를 들어 www.cnn.com)를 기입하여 특정사이트에 접속을 시도하는 사용자의 최초 통신을 가로채는 DPI는 이미 '설명 2'의 화살표 이전에 있게 되나, 이는

---

34) 이를 강조하기 위하여 토론자로 참여한 KT측 대리인의 토론문(구태언, 앞의 글, 78쪽)에는, 설명 2와 설명 3의 말미에 굵은 글씨체로 "개인식별불가"라고 표시하였고, 설명 5의 말미에는 "3자 정보제공 없음"이라고 덧붙였다.

도안에서 생략되었다. 또한 '설명 5'의 화살표는 그 부적절한 설명[35]과는 달리, 사실은 DPI 행위가 실시되게 된다. 인터넷 사용자를 기준으로 볼 때, 인터넷 사용자의 모든 송·수신정보가 DPI되므로 무차별적이고 전방위적인 '훔쳐보기'가 실시된다고 보는 것이 정확하다. 다만 국정원의 패킷감청과 차이가 있다면, ① 피감청 서비스(즉 쿡 스마트웹)에 가입한 당사자가 다수이므로 이들을 구분하기 위하여 꼬리표(UID)를 달아준다는 점, ② 감청주체가 사기업이라는 점, ③ 판매를 위해 수집된 '도청'[36]자료가 자동으로 분석·축적된다는 점 등이다.

다음으로, 수집의 대상이 되는 '제휴된 사이트'에 대하여 살펴보자. KT 측의 설명에 의하면 "PC(이용자)가 제휴된 사이트를 방문하면 PC(브라우저)가 난수를 사이트로 전달"한다(설명 4)라고 하면서, "제휴된 사이트의 쿡 스마트웹 경로를 통해 난수가 쿡 스마트웹에 전달"한다고 표현하고 있다. 이는 곧 정보수집의 대상이 되는 사이트는 사전에 협의된 '제휴된 사이트'에 한정됨을 의미하므로, 쿡 스마트웹 서비스가 폐색망(Closed Network)에서 진행됨을 의미한다.

여기서 필자는 "그렇다면 굳이 모든 데이터를 망라적으로 분석하게 되는 DPI 기술을 활용할 이유가 있는가?" 하는 의문을 가지게 되었다. 1·2세대 맞춤형 광고에서처럼 '제휴된 사이트'에서 필요한 정보만을 골라서 전달해 준다면, 회선을 오가는 막대한 분량의 데이터를 몽땅 수집해서 다시금 필요한 정보만을 선별해야 하는 비효율적 수고를 덜 수 있기 때문이다. 또한 이런 방식이라면 '제휴된 사이트'에서만 필요한 정보를 수집할 수 있다는 1·2세대의 벽을 넘어, 사용자가 접속하는 전세계의 모든 웹-페이지에서 정보를 수집할 수 있다는 DPI형 맞춤광고의 가장 큰 장점

35) Phorm사의 기술은 '제휴된 사이트'만을 대상으로 하지 않으며, KT의 인터넷 회선 전체이지 별도의 '쿡 스마트웹의 경로'라는 것이 존재하지도 않는다. 또한 "난수가 쿡 스마트웹에 전달"되는 것으로 표현하고 있으나 그 어떤 사이트도 '쿡 스마트웹'에게 전달하지 않으며, 오히려 '쿡 스마트웹'이 사용자에게 전달하고자 송출된 데이터들을 훔쳐보는(DPI) 것에 불과하다.

36) DPI형 인터넷 맞춤광고에서의 DPI는 정확히 도청에 해당하나, 본고에서는 지난 논문과의 융통성 있는 연계를 위하여 편의상 패킷'감청'이라고 표현하고 있음을 이미 앞에서 밝힌 바 있다(주 3).

이 무의미해지기 때문이기도 하다.

이러한 의문은 “KT의 이러한 설명이 사실인가?” 하는 물음표로 변모하였다. 왜냐하면 Phorm의 데이터분석엔진의 이름이 폐색을 의미하는 ‘closed’가 아니라 개방을 의미하는 ‘open’을 담고 있는 OIX(Open Internet Exchange)로 명명되었다는 것을 발견했기 때문이다. 이러한 단초를 들고 긴 시간동안의 확인을 거듭한 결과, 필자는 KT측의 이러한 설명이 ‘거짓’이거나 최소한 ‘오기’ 이상이라는 확신을 가지게 되었다. Phorm의 시스템을 설명하고 있는 그 어떤 문서에서도, Phorm의 정보수집이 ‘제휴된 사이트’만을 대상으로 하는 폐색망에서 운용된다는 설명을 찾아볼 수 없었기 때문이다.[37] 오히려 개방망(Open Network)에서의 정보수집을 전제하면서 웹-검색엔진(Web Crawler)과의 차이점에 대해 검토를 하고 있거나,[38] 전혀 계약관계가 없는 사이트를 대상으로 정보를 수집하는 심각한 문제점을 가지고 있다는 점을 지적하고 있을 뿐이었다.[39] 나아가 Phorm사의 COO(Chief Operating Officer)인 Virasb Vahidi가 뉴욕타임즈와의 인터뷰에서, 그 수집대상의 범위에 대하여 ‘모든 인터넷(entire Internet)’[40]이라고 밝혀 이를 명시적으로 인정한 기사[41]까지 발견되었다.

---

37) 따라서 ‘제휴된 사이트’가 의미를 가진다면, 이는 정보의 수집대상이 됨을 동의했다는 의미에서의 ‘제휴’가 아닐 것이다. 쿡 스마트웹으로부터 정보를 받아 광고를 하기로 결정한 사이트, 즉 KT의 광고방식을 구매하여 직접 광고를 하게 되는 사이트가 KT와 계약을 했다는 의미에서의 ‘제휴’가 될 것이다.

38) Clayton, 앞의 글, 5-6쪽. 전세계의 모든 웹페이지에 대한 전방위적 정보검색을 목적으로 하는 검색엔진의 경우, 그 검색을 허가하는 범위와 접근을 제한하는 한계점에 대하여 명시한 웹페이지측의 문서(robots.txt)를 준수하게 되는데, Phorm사의 DPI는 이러한 협약조차도 준수하지 않는다는 의구심을 Clayton 또한 버리지 못하고 있다.

39) 그대로 인용하면 다음과 같다. “주로 사용되는 제3자 광고네트워크사를 통한 맞춤형 광고의 경우 수집되는 사용자 정보는 사용자가 방문한 웹사이트와 계약관계에 있는 제3자 광고네트워크사가 수집하는 사용자 정보로 제한된다. 반면에 ISP가 DPI를 통해 수집하는 사용자에 관한 정보는 계약관계의 여부와 상관없이 사용자의 모든 온라인 행태와 사용자가 보는 웹페이지의 내용까지도 수집된다는 점에서 개인정보침해의 이슈가 좀 더 심각하다고 할 수 있다.”: 양지연, 앞의 글, 7쪽 주 9.

40) 기사의 내용을 그대로 인용하면 다음과 같다. “As you browse, we’re able to

기술논문이 아닌 법학논문인 본고에서 이 부분의 의혹을 정확하게 입증하는 것이 불가능하거니와 무의미하기도 하다. 그러나 이상과 같은 검토내용과 더불어 이 부분이 Phorm의 핵심적 기술내용에 해당한다는 점을 고려해 볼 때, 2년여 남짓한 시간동안에 기술내용이 급변경되어 KT에게 전혀 다른 시스템이 공급된다는 것은 상식선에서도 불가능하다고 판단된다.[42]

요컨대 KT의 DPI는 제휴된 폐색망에서만 진행되는 것이 아니라, 사용자가 접속하는 모든 웹사이트, 즉 전세계의 모든 웹-페이지를 대상으로 무차별적이고도 전방위적인 권한 없는 수집을 실시하게 된다.

2.2.2. 쿠키의 변조행위

다음으로 설명 2에서 "24자리 난수를 쿠키에 담아 고객의 PC에 전송"이라고 표현하는 부분을 살펴보자. 앞서 살펴본 바와 같이 '24자리 난수'는 피감청 서비스(즉 쿡 스마트웹)에 가입한 당사자가 다수이므로 이들을 구분하기 위하여 달아준 꼬리표(UID)를 말한다. 설명에 의하면 쿠키에 '담아' 전송한다고 표현하고 있지만, 이를 좀 더 정확히 표현하자면 쿠키를 변조하여 꼬리표를 단다는 것이 맞다. 왜냐하면, 사용자의 의사에 반하거나 사용자가 미처 인식조차 하지 못하는 상황에서 진행되는 일방적 '내용 변경'이 있기 때문이다.

이 부분을 기술적 진행순차에 의해 표현하면 다음과 같다.[43] ①②③과 ⑤⑥⑦⑧은 앞서 설명했으니 ④에 중점을 두어 살펴보기 바란다.

---

categorize all of your Internet actions," said Virasb Vahidi, the chief operating officer of Phorm. "We actually can see the entire Internet."

41) The New York Times, "A Company Promises the Deepest Data Mining Yet", 2008.3.20자, <http://www.nytimes.com/2008/03/20/business/media/20adcoside.html?_r=3&ref=busine&oref=slogin>, 검색일: 2010.4.1.

42) 이러한 필자의 판단이 맞다면, 일국의 국회에서 진행되는 토론회에서 사용되는 토론문에, 고의적인 '거짓'이거나 과실로 인한 '오기'이거나를 불문하고 '허위정보'를 제공하였다는 사실 자체만으로도 KT는 비난받아 마땅하다고 하겠다.

43) 이는 Richard Clayton, 앞의 글, 2-5쪽의 내용을 필자의 시각에서 재구성한 것임.

① 사용자가 접속을 원하는 사이트의 주소(예를 들어 www.cnn.com)를 기입하면, 사용자의 브라우저는 그 접속요청의 신호(Query)를 발송한다.
② 발송된 신호가 회선을 타고 진행하면, Phorm의 DPI 장치가 이를 가로챈다.
③ 가로챈 신호의 내용을 살펴보고 꼬리표의 부착 여부를 검토한다.
④ 검토의 결과 꼬리표가 부착된 바가 없다면, Phorm의 장치는 꼬리표를 달기 위한 유인·변조 행각을 시작한다. 즉 (i) 허위의 '재접속 요청신호[44](www.cnn.com의 서버주소가 일시적으로 www.qooksmartweb.com으로 변경되었으니 그쪽으로 재접속하라는 허위내용의 신호)'를 사용자의 브라우저에 발송한다. (ii) 바뀐 주소로의 재접속을 요청받은 사용자의 브라우저는, 다시금 제공받은 허위주소(www.qooksmartweb.com)로 접속요청의 신호를 발송한다. (iii) 이를 기다리고 있던 Phorm의 서버(www.qooksmartweb.com)는, 사용자의 쿠키에다 추적용 꼬리표를 심는다. (iv) 성공적으로 꼬리표를 단 Phorm의 서버는, 웹-페이지의 내용이 송출되어 오길 기다리고 있던 사용자의 브라우저에 또다시 허위의 '재접속 요청신호'(바뀐 주소인 www.qooksmartweb.com의 서버주소가 또다시 www.cnn.com으로 변경되었으니, 그쪽으로 재접속하라는 허위내용의 신호)를 발송한다.
⑤ 재접속 요청신호를 받은 브라우저는 꼬리표를 단 채로 다시금 제공받은 주소(www.cnn.com)로 접속을 시도한다.
⑥ www.cnn.com의 서버는 (최초의)접속요청을 받고, 해당 페이지를 구성하는 데이터들을 송출한다.
⑦ 꼬리표가 몰고 온 송출 데이터들을 Phorm의 DPI장치가 가로채어 수집·축적을 위한 복사본을 만든다.
⑧ 꼬리표를 떼어내고 원본 송출 데이터를 사용자의 브라우저로 보낸다.

요컨대 Phorm의 장치가 사용자의 브라우저를 속여 다른 장소로 유인한 후, 쿠키의 내용을 변조하여 꼬리표를 달고, 이를 통해 사용자의 데이터만을 구별하여 DPI한다는 것이다.

이처럼 사용자의 브라우저를 '유인'하고 '기망'하며 '변조'하는 Phorm의 절묘한 기술이, 어찌하여 KT측의 도안에는 전혀 등장하지 않는 것인

44) 이를 기술적으로 '307 일시적 재전송 쿼리(307 Response)'라고 한다.

가?[45] 또한 이렇듯 허위와 변조로 채워진 내용을, "24자리 난수를 쿠키에 담아 고객의 PC에 전송"이라는 선량함이 넘치는 문장으로 표현하는 것이 과연 타당한가?

Ⅲ. DPI형 맞춤광고의 법리적 검토

지금까지 살펴본 DPI형 맞춤광고의 기술적 검토를 기반으로 개별 쟁점사항에 대한 법리적 검토를 해 보기로 한다. 각 쟁점들을 살피면서 구체적으로 언급이 되겠으나, KT나 Phorm이 말하는 개인정보 보호나 통신비밀의 보호, 그리고 프라이버시 문제와 관련한 '무결성'의 주장은 전혀 터무니없다는 점을 미리 밝히고 시작하고 싶다. 오히려 허술한 입법으로 대처할 경우, 그 치명적 유해성으로 인하여 돌이킬 수 없는 심각한 사회적 부작용이 초래될 것임을 본고를 준비하면서 다시 한 번 확인하게 되었다.

또한 기술적 검토에서 살펴본 바와 같이, DPI형 맞춤광고의 경우 그 기술적 기반이나 광고시스템의 당사자가 종래의 1·2세대 맞춤광고와는 판이하게 다르다. 즉 완전히 다른 기술인 것이다. 이러한 상이함 덕분에 각 쟁점에 대해 요구되는 규제의 수준 또한 현격한 차이가 있게 됨은 당연한 것이다. 바꾸어 말하건대, 단순히 '맞춤광고'라는 비즈니스 상품명의 표현을 공유한다고 하여, DPI형 맞춤광고를 1·2세대 맞춤광고와 동격으로 취급할 수는 없다는 것을 검토에 앞서 다시 한번 강조하고 싶다.

1. 사용자의 특정 가능성

45) KT측 대리인의 토론문에는 이에 관한 내용이 전무하다. 한편 발제자였던 임종인, 앞의 글, 39쪽에는 이에 관한 도안이 있으나 그 출처에 대해 함구하고 있으므로, 이는 KT측으로부터 제공받은 것이 아니라 발제자 스스로가 작성한 것으로 추정된다. 왜냐하면 발제문을 살펴보면 KT측으로부터 제공받은 도안들은 반드시 그 출처가 KT로 명기되어 있기 때문이다.

인터넷 사용자의 특정 가능성은 비단 맞춤광고 뿐만이 아니라 인터넷 환경에서 비롯되는 각종의 이슈들에 전반적으로 관련되는 본질적인 문제이다. 인터넷상에서 사용자를 특정한다는 것은 단순히 그 사용자를 인지한다는 의미를 넘기 때문이다. 왜냐하면 실제 공식적으로 제공되는 정보가 기본정보라 할 수 있는 로그인 정보에 불과하다 하더라도, 비공식적으로 수집가능한 다른 정보(최근 방문한 사이트의 분류, 자주 방문하는 사이트의 내용, 구매한 상품의 내역 등)와의 결합을 통해 인지의 수준을 넘어 그 사용자의 모든 면모(사상, 관심분야, 기호, 상품의 구매력 등)를 종합적으로 관찰해 볼 수 있기 때문이다. 따라서 규제의 필요성이 대두한다.

한편 이렇듯 얼마든지 비공식적으로 수집가능한 정보의 경우, 수집되는 정보 자체만을 가지고서는 바로 '개인정보'에 해당한다고 인정하기가 어려운 정보일 경우가 많다.[46] 따라서 이에 대한 적절한 수준의 통제라는 것이 그리 선명하지도 않고, 또 워낙에 다양한 형태의 정보가 존재하므로 실제 규제의 형태로 그 모든 다양성을 감당해 내기도 힘들다. 나아가 인터넷 접속을 위해서는 반드시 필요한 정보가 신상정보 이상의 사용자 특정성을 가지기도 하고(IP주소, 접속시간 등), 분석시스템이 가동되지 않는 한 수집되는 각각의 정보만을 가지고는 개인정보의 범주에 포함시킬 수 없는 경우(검색어, 이동경로 등)도 많다. 한마디로 규제하기가 대단히 곤란하다고 할 수 있다.

이에 대하여 우리나라는 아직 완성된 형태의 입법을 마련하고 있지 못하다. 현재 가이드라인의 마련을 위한 준비 작업[47]이 진행되고 있는 단

---

46) 예를 들어 온라인 쇼핑몰이 취합하는 '구매상품의 내역'에 관한 정보의 경우, '구매상품의 내역'이라는 그 자체는 신상정보와 연결되지 않는 한, 사용자 특정과는 무관한 정보일 경우가 대부분이다. 한편, 쇼핑몰의 입장에서는 이러한 정보를 취합하는 것이 당연한 일이기도 하다. 서비스이용에 대한 과금의 결정, 결제의 유무, 배송의 유무, 반품 가능성 등 영업활동을 위해 필수적인 사항이거나, 애프터서비스에 대한 대비, 쿠폰의 지급 등 그 정보의 취합이 쇼핑몰이 아니라 오히려 고객을 위해 이루어지는 경우가 대다수이기 때문이다.

47) 방송통신위원회가 가이드라인의 제정의사를 밝힌 바 있다. 이에 관한 기사는 "방통위, 연내 인터넷 맞춤형광고 가이드라인 만든다", 파이낸셜뉴스, 2009.10.13

계이므로, 규제의 필요성을 공감[48]하고 있는 수준이라고 해 두는 것이 적절하겠다. 외국의 상황도 크게 다르지 않다. 미국[49]을 비롯한 각국[50]의 경우에도 현재 입법을 위한 논의가 진행되고 있을 뿐 구체적인 입법을 보유하고 있는 나라를 찾아보기는 힘들다.

한편 인터넷 사업자의 입장에서는 자율규제의 방법으로 이에 대처하고 있다. ① 식별가능한 개인정보(Personally Identifiable Information, 이하 PII)[51]와 기타정보(Non-PII)를 분리하여 관리하고, ② 구체적인 분리방법(De-Identification)으로 익명화(Anonymization), 가명화(Pseudonymization) 등의 조치를 취하며, ③ 사용자 정보의 보관기관을 한정하는 등의 일련의

자, <http://www.fnnews.com/view?ra=Sent0701m_View&corp=fnnews&arcid=091012224015&cDateYear=2009&cDateMonth=10&cDateDay=13> 검색일: 2010.4.1. 한편 한국인터넷진흥원에서도 '인터넷 권리장전'의 제정을 추진하고 있으며, 이는 올 하반기에 의견수렴과정을 거쳐 공포될 예정이다. 이에 관한 상세는, 한국인터넷진흥원 인터넷정책단 법제분석팀, "인터넷 권리장전 제정 추진계획(안)", (한국인터넷진흥원, 2010) 참조.

48) 이와 관련한 기사로는 "2010년 정보보호 정책 이렇게 바뀐다", 디지털데일리, 2009.12.31자, <http://www.ddaily.co.kr/news/news_view.php?uid=57985> 검색일: 2010.4.1 참조.

49) 미국의 경우, 가칭 프라이버시 법안(Privacy Bill)의 통과 여부를 두고 프라이버시 관련 단체와 사업자 단체의 격렬한 설전이 오가고 있는 상황이다. 프라이버시 법안은 <http://www.reputationdefenderblog.com/wp-content/uploads/2010/05/Privacy_Draft_5-10.pdf> 검색일: 2010.4.1.에서 확인할 수 있으며, 이와 관련한 기사는 <http://www.nytimes.com/2010/05/05/business/media/05adco.html> 검색일: 2010.4.1.; <http://www.forbes.com/2010/05/04/privacy-web-advertising-technology-bill.html> 검색일: 2010.4.1.; <http://www.reputationdefenderblog.com/2010/05/04/internet-advertising-privacy-bill-draws-criticism-from-both-sides/> 검색일: 2010.4.1.등에서 확인할 수 있다.

50) 이에 대한 간략한 정보는, 한국인터넷진흥원 인터넷정책단 법제분석팀, 앞의 글, 5-11쪽 참조.

51) 개인식별이 가능한 정보란 ① 개인을 식별하거나, 개인을 식별할 수 있거나, 접촉하거나, 위치를 알아낼 수 있는 정보, ② 그러한 정보를 이용하여 개인의 식별정보나 또는 연락정보를 추출해 낼 수 있는 정보를 의미한다. 구체적으로는 이름, 주소, 전화번호, 팩스번호, 이메일 주소, 재무정보, 의료기록, 사회보장번호(우리의 경우 주민등록번호), 신용카드정보를 포함하나 이에 제한되지는 않는다: 양지연, 앞의 글, 8쪽.

조치들[52]과 함께, 시장참여 사업자들이 자율적 규제를 위한 가이드라인[53]을 마련하여 준수하고 있다. 특히 IAB(the Interactive Advertising Bureau)와 NAI(the Network Advertising Initiative)가 공동으로 준비한 자율규제 가이드라인(Self-Regulatory Principles for Online Behavioral Advertising)[54]은 인터넷 맞춤광고에 대한 법적 문제와 동시에 구체적인 기술적 내용[55]도 담고 있어 주목할 만하다.

1.1. KT측의 주장

KT는 토론문[56]을 통해 익명성의 보장,[57] 처리 및 저장의 강화된 보안 적용,[58] 최소한의 정보의 처리와 저장,[59] 정보조합을 통한 개인식별 불가능[60] 등을 주장하여 '사용자 특정 가능성'에 대한 우려를 일축했다. 개인

52) 이에 관한 상세는 양지연, 앞의 글, 8-11쪽.

53) 인터넷 맞춤광고에 대한 가이드라인의 제정은 2007년 미국 FTC(Federal Trade Commission)의 가이드라인에서부터 시작된다. 이에 관한 상세는 <http://en.wikipedia.org/wiki/FTC_Regulation_of_Behavioral_Advertising> 검색일: 2010.4.1; 양지연, 앞의 글, 11-13쪽에서 확인할 수 있다.

54) 이는 <http://www.iab.net/media/file/ven-principles-07-01-09.pdf> 검색일: 2010.4.1에서 다운로드 받을 수 있다.

55) 이는 <http://www.iab.net/media/file/CLEAR_Ad_Notice_Final_20100408.pdf> 검색일: 2010.4.1에서 다운로드 받을 수 있다.

56) 구태언, 앞의 글, 78쪽.

57) 구체적으로 ① 무작위 추출된 난수로 Profile 관리: 역추적 불가, ② 난수로 이용자 식별 불가: Browser만을 식별, ③ Profile로 인한 이용자 식별 가능성 배제 등을 근거로 밝혔다.

58) 구체적으로 ① 데이터는 처리 즉시 폐기, 일체의 기록이 남지 않음, ② 관리자 또한 운영에 필요한 한정된 시스템정보만 접근가능, ③ 정보는 인코딩되어 난수로도 Profile에 대한 접근 불가 등을 근거로 밝혔다.

59) 구체적으로 ① 80 Port의 HTTP 데이터 중에서도 Text 데이터만을 대상, ② 개인식별가능정보 및 Webmail 제거, ③ 광고 카테고리, 시간 및 난수만을 처리 등을 근거로 밝혔다.

60) 구체적으로 ① KT의 ISP 등 네트워크와 시스템은 별도로 독립적으로 운영됨, ② 내외부적인 무단접근에 대한 기술적/관리적 예방 및 탐지수단 존재, ③ 제3자에 의한 기술적 검증완료, ④ ISP 네트워크와 본 시스템간의 정보교류 불가능, ⑤ 공인 감독기관의 외부 감시 시스템 구축 추진 중 등을 근거로 밝혔다.

정보 보호와 내부보안 강화를 위한 강한 의지를 표명하는 동시에 훌륭한 기술적·시스템적 대책을 강구하고 있다는 주장으로 판단된다. 구체적으로는 무려 14개 항의 내용을 밝히고 있는데, 크게 ① 쿠키에 UID를 심을 때 24자리의 난수를 사용하여 익명성 보장을 꾀하고 있다는 점, ② Phorm이 제공하는 맞춤광고 시스템과 KT가 보관하는 고객의 신상정보가 완전히 분리되어 조합이 불가능하다는 점, ③ 정보의 수집시 개인식별 가능정보나 웹메일 등의 민감한 정보는 제거한다는 점 등으로 구분해 볼 수 있겠다.

1.2. 구체적인 검토

1.2.1. 24자리 난수에 대하여

익명화를 위해 24자리 난수를 사용한다는 점은, 별다른 익명화 정책이 없는 국내의 많은 업체들에 비해 바람직한 정책임은 분명하다. 특히 쿠키 속의 ID를 익명화한다는 점에서 'AOL(America Online, Inc.) 검색어 노출사건'[61]과 같은 쿠키정보의 오용으로 인한 부작용을 방지할 수 있다는 장점이 있다고 평가할 수 있겠다. 그러나 이러한 난수처리가 곧바로 완전무결한 익명화를 담보하는 것은 아니다. 난수방식은 가장 보편적인 익명화 방식중의 하나이고,[62] 난수방식 말고도 다양한 익명화 방식이 존재한다.[63] 각 방식은 모두 장단이 있을 뿐 무결성이 입증된 그 어떤 방식은

---

61) 쿠키ID와 Non-PII정보가 결합되어 65만명의 사용자가 3개월간 식별당한 사건을 말한다. 이에 관한 기사는 "AOL's Big Privacy Blunder", 오마이뉴스, 2006. 8.7자, <http://english.ohmynews.com/articleview/article_view.asp?article_class=4&no=309830&rel_no=1>, 검색일: 2010.4.1; TechCrunch, "AOL Proudly Releases Massive Amounts of Private Data", 2006.8.6자, <http://techcrunch.com/2006/08/06/aol-proudly-releases-massive-amounts-of-user-search-data/>, 검색일: 2010.4.1 등 참조.

62) 예를 들어, 'AOL 검색어 노출사건'의 장본인인 AOL의 경우에도 그 사건당시 이미 사용자의 이름과 ID, IP주소 등을 난수처리(random ID Number)하여 익명화하고 있었다. 당해 사건은 쿠키ID의 익명화를 실시하지 않아 비롯된 사건이다.

63) 국제적으로 지명도 있는 인터넷 관련업체들은 모두들 고유한 익명화방식을 선

현재까지 존재하지 않는다고 보아야 한다. 또한 24비트(즉 24자리)라는 것도 그리 대단한 것만은 아니다. 흔히 온라인에서 사용하는 암호화기술(Secure Socket Layer, SSL)의 경우, 64비트·128비트·256비트 등 필요한 암호화수준에 따라 다양한 형태가 존재하며, 설사 미국정부가 최고급 보안데이터에 사용한다는 AES(Advanced Encryption Standard) 256비트라 할지라도 천재적 해커들의 공략 앞에서 완전한 '무결성'을 장담할 수는 없는 것이다.

따라서 Phorm의 24자리 난수정책은 국제동향을 따라가고 있다는 정도의 의미는 있으나, 이를 곧 완전한 익명화를 담보하는 '만병통치약'으로 바라볼 수는 없다.

1.2.2. PII와의 분리보관에 대하여

흔히 로그인정보로 통칭되는 PII, 즉 KT가 보관하는 식별가능한 개인정보와 DPI형 맞춤광고 시스템에서 각 사용자를 특정하기 위해 부여하는 꼬리표(UID, 즉 24자리의 난수)를 분리보관한다는 것은 일단 바람직하다. 개인정보 보호의 차원에서도 그러하고, 시스템의 안정성 차원에서 그러한 정책을 취하는 쪽이 유리할 것이다.

그러나 KT가 밝힌, Phorm이 제공하는 맞춤광고 시스템과 KT가 보관하는 고객의 신상정보가 완전히 분리되어 조합이 불가능하다는 주장은 이상하다. 그 말 자체가 모순적이기 때문이다. 왜냐하면 인터넷 맞춤광고 비즈니스 모델이 결국에는 사용자에게 적합한 광고가 시연되는 것을 목적으로 하는 것인데, Phorm의 시스템이 수집한 정보가 KT가 보관하는 고객정보와 완전히 분리되어 진정 조합이 불가능하다면 그 사용자에게 어찌 맞춤광고를 시연할 수가 있는가? 시스템적으로 분리가 되고 말고를 떠나서, 최종적으로는 그 사용자를 특정할 수 있어야만[64] 그에게 광고를

택하고 있다. 이는 일종의 영업비밀에 속하므로 구체적으로 알아내기는 힘들지만, 개인정보 보호정책의 일환으로 추상적인 메커니즘과 방침 등이 공개되고 있는 상황이다. 예를 들어, 마이크로소프트사의 경우에는 '단방향 암호화 해시(one-way cryptographic hash)'라는 방식을 채택하고 있는 것으로 알려져 있다.

64) 사용자의 컴퓨터에 준비된 광고를 송출하기 위해서는 송부주소를 알아야 하므

할 수 있다.[65] 결국 KT의 이러한 주장은 'DPI시스템을 관리하는 KT의 직원과 쿡 인터넷 서비스의 가입자 리스트를 관리하는 KT직원이 친하지 않아 정보를 공유하지 않는다'라는 수준의 주장으로 받아들여져야 한다.

1.2.3. 내부적 오용가능성에 대하여

지금까지 수없이 경험한 각종의 '개인정보 유출사건'에서 가장 빈번한 사례로 등장하는 '특정직원의 내부적 오용가능성'은 어떠한가? 즉 KT의 두 직원이 친하지 않다는 점을 인정한다고 가정할 때, DPI시스템을 관리하는 직원 스스로가 DPI시스템을 사용하여 오용할 가능성은 없는가 하는 점이다.

KT의 주장에 의하면 ① 데이터는 처리 즉시 폐기, 일체의 기록이 남지 않음, ② 관리자 또한 운영에 필요한 한정된 시스템정보만 접근가능, ③ 정보의 인코딩으로 난수로도 Profile에 대해 접근 불가함 등을 근거로 오용 가능성을 일축했다. 그러나 이러한 시스템적 보안구조는 어디까지나 기술적 차원에서의 논의일 뿐, 이를 근거로 오용가능성이 없다고 단정할 수는 없다. 왜냐하면, 이러한 시스템적 보안구조에도 불구하고 이에 접근할 수 있는 관리자(admin)는 통상 해당 시스템에 관한 전능한 권한[66]을 가지게 되기 때문에 얼마든지 조작[67]이 가능하다.[68]

로 최소한 사용자의 IP주소는 반드시 알아야 하고, 그렇다면 내부적 분리정책에도 불구하고 사용자의 특정가능성은 엄연히 존재하는 것이다.

65) 만약 절대적으로 조합이 불가능한 채로 Phorm의 시스템이 수집한 정보가 활용될 수 있는 경우라면, 'KT의 쿡서비스에 가입한 회원들이 취하는 인터넷 활동의 행태연구를 위한 통계' 정도밖에 없을 것이다.

66) 세상에 존재하는 어떠한 시스템도 완전무결한 것은 없기 때문에 고장이나 사고 등에 대비해야 하고, 이를 위해 시스템 관리자는 시스템의 전반에 대하여 모든 형태의 작업을 할 수 있는 전능한 권한이 부여된다.

67) 예를 들어 '즉시 폐기한다'는 보안규칙을 '1주일 동안 존속시키다가 폐기한다'로 변경하여 데이터의 존속기간을 늘인다든지, '인코딩'된 데이터를 '디코딩'시킨다든지 하는 일은 얼마든지 가능하다.

68) 우리가 경험한 많은 정보유출 사건의 경우에도, '시스템 보안구조'상의 문제보다는 시스템에 접근가능한 '사람의 문제'일 경우가 대부분이었다는 점을 상기한다면 이해가 쉬울 것이다.

또한 Phorm의 시스템이 DPI기술을 사용한다는 점에서 그 오용의 가능성은 더욱 증가한다. 즉 인터넷을 오가는 모든 정보(즉 데이터 패킷)들은 모두 IP주소라는 목적지의 주소를 담고 있다. 한편, DPI라는 기술은 그 패킷들을 중간에 가로채서 열어보는 기술이므로, DPI를 실시한다는 것 자체가 IP주소를 지득하게 된다는 것을 의미한다. 따라서 DPI시스템을 담당하는 관리자가 가장 손쉽게 접할 수 있는 정보가 아마도 IP주소가 될 것이다. 그렇다면 DPI시스템을 담당하는 KT의 그 직원은 굳이 쿡 인터넷 서비스의 가입자 리스트를 관리하는 직원의 협조를 구하지 않고, 스스로도 얼마든지 사용자를 특정해낼 수 있다.[69] 주지하다시피 인터넷상에서 특정성이 가장 높은 것이 IP주소가 아닌가? 그렇다면, 굳이 두 직원이 친하지 않아도 오용이 가능한 것이다.

1.2.4. 민감한 정보의 제거에 대하여

정보의 수집시 PII나 웹메일 등의 민감한 정보가 제거된다는 것은, DPI를 실시하여 수많은 데이터 패킷을 무차별적·전방위적으로 수집하는 단계에서 불필요하거나 수집하기가 부담스러운 정보를 선별한다는 의미이다. Phorm에서 밝힌 바[70]를 기초로 간단히 예를 들어보면, 수집된 데이터들의 내용 가운데서 'and/but/the/or/a' 등의 불필요한 내용, 또는 흔히 이메일 주소에 포함되는 '@'이 포함된 단어, 성명을 추측할 수 있는 'Mr'나 'Mrs'라는 단어 뒤에 오는 내용, 그리고 우편번호 등 수집하기가 부담스러운 정보는 폐기된다는 것이다.

우리는 이미 이러한 필터링 방식의 선별작업에 익숙해져 있다. 각종의 게시판에서 음란하거나 욕설을 담은 문서의 작성을 방지하기 위해,[71] 또

---

69) 이러한 견해는 토론회 당시 발제자로 참여했던 임종인 교수도 "내부적으로 특정IP에 대한 난수값 추적가능→IP와 성향정보 결합에 따른 오용가능성"이라고 하여, 그 우려를 명시적으로 밝힌 바 있다. 이는 임종인, 앞의 글, 41쪽에서 확인할 수 있다.

70) Clayton, 앞의 글, 6-7쪽.

71) 게시판 관리자가 '게시판 설정'의 단계에서, 문제발생이 예상되는 단어나 문장들을 나열·조합하게 된다.

는 인터넷 스토리지 사이트에서 최신영화의 불법적인 다운로드를 방지하기 위해[72] 작성금지 문구가 설정되어 있는 상황을 쉽게 접할 수 있기 때문이다. 따라서 이러한 주먹구구식 대응이 얼마나 비효율적인지를 너무나 잘 알고 있기도 하다.[73] 인터넷상에서 진행된 필터링의 역사가 꽤나 오래되었음에도 불구하고, 지금도 여전히 욕설이 난무하고 최신영화는 다운로드 되고 있기 때문이다.

또한 이러한 필터링에 있어 가장 큰 문제는 설정이 자의적이라는 것이다. 예를 들어, DPI 관리자가 오용을 위해 '@'라는 문자를 필터링 대상에서 제외하면 그만인 것이다. 이에 더하여 DPI방식의 고유한 위험성을 언급할 수 있다. 무차별적으로 DPI한 데이터들을 필터링을 하기 위해서는, 일단 폐기할 정보와 폐기하지 않을 정보를 구별하지 않고 수집한 다음 모두 읽어 보아야만 비로소 선별을 할 수 있다. 폐기의 이전에는 일시적이나마 폐기대상 정보가 저장되고, 이 또한 일단 읽어 들여진다는 점이 여전히 미결의 문제로 남는다.

1.3. 소결

지금까지 살펴본 바를 종합해 보면, Phorm이 강조하는 개인정보 보호 및 익명화 기술이 크게 우수할 것도 없다는 결론을 내릴 수 있다. 페이지마다 등장하는 '24자리 난수'는 그냥 국제적 수준을 따라가는 정도이고, 사용자의 특정 가능성은 엄연히 존재하고, 내부적 오용 가능성은 DPI 기술의 특성상 1·2세대 인터넷 맞춤광고의 경우보다 더 높고, 민감정보에 대한 필터링 방식도 주목할 만한 것이 못된다.

이러한 검토를 고려해 보면, 당사자가 전혀 특정되지 않는 Phorm의 선진적인 기술에 의해 통신비밀보호법상의 감청에 해당하지 않는다는 KT의 주장이 얼마나 터무니없는 것인지 잘 알 수 있다. KT측의 토론문에

---

72) 해당 스토리지의 관리자가 최신 영화의 제목이나 주연배우의 이름 등을 지정하여 검색이 불가능하도록 설정한다.

73) 물론 수준의 차이가 있겠으나, 이러한 필터링방식으로 진행되는 선별로는 무결성을 단정하기가 곤란하다는 점은 동일하다.

의하면, ① 통신의 자유란 통신의 비밀에 대한 보호인데, 개인이 특정되지 않으면 '비밀성'이 보장되므로 통신의 자유가 보호되고, ② 감청의 대상은 특정 '당사자'간의 통신인데, 익명화와 역추적 불가 등으로 당사자 특정 가능성이 배제되어 감청에 해당하지 않는다고 한다. 또한 감청은 통신내용의 지득 또는 채록이 요건인데 ③ 통신내용이 전혀 저장됨이 없이 광고 카테고리와 매칭시간, 그리고 난수만 남게 되어 통신내용을 알 수 없고, ④ 채록은 채집하여 기록하는 것인데, 이용자의 통신내용이 전혀 기록·저장되지 않으며, ⑤ 시스템적으로 통신내용은 제거되도록 구현되어 있어 지득·채록의 고의 또한 부재하여 감청에 해당하지 않는다고 주장하고 있다.[74]

통신비밀보호법상의 감청에 관하여 이러한 논리구성을 시도한다는 것 자체에 동의할 수 없으나, 굳이 이에 대하여 응하자면 다음과 같이 말하고 싶다.

> Phorm의 노력에도 불구하고 사용자의 특정가능성이 엄연히 존재하므로 ①과 ②는 의미가 없고, DPI기술 자체가 패킷의 내용을 열람하는 것이므로 지득에 해당되어 ③도 의미가 없으며, ④와 ⑤의 경우에는 내부자의 자의적 설정이나 오용에 의해 얼마든지 조작 가능한 사항이라 받아들여질 수 없다. KT의 근거가 다 사라졌는데, 그렇다면 스스로 감청에 해당함을 인정하는 것인가?

2. 동의를 통한 면책 가능성

DPI의 규제와 관련하여 가장 뜨거운 이슈는 바로 '동의'이다. 상업화된 DPI기술이 처음 등장한 미국의 경우, DPI에 대한 폐해를 잘 알면서도 '사용자의 동의(Consent)'가 있는 한 전자통신비밀보호법(Electronic Communications Privacy Act of 1986, ECPA) 위반으로 다스릴 수 없었기 때문이다.[75] 이에 현재 미국정부가 입법을 준비하고 있음은 이미 지난

---

74) 구태언, 앞의 글, 79쪽.

75) 18 U.S.C. § 2511(2)(a)(i); § 2511(2)(c); § 2511(2)(d).

논문에서도 밝힌 바가 있다.[76]

한편, 인터넷 맞춤광고에 있어서도 동의의 문제는 뜨겁다. 옵트인(Opt in)[77]이냐 옵트아웃(Opt out)[78]이냐를 두고 프라이버시 관련 단체와 사업자 단체 간에 끊임없는 줄다리기를 해오고 있기 때문이다. 아직까지 그 결판은 나지 않은 것으로 보인다. 사업자단체의 자율규제인 IAB/NAI의 가이드라인에서는 "동의가 필요하다"고만 정하고 있을 뿐 구체적으로 그것이 '옵트인'인지 '옵트아웃'인지는 밝히지 않고 있다.[79] 이런 상황에서 실제 사업의 운영은 '옵트아웃'으로 진행되고 있기 때문에, 프라이버시 관련 단체는 그 비판을 지속하고 있다. 가칭 프라이버시 법안(Privacy Bill) 또한 사정이 다르지 않다. '옵트인'을 요구하는 동시에 '옵트아웃'도 허용하고 있으므로 그 결과에 있어서는 별 차이가 없다.[80]

Phorm의 경우에도, 다른 사업자와 마찬가지로 '옵트아웃' 정책으로 시스템이 운용된다고 밝힌 바 있다.[81]

2.1. KT측의 주장

KT측은 토론문을 통해 '사용자의 동의'가 있기 때문에 우려되는 각종의 법적 문제를 일괄로 해결할 수 있다는 입장을 보이고 있다. 불투명한 표현으로 파악하기가 난삽한 부분이 많으나, KT가 구성한 논점을 그대로

---

76) 오길영, 앞의 글, 416-417쪽. 이에 관하여는 <http://www.pcworld.com/article/163740/us_lawmakers_target_deep_packet_inspection_in_privacy_bill.html>, 검색일: 2010.4.1.; <http://comlaw.wordpress.com/2009/04/24/nyt-online-privacy-bill-on-deep-packet-inspection-dpi/>, 검색일: 2010.4.1. 등 참조; 입법의 진행상황을 파악하기 위해 지난 논문이 탈고된 이후 지속적으로 관찰해오고 있으나, 아직까지 입법이 되었다는 소식을 접하지는 못하였다.

77) 서비스를 받겠다고 미리 동의한 사람에게만 서비스를 시행하는 방식.

78) 일단 서비스를 전반적으로 시행하고 이를 거부하는 사람은 제외하는 방식.

79) IAB/NAI, "Self-Regulatory Principles for Online Behavioral Advertising", (AAA/ANA/BBB/DMA/IAB, 2009), 14쪽, Ⅲ. Consumer Control 이하 참조.

80) 주 49의 법안, 8쪽, Section. 3. Notice and Consent Requirements for the Collection, Use, and Disclosure of Covered Information 이하 참조.

81) Richard Clayton, 앞의 글, 2쪽.

사용하여 이를 정리해 보면 다음과 같다.

2.1.1. 감청 여부와 관련한 KT의 주장

감청 여부와 관련하여 KT는 ① 감청의 해당 여부는 형식에 구애되지 아니하고 실질적인 동의 여부, 즉 프라이버시에 대한 실질적인 통제권을 행사했는지 여부에 따라 판단되어야 하고, ② 통신비밀보호법상에는 동의의 방식에 대한 규정이 없으므로 '묵시적인 동의'도 가능하며, 따라서 ③ 통신비밀보호법상의 동의 여부의 판단기준은 프라이버시에 대한 통제권 여부에 따라 판단하게 되는데 이용자의 상황에 대한 인식과 더불어 통제권의 행사 가능성이 고려되어야 하고, KT의 맞춤광고는 ④ 서비스의 내용과 탈퇴방식을 명시적으로 고지하게 되므로 이를 통한 이용자의 상황에 대한 인식과 통제권이 행사 가능하므로 감청에 해당하지 않는다고 한다.[82]

도대체 무슨 말을 하고 있는 것인지 명확하게 파악하기 곤란하나, 통신비밀보호법의 내용을 이렇듯 어처구니없는 방식으로도 해석할 수 있다는 전제 아래서 KT측의 논리를 요약해 보면, (i) 통신비밀보호법상에 동의에 관한 규정이 없으므로 묵시적 동의도 허용되는데, (ii) 옵트아웃으로 서비스 이용자의 상황인식과 통제권이 부여되니 묵시적 동의를 얻은 것으로 되고, (iii) 따라서 KT의 서비스는 감청에 해당하지 않는다고 하는 주장으로 정리해 볼 수 있겠다.

2.1.2. 감청의 동의요건에 관한 KT의 주장

KT는 토론회 당시 제공한 보충자료를 통해 통신비밀보호법상의 감청에서 필요한 '동의의 요건'에 관하여 구체적으로 언급한 바 있다. 이는 또 다른 토론자로 참석하였던 장여경이 그 토론문[83]에서 자발적으로 동의한 감청과 관련하여 제3자가 전화통화자 중의 일방만의 동의를 얻어

82) 구태언, 앞의 글, 80쪽.

83) 장여경, "패킷감청과 통신의 비밀", 패킷감청의 문제점과 개선방안에 대한 토론회 자료집(2010), 72쪽.

통화내용을 녹음한 경우 통신비밀보호법에 위반한다고 설시한 판례[84]를 인용하면서 이러한 대법원의 입장에 의하면 KT의 경우 양 당사자(통신의 송신자와 수신자)의 동의를 얻어야만 한다고 주장했기 때문에 비롯되었다.

이러한 주장에 대하여 KT측은 "당사자 일방이 전화통화 내용을 녹음하는 것이 불법감청에 해당하지 아니한다고 한다면, 그러한 당사자는 언제나 대화의 내용을 녹음하여 이를 제3자에게 제공할 수 있고, 이는 제3자가 대화의 당사자 중 일방의 동의를 얻어 대화를 녹음하는 것과 질적으로 다를 것이 전혀 없어 논리적 일관성이 없다"고 하면서 해당 판례가 학계[85]의 비판을 받고 있음을 지적하였다.[86]

요컨대 제3자(즉 KT)가 일방당사자(쿡 스마트웹의 이용자)의 동의를 얻어 녹음한 행위(즉 KT가 웹-페이지를 DPI하는 행위)를 일방당사자에 의한 녹음행위(인터넷 사용자 스스로 정보수집을 하는 경우)와 달리 보아야 할 타당한 근거가 없으므로, 판례의 입장에 동의할 수 없다는 것이다.

2.1.3. 기타 동의와 관련한 KT의 주장

'동의의 요건' 문제의 연장선상에서 KT는, ① 가사 양 당사자의 동의가 필요하다고 가정하더라도 http로 접근할 수 있는 웹사이트는 공개된 웹사이트라고 주장하고 있다.[87] ② 이러한 웹사이트는 일반 공중에 대하여 당해 웹사이트 및 그 내용의 접근을 허용하고 있는 공적인 영역의 서비스이므로 사생활의 영역과는 구분되고, ③ 다만 'https,[88] 이메일, 메신저 등 비공개 정보는 제거'하므로 명시적인 비공개 자료를 제외하고 있

84) 대법원 2002.10.8. 선고, 2002도123 판결.

85) KT측이 학계의 비판으로 들고 있는 논문은 하태훈, "통화자일방의 동의를 받은 제3자의 전화녹음과 통신비밀보호법 위반: 대법원 2002.10.8. 선고, 2002도123 판결", 안암법학 제17호(안암법학회, 2003)이다.

86) 구태언, "보충자료", 패킷감청의 문제점과 개선방안에 대한 토론회 자료집(2010), 2쪽.

87) 구태언, 앞의 "보충자료", 2쪽.

88) https는 보안목적으로 암호화된 웹-페이지를 말한다.

음을 밝히고 있다.

한편, KT는 쿠키의 변조행위에 대한 동의에 관하여는 구체적인 설명을 하지 않고 있다. 다만 앞서 살펴본 그림 2의 설명 2에서 보듯, “24자리의 난수를 쿠키에 담아 ‘동의’한 고객의 PC로 전송”이라는 간략한 설명만을 붙이고 있을 뿐이다.

2.1.4. 주장의 정리

지금까지 살펴본 바와 같이 KT가 구성한 논점과 그 논점에 대해 KT가 주장한 내용이 전혀 일치하지 않는다. 글을 쓰는 지금에 와서 KT의 정확한 입장을 알 방도가 없으나, 타당성의 검토를 위해 필자의 시각에서 그 논리의 진행을 임의로 재구성해 보기로 한다.

먼저 2.1.2.에서 언급하고 있는 감청의 동의요건에 대한 KT의 입장에서 시작하는 것이 좋겠다. 살핀 바와 같이, ① KT는 제3자의 녹음행위시의 동의와 관련하여, 통신당사자 쌍방의 동의가 필요하다는 입장인 토론자 장여경을 반박하는 것으로 미루어 볼 때 통신당사자 일방의 동의만 있으면 족하다는 입장을 취하고 있는 것으로 생각된다. 즉 일방당사자인 사용자의 동의만 있으면 DPI가 불법이 아니라는 것이다.

그렇다면 일방당사자인 사용자의 동의가 있어야 하는데, 2.1.1.에서 밝힌 바에 의하면 ② 통신비밀보호법은 구체적인 동의의 방식을 법정하고 있지 않아 묵시적 동의방식도 문제없다는 입장이다. 따라서 묵시적 동의의 하나인 KT의 ‘옵트아웃’으로 사용자측의 동의는 해결된다는 것이다.

다음으로 상대방인 웹-페이지측의 동의에 대하여는 2.1.3.에서 살핀바와 같이 ③ 일단 KT는 일방의 동의만이 필요하다는 입장이므로 사용자측의 동의만 있으면 문제될 것이 없으나 ④ 설사 쌍방의 동의가 필요하다 할지라도 http로 접근할 수 있는 사이트는 공개되어 있는 것이므로 그 성질상 동의를 얻은 것과 마찬가지라는 입장이다.

마지막으로 2.1.3.에서 보듯 ⑤ 쿠키의 변조에 대한 사용자의 동의에 대하여는 함구하고 있다.

2.2. 구체적인 검토

2.2.1. 동의의 요건에 관하여

먼저 통신비밀보호법의 규정을 확인해 보기로 하자. 통신비밀보호법은 제2조 제7호의 정의규정에서 "'감청'이라 함은 전기통신에 대하여 당사자의 동의없이 전자장치·기계장치등을 사용하여 통신의 음향·문언·부호·영상을 청취·공독하여 그 내용을 지득 또는 채록하거나 전기통신의 송·수신을 방해하는 것을 말한다"고 규정하고 있다. 즉 감청은 '전기통신'에 있어 당사자의 동의가 없는 경우가 요건이 된다. 여기서 두 가지의 질문이 발생한다. '감청은 전기통신만 해당하는가, 대화는 상관이 없는가' 하는 점과 '당사자의 동의란 구체적으로 일방당사자의 동의인가 쌍방당사자의 동의인가' 하는 점이다.

한편, 제3조 제1항에서는 "누구든지 이 법과 형사소송법 또는 군사법원법의 규정에 의하지 아니하고는 우편물의 검열·전기통신의 감청 또는 통신사실확인자료의 제공을 하거나 공개되지 아니한 타인간의 대화를 녹음 또는 청취하지 못한다"고 규정하고 있다. '전기통신의 감청'과 '타인간의 대화'를 분리하여 규정하고 있는 것으로 볼 때 입법자는 이를 구분하여 다루고 있는 것이다. 즉 타인간의 대화의 경우 '녹음이나 청취'를 금지하고 있다. 바로 이 점을 앞의 두 물음에 비추어 보면, 적어도 하나의 질문은 해결이 된다. 통신비밀보호법이 상정하는 감청은 '음향[89]·문언·부호·영상' 등을 송수신하는 '전기통신 뿐'이고, 대화의 녹음행위는 감청에는 해당하지 않으나 금지된다는 것이다. 그렇다면 남은 하나의 질문, 즉 감청에 있어 '당사자의 동의란 구체적으로 무엇인가'하는 물음에 대해 이를 일방당사자의 동의로 파악하는 '일방동의설'과 쌍방당사자의 동의가 필요하다는 '쌍방동의설'이 존재한다.[90]

---

89) 사람의 소리, 즉 말을 음향이라 표현할 수 있는가 하는 애매함이 남는다. 몇 개의 국어사전을 통해 검토해 본 결과, 음향은 "물체에서 나는 소리와 그 울림"이라고 정의하고 있다. 또한 사람간의 '대화'는 따로 규정되어 있으므로, 여기서의 음향에는 사람이 말을 하는 소리는 포함되지 않는다고 해석하는 것이 타당하다.

90) 하태훈, 앞의 글, 86-87쪽.

여기까지의 간략한 검토를 바탕으로, KT의 주장으로 돌아와 보자. 일단 KT가 인터넷 맞춤광고용으로 수집하는 정보가 사람의 소리, 즉 '대화'일 가능성은 거의 없다.[91] 상정되는 수집의 대상이 사용자가 브라우저를 사용해 접속하는 웹-페이지이기 때문이다.[92] 따라서 대상규정은 동법 제2조 제7호이고, 동법 제3조 제1항이 법정하고 있는 '타인간의 대화'는 아예 논의의 대상이 아니다. 그럼에도 불구하고 장여경과 KT는 제3자가 '대화'를 녹음한 판례를 대상으로 논박을 벌이고 있다. 즉 KT는 규정해석의 오류로 인하여 엉뚱한 판례를 대상으로 엉뚱한 주장을 하고 있는 것이다.[93]

2.2.2. 사용자측의 동의에 관하여

다음으로 KT가 주장하는 사용자측의 '묵시적 동의'에 대하여 살펴보자. 살핀 바와 같이 통신비밀보호법 제2조 제7호는 '동의'라고 할 뿐 그 동의가 명시적인지 묵시적인지는 언급하고 있지 않다. 그렇다고 이를 일방당사자의 '묵시적 동의가 있으면 가능하다'는 자의적 주장은 도대체 어떠한 근거에서 비롯된 것인지 궁금하지 않을 수 없다. 통신비밀보호법상

91) 굳이 가능성을 말하자면, 인터넷 전화나 실시간 음성채팅 정도가 해당될 것이다. 그렇다면 이렇듯 패킷화된 사람의 '대화 데이터'를 DPI하는 경우는 어떠한가? 이를 전기통신으로 보아 감청으로 파악한다면, 사용자의 '명시적 동의'가 있는 경우에 한하여 각 학설(일방동의설과 쌍방동의설)의 입장이 중요하게 작용할 것이다. 그러나 종래의 판례의 기준에 따를 때, 이를 '대화'로 파악한다면 일방당사자의 명시적 동의가 있다고 하여도 통신비밀보호법 위반에 해당하게 될 것이다.

92) Phorm의 기술에 대해 설명한 각종의 보고서를 살펴보아도, 정보수집의 대상은 주로 웹-페이지에 한정된다.

93) 지면관계상 이에 관하여 구체적으로 검토할 여유가 없으나, 필자는 쌍방동의설을 지지하는 바이다. 그러나 이렇듯 범죄구성의 중요부분이 학설에 맞겨져 있다는 것 자체에 동의할 수 없다. 명쾌히 규정하여 입법으로 해결하는 것이 바람직할 것이다. 이러한 점은 KT가 일방동의설의 주장 근거로 밝히고 있는 하태훈 교수의 입장에서도 동일하다. 정확히 말하자면 하태훈 교수 또한 일방동의설을 취하여 문제해결을 도모하고 있는 것이 아니라, 학설에 의할 경우의 모순점을 지적하면서 결국 입법적 보완이 필요함을 강조하고 있기 때문에, KT가 당해 논문을 일방동의설의 근거로 삼는 것도 적절하지 못하다.

의 감청은 헌법 제18조가 명정하고 있는 국민의 기본권에 대한 제한이다. 이러한 제한이 헌법 제37조 제2항에 의해야 함은 두말할 나위도 없거니와, 바로 이러한 이유 때문에 통신비밀보호법은 감청에 있어 영장주의[94]를 채택하고 있다. 만약 KT의 주장대로 일방당사자의 '묵시적 동의'가 가능하다면, 사기업의 영리라는 사익이 아니라 '국가안보'나 '수사목적'이라는 공익이 있는 상황에서조차 굳이 영장(감청허가서)을 요구할 이유가 있을까? 수사기관이 전국민을 상대로 동의를 구하는 옵트아웃 방식의 이메일을 한번 보내놓고, 동의 거부의 답신 메일을 보내지 않은 국민에 대해서는 묵시적 동의가 있었다고 주장하면 그만일 것이기 때문이다. 따라서 KT는 헌법과 통신비밀보호법의 원리에 대해 심대한 오해가 있다고 판단되며, '묵시적' 동의는 인정될 수 없음을 '명시적'으로 밝힌다.

한편, 쿠키의 납치와 변조[95]행위에 있어 사용자의 동의에 대하여 살펴보자. DPI의 실시여부와 무관하게 쿠키를 납치하는 행위 그 자체만을 두고 볼 때, 이에 대한 법적 평가는 무엇이라 할 수 있는가? 묵시적 동의가 인정되지 않는 한, 통신비밀보호법 제2조 제7호상의 '감청'에 해당한다. 왜냐하면 법문은 "전기통신에 대하여 당사자의 동의 없이 전자장치·기계장치등을 사용하여 …… 전기통신의 송·수신을 방해하는 것을 말한다"고 규정하여, '전기통신의 송·수신을 방해하는 것'도 감청에 포함되기 때문이다. 사용자의 입장에서는 접속에 지장이 없으므로 '방해'라고 할 만한 것이 없었다고 주장해 볼 수 있겠다. 그러나 '유인'하였으므로 브라우저를 통해 무언가를 하고자 하는 사용자의 의사(납치없이 바로 접속하고자 하는) 실현을 방해하였고, 일시적으로나마 Phorm의 서버에 머물러 있게 되므로 물리적인 시간의 정체 또한 있었다. 따라서 KT가 쿡 스마트 웹을 실시하기 위해서는 꼬리표를 달 때마다 법원의 감청허가서가 필요

94) 엄밀하게 말하자면, 영장주의에 의한다고 단언하기는 곤란하다. 법문상의 표현이 법관이 아니라 '법원'에 의한, 영장이 아니라 '감청허가서'에 의하도록 되어 있기 때문이다. 그러나 이러한 표현상의 차이에도 불구하고 영장주의에 의해야 한다는 점은 학계나 실무계에 있어 공통된 견해이라는 점을 단언할 수는 있다.

95) 여기서의 변조는 권한 없는 자가 문서의 내용을 변경하였다는 의미에서 사용되었고, 형법 제231조의 '사문서의 변조죄'를 의미하는 것은 아니다.

하겠다.[96]

그렇다면 감청허가서의 문제를 고려하지 않는다면 가능한 일인가? 그렇지 않다. 우리의 '정보통신망 이용촉진 및 정보보호 등에 관한 법률' 제49조의2 제1항이 "누구든지 정보통신망을 통하여 속이는 행위로 다른 사람의 정보를 수집하거나 다른 사람이 정보를 제공하도록 유인하여서는 아니 된다"고 규정하고 있기 때문이다. Phorm의 서버가 2회에 걸쳐 '허위의 재발송 요청신호'를 보내게 되므로 이는 전형적인 '속이는 행위'에 해당하고, 사용자의 개인정보를 가득 담고 있는 쿠키를 납치하여 Phorm의 서버로 불러들이므로 '다른 사람(인터넷 사용자)의 정보를 수집'하는 행위에 해당한다. 또한 이러한 납치·변조 행각이 '다른 사람(인터넷 사용자)이 정보를 제공하도록 유인'하는 행위에 속함은 자명하다. 결국 Phorm의 시스템은 적어도 대한민국내에서는 가동될 수 없는 것이다.

2.2.3. 웹-페이지측의 동의에 관하여

웹-페이지측의 동의에 관하여 KT는, 'http'로 접속가능한 웹사이트는 공적인 영역의 서비스이므로 일반 공중에 대하여 해당 웹사이트 및 그 내용의 접근을 허용하고 있기 때문에 DPI를 통한 Phorm의 무단수집이 문제되지 않는다는 입장이다. 즉 공개된 사이트이므로 수집이나 이용에 있어 동의가 필요 없다는 것이다. 이러한 주장에 관하여 살펴보자.

먼저 우리 저작권법은 제10조 제2항에서 "저작권은 저작물을 창작한 때부터 발생하며 어떠한 절차나 형식의 이행을 필요로 하지 아니한다"고 밝히고 있다. 따라서 일단 저작이 완성되기만 하면, 저작자는 동일성유지권(동법 제13조)과 같은 저작인격권과 배포권(동법 제20조)·복제권(동법 제16조)과 같은 저작재산권을 가지게 된다(동법 제10조 제1항).

한편, 타인이 해당 저작물을 사용하기 위해서는 저작재산권자의 이용허락을 받아야 하는데(동법 제46조), 이 경우 허락받은 타인은 허락받은 이용방법과 조건의 범위 안에서만 그 저작물을 이용할 수 있다(동법 제

96) 이러한 경우는 통신비밀보호법상 감청허가서의 발부요건에 해당하지 않으므로, 감청허가서가 발부될 수 없음은 당연하다.

46조 제2항). 이러한 이용은 저작재산권자의 동의 없이는 양도가 불가능하다(동법 제36조 제3항). 만약 이러한 사항을 준수하지 않고 저작재산권을 복제나 배포하는 경우에는, 이는 저작권의 침해에 해당하여 5년 이하의 징역 또는 5천만원 이하의 벌금에 처하거나 두 처벌을 동시에 받게 된다(동법 제136조 제1항).

혹여 공개된 인터넷 사이트는 아날로그 저작물이 아닌 디지털 웹-문서이므로 해당사항이 없다고 주장할지도 모르겠다. 그래서 '네이버'에 접속해 보았다. 네이버는 '이용약관'[97] 제17조 제1항에서 '권리의 귀속'에 관하여, "'서비스'에 대한 저작권 및 지적재산권은 '회사'에 귀속됩니다. 단, '회원'의 '게시물' 및 … 등은 제외합니다" 하고 규정하고 있다. 네이버가 작성하거나 운영하는 서비스는 네이버에 귀속하고, 회원이 작성한 게시물은 예외라고 밝히고 있다. 회원이 작성한 게시물에 대하여는 동약관 제15조에서 따로 정하고 있는데, "회원이 '서비스' 내에 게시한 '게시물'의 저작권은 해당 게시물의 저작자에게 귀속됩니다" 하고 정하고 있어 회원이 작성한 게시물의 저작자는 회원 자신임을 밝히고 있다. 결국 네이버가 운영하는 서비스내에서는 주인없는 웹사이트가 존재하지 않는 것이다. 이런 상황은 다른 포털업체도 마찬가지이며, 외국이라고 다르지 않다.

따라서 KT의 주장과는 달리 자유로이 접속이 용이한 소위 공개된 'http' 사이트라고 하더라도, 모든 웹사이트에는 저작자와 저작권이 존재하므로 저작권법 제46조의 '이용허락'이 필요하고 동조 제2항에 의해 '이용방법과 조건의 범위 안에서만' 접근이 가능하겠다.

여기서 '이용허락'에 관하여 살피면, 변조된 쿠키로 (웹-페이지 내용의) 송출요청[98]을 받은 웹-페이지가 '이용허락'[99]을 한 당사자는 Phorm이 아닌 브라우저의 사용자이다. 쿠키가 변조되긴 했으나 여전히 송출될 IP주

---

97) 이에 관한 상세는 <http://www.naver.com/rules/service.html#a17>, 검색일: 2010. 4.1.에서 확인할 수 있다.

98) 정확히 말하자면, 쿠키가 아니라 브라우저가 보낸 '접속요청 신호'의 패킷(SYN 1)이다.

99) 정확히 말하자면, 접속의 요청을 받아 그 접속을 허락하는 웹-페이지는 '접속받음 신호'의 패킷(FIT WAIT 1)을 보낸다.

소는 사용자의 컴퓨터의 주소를 가리키고 있을 것이기 때문이다.[100][101] 따라서 Phorm은 이용허락의 당사자가 아니므로 저작물에 접근할 권한이 없으며, 이를 복제하거나 배포할 권한도 없으므로 DPI와 OIX를 운용하는 것은 저작권침해에 해당한다.

나아가 '로그인'을 요구하는 회원제 서비스의 경우에는 더 큰 문제이다. 로그인 자체가 회원만의 접속을 허락하고 비회원의 접속을 제한하기 위함이라는 점을 고려해 볼 때, 비회원에게는 로그인 후 접속하게 되는 모든 사이트는 이용허락의 유무를 떠나 '공개'조차 되었다고 볼 수 없다. KT의 주장대로라면, 공개되지 않은 사이트는 DPI되지 말아야 한다. 공개된 사이트를 DPI하는 것이 무슨 문제이냐는 것이 KT의 논지였기 때문이다. 그런데 기실 DPI 장치는 공개와 비공개를 구분하지 않고 사용자를 향해 송출되는 모든 패킷들을 무차별적으로 DPI하게 된다. 따라서 사용자가 접속한 사이트가 회원제 서비스가 제공한 것이라 할지라도 달리 취급될 수가 없다. 결국 사용자가 접속하는 모든 사이트는 DPI에 희생되게 되므로, 공개 운운하던 KT의 주장 또한 이유 없다.

Ⅳ. 마치며

지금까지 KT와 Phorm이 시도하고 있는 인터넷 맞춤광고에 대하여, 기술적 측면과 법리적 측면으로 구분하여 검토해 보았다. 분량도 논문으로서는 다소 과하고 쟁점도 다양하고 많아, 결론이라 하여 이를 다시금 재

---

100) DPI 장치는 사용자를 향해 송출되는 웹-페이지의 패킷들을 가로채서, 복사본을 만든 후 꼬리표를 떼어낸 원본을 사용자에게 보낸다. 따라서 각 패킷들은 사용자를 향해 송출되도록 주소가 설정되어 있고, 그렇다면 웹-페이지는 '사용자'가 해당 페이지를 읽도록 '이용허락'을 한 것임을 알 수 있다.

101) 설사 그 당사자에 Phorm의 DPI장치가 포함되는 것으로 가정해 본다고 하여도, 사전계약이 없는 상태로 인터넷 광고에 활용하기 위하여 DPI되는 것을 '이용방법과 조건'으로 이용을 허락했다고 볼 수는 없다. 통상적으로 열람이나 다운로드를 상정하고 있을 뿐 매우 특수한 감청(DPI)을 예상하고 있다고 보기가 곤란하기 때문이다.

언급하지는 않기로 하겠다. 해당 부분에 있어 충분한 검토와 논리의 정리가 있었고, 무엇보다 주제 자체가 워낙 난삽하여 일목요연한 논리의 진행이 불가능하기 때문이기도 하다. 이러한 이유로 KT측이 밝힌 토론의 결론[102]을 반박하는 것으로 본고의 결론을 갈음하고자 한다.

KT는 결론에서, "본건 서비스와 방식이 유사한 인터넷 쿠키 및 온라인 맞춤형 광고 서비스는 다수의 포털, 전자상거래 웹사이트 등에서 이미 일반화·상용화 되어 있음"을 주장한다.

여기에 대하여 필자는 "전혀 그렇지 않다"고 답한다. 지금까지 살펴본 바와 같이, DPI형 맞춤광고는 1·2세대 맞춤광고와는 기술적으로도 유사하지 않고 야기하는 법적 문제점도 상이하다.

또한 KT는 결론에서, "본건 서비스는 감청이나 사생활(Privacy) 침해 우려를 원칙적으로 배제하도록 설계되었으며, 오히려 사생활 보호에 부합하면서도, 인터넷 이용자들의 관심과 선호를 반영하여 이용자에게 맞춤형 광고제공이 가능함"을 주장한다.

여기에 대하여 필자는 "이 또한 전혀 그렇지 않다"고 답한다. 지금까지 살펴본 바와 같이, DPI형 맞춤광고는 명확하게 감청에 해당하며 심각한 사생활 침해의 우려를 안고 있기도 해서 도저히 도입이 불가능한 기술이다.

마지막으로 KT는 결론에서, "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"을 주장한다.

여기에 대하여 필자는 "이는 정말이지 전혀(!) 그렇지 않다"고 답한다. 지금까지 살펴본 바와 같이, DPI형 맞춤광고는 통신비밀보호법의 법리상 명확하게 감청에 해당하고 비단 감청뿐만이 아니라 저작권의 침해와 더불어 정보통신망법 위반에 해당하기까지 한다. 또한 헌법공부를 더 해 보라고 권고하고 싶다.

글을 마치면서 한 가지 더하고 싶은 말이 있다. 이렇듯 감청이 상업화

---

102) 구태언, 앞의 글(주 33), 80쪽.

되면 누가 가장 반길 것인가 하는 점이다. 물론 본문에서 밝힌 바와 같이, 막대한 네트워크 회선 점유율을 가지고 있는 KT야말로 인터넷 광고 산업을 한 손에 쥐게 되니 더할 나위 없이 좋을 것이다. 그러나 우리는 이를 지켜보면서 뒤에서 즐거워하고 있을 그 누군가를 잊지 말아야 한다. 대한민국의 대부분의 네트워크 회선에다 자진해서 감청장비를 달아 준다면 가장 반길 이가 누구인가?! +_+

<참고문헌>

구태언, “온라인 맞춤광고(OBA)에 대한 입장”, 패킷감청의 문제점과 개선방안에 대한 토론회 자료집, 2010.

_____, “보충자료”, 패킷감청의 문제점과 개선방안에 대한 토론회 자료집, 2010.

김민중/안종근/육희숙, “인터넷상 쿠키를 통한 개인정보침해의 법적 문제”, 법학연구 제24집, 전북대학교 법학연구소, 2006.

나종연, “온라인 타겟 마케팅과 소비자 프라이버시 보호”, 한국 CPO 포럼 2009년도 제5차 Privacy Round Up 발표자료, 2009.

양지연, “온라인 맞춤형 광고: 개인정보보호와 정보이용의 균형점을 찾아서, 미국 FTC와 EU의 가이드라인에 비추어”, LAW & TECHNOLOGY 제5권 제2호, 서울대학교 기술과법센터, 2009.

오길영, “인터넷 감청과 DPI(Deep Packet Inspection)”, 민주법학 제41호 (2009).

임종인, “DPI 기술 활용 민간 관심기반 광고서비스의 문제점 검토”, 패킷감청의 문제점과 개선방안에 대한 토론회 자료집, 2010.

장여경, “패킷감청과 통신의 비밀”, 패킷감청의 문제점과 개선방안에 대한 토론회 자료집, 2010.

하태훈, “통화자일방의 동의를 받은 제3자의 전화녹음과 통신비밀보호법 위반: 대법원 2002.10.8. 선고, 2002도123 판결”, 안암법학 제17호, 안암법학회, 2003.

한국인터넷진흥원 인터넷정책단 법제분석팀, “인터넷 권리장전 제정 추진계획(안)”, 한국인터넷진흥원, 2010.

한국인터넷진흥원, “온라인 맞춤형 광고에 대한 인식조사”, 2009년 하반기 인터넷이슈 기획조사, 한국인터넷진흥원, 2009.

“KT, 개인형 맞춤 광고 서비스 논란: 거센 풍랑에 고개 숙인 신 사업”, 디시뉴스(DCNEWS.IN), 2010.3.11자.

"2010년 정보보호 정책 이렇게 바뀐다", 디지털데일리, 2009.12.31자.
"AOL's Big Privacy Blunder", 오마이뉴스, 2006.8.7자
"방통위, 연내 인터넷 맞춤형광고 가이드라인 만든다", 파이낸셜뉴스, 2009.10.13자.

Clayton, Richard, "The Phorm 'Webwise' System", 2008.
Gaspari, Elio, "A trapaça do rastreador da Oi no Velox", 2010.3.31자
IAB/NAI, "Self-Regulatory Principles for Online Behavioral Advertising", AAA/ANA/BBB/DMA/IAB, 2009.
London Stock Exchange Market News, "Phorm, Inc. Commercial Deployment in Brazil", 2010.3.26자.
TechCrunch, "AOL Proudly Releases Massive Amounts of Private Data", 2006.8.6자
The New York Times, "A Company Promises the Deepest Data Mining Yet", 2008.3.20자.
The Register, "Phorm turns up in Brazil", 2010.3.26자.

<http://www.assembly.go.kr/renew09/brd/formation/last_pro_vw_detail.jsp?programId=86&infoId=7304&index=769&gotopage=1>
<http://www.linkedin.com/in/jbrooksdobbs>
<http://www.linkedin.com/pub/brooks-dobbs/a/292/3bb>
<http://www.cade.gov.br/Default.aspx?d95aad7ab86e80946fa06cce61>
<http://www.cade.gov.br/temp/t245201019008085.pdf>
<http://habeasdata.doneda.net/2010/05/06/a-cartada-final-da-phorm-no-brasil-parceria-com-empresa-do-grupo-oi-retirada-da-pauta-do-cade/>
<http://www.freepatentsonline.com/7319975.html>
<https://www.google.com/accounts/ServiceLogin?service=adwords&hl=en_KR&ltmpl=adwords&passive=true&ifr=false&alwf=true&continue=https%3A%2F%2Fadwords.google.com%2Fum%2Fgaiaauth%3Fapt%3

DNone%26ugl%3Dtrue&sourceid=awo&subid=il-iw-ha-EN_GLBL_SKWS-AWFEEN&gsessionid=G9_gInx4moJikdBnZ9CUDg>
<http://www.reputationdefenderblog.com/wp-content/uploads/2010/05/Privacy_Draft_5-10.pdf>
<http://www.nytimes.com/2010/05/05/business/media/05adco.html>
<http://www.forbes.com/2010/05/04/privacy-web-advertising-technology-bill.html>
<http://www.reputationdefenderblog.com/2010/05/04/internet-advertising-privacy-bill-draws-criticism-from-both-sides/>
<http://en.wikipedia.org/wiki/FTC_Regulation_of_Behavioral_Advertising>
<http://www.iab.net/media/file/ven-principles-07-01-09.pdf>
<http://www.naver.com/rules/service.html#a17>
<http://www.iab.net/media/file/CLEAR_Ad_Notice_Final_20100408.pdf>
<http://www.pcworld.com/article/163740/us_lawmakers_target_deep_packet_inspection_in_privacy_bill.html>
<http://comlaw.wordpress.com/2009/04/24/nyt-online-privacy-bill-on-deep-packet-inspection-dpi/>

<Abstract>

Deep Packet Inspection Based Internet Targeted Advertising Systems and Their Illegality

Oh, Kil-Young
Lecturer, Sogang Univ.

This paper focuses on analysis of the illegality of Deep Packet Inspection, DPI, Based Internet Targeted Advertising Systems, DPI Based Advertising, such as that which Korea Telecom, KT, have recently been trying to introduce into the Korean communications infrastructure.

Firstly, whilst KT argues that safeguards are in place to protect personal information, avoid interception of that information and infringement of privacy, I suggest that there are serious technical problems arising from the methods used. In addition claims by KT that DPI Based Advertising is similar to existing Internet Targeted Advertising Systems are shown to be untrue.

Secondly, I consider specific illegal aspects resulting from DPI Based Advertising by means of technical analysis. In contrast to assertions by KT DPI Based Advertising cannot be considered permissible under Korean Law for the following reasons:

1) There is the possibility that an internet users real identity may be revealed;

2) The operation of DPI represents interception of communications contrary to the Communications Privacy Act as does the alteration of Cookies;

3) The operation of DPI is also contrary to Copyright Law as well as the Act on the Promotion of Information and

Communications Network Utilization and User Protection.

In conclusion it is shown that DPI Based Advertising is obviously illegal under Korean law.

Key Words: Internet Targeted Advertising Systems, DPI Based Advertising, Deep Packet Inspection, Qook Smartweb, Phorm