연구총서 13-B-03

K O R E A N I N S T I T U T E O F C R I M I N O L O G Y

망 중립성(Net Neutrality)과 통신비밀보호에 관한 형사정책

Criminal Policy on Net Neutrality and Communication Confidentiality

전현욱 · Chris Marsden · Michael Geist

KIC 한국형사정책연구원
Korean Institute of Criminology

▌전현욱

한국형사정책연구원 부연구위원, 법학 박사

▌Chris Marsden

영국 Sussex 대학 교수

▌Michael Geist

캐나다 Ottawa 대학 교수, 캐나다 인터넷과 전자상거래 연구소장

발간사

오늘날 눈부신 정보기술의 발전은 우리 삶에 많은 편리를 가져다주지만, 동시에 "정보의 지배가 곧 힘이며 자유의 조건"이 되고 있습니다. 하지만 정보기술이 우리의 삶에 미치는 영향에 대한 규범적 인식은 기술의 발전 속도를 따르지 못하고 있습니다. 새로운 현상에 대한 규범적 인식의 부재는 가치관의 혼란을 야기하고, 분쟁과 일탈이 증가하는 원인이 됩니다. 보편적 규범을 확인하기 어려운 곳에서 사람들은 일반적으로 각자의 이해관계에 따라 자신의 행위방향을 결정하기 때문입니다. 그런데 이러한 문제에 대응해야 하는 국가 역시 이를 해결하기 위한 법정책의 방향을 설정할 가치기준을 찾기 어렵습니다. 그래서 이는 결국 국가 정책의 혼선으로 이어져 "집행결손" 또는 "법의 흠결"이라는 문제 상황을 낳게 됩니다.

이 보고서에서 다루고 있는 "망 중립성(Net Neutrality)"은 정보기술의 발전으로 인해 새롭게 등장한 개념입니다. 이 용어가 학술문헌을 통해 등장하기 시작한 것은 2003년 이후로, 관련 연구자들에게도 매우 새로운 개념입니다. 그래서 망 중립성과 관련하여 우리 사회에서 보편적으로 승인된 가치기준을 확인하는 것은 쉽지 않습니다. 그러나 이미 인터넷이 생활필수품이 되어버린 매일 매일의 일상생활 속에서 망 중립성은 스마트TV를 통해 우리의 안방에, 그리고 스마트폰을 통해 우리의 손위에 놓여있는 문제가 되고 있습니다. 이러한 이유로 이미 기업과 기업간, 그리고 기업과 소비자간의 이해관계 충돌이 법적 분쟁이 되어 다양한 사회적 비용을 야기하는 원인이 되고 있는 것이 현실입니다.

하지만 사실 "망 중립성"을 침해 또는 제한하는 행위에 대한 형사정책은 이미 형법학의 오랜 관심사였습니다. 왜냐하면, 망 중립성은 "통신"의 비밀이라는 매우 중요한 법익에 관한 논의의 핵심에 맞닿아있기 때문입니다. 주지하는 바와

같이, “통신의 비밀과 자유”는 민주사회의 필수 전제조건으로 매우 중요한 법익이며 강력한 형법적 보호가 필요한 가치 중 하나라는 점에 대해서는 보편적 승인이 있습니다. 그래서 우리나라는 20여 년 전에 이미 “통신비밀보호법”을 제정하여 시행하고 있습니다. 이는 당시 전기통신이라는 기술의 발전과 보급으로 인해 기존의 “형사소송법”상 압수·수색 규정이 더 이상 통신의 비밀을 합리적으로 보호할 수 없게 되었다는 규범적 요청에 대한 입법적 대처였습니다. 그러나 현대 정보사회에서 이미 음성 통신에 비하여 데이터 통신의 비중이 훨씬 커지게 되었고, 그래서 인터넷의 자유로운 이용은 표현의 자유의 전제조건으로 공론장 형성에 없어서는 안 되는 필수 요소이며 가장 중요한 시민의 기본권 중 하나가 되었습니다. 이러한 상황에서 음성통신을 위주로 만들어진 기존의 통신비밀 보호 규범체계에 대한 인식이 데이터 통신의 영역에서 크고 작은 혼란을 겪고 있는 것입니다. 이처럼 끊임없는 기술의 발전은 다시 한 번 규범적 인식의 변화를 요구하고 있습니다.

그렇기 때문에 망 중립성 문제는 단순히 기업 및 개인 사이의 이해관계 상충의 문제로만 보아서는 안 됩니다. 이는 비밀이 엄수되어야 하는 통신에 대한 사적 개입을 어디까지 허용하고 또한 어떻게 통제할 것인가의 문제이며, 따라서 그 해결을 위한 정책의 방향은 통신비밀에 관한 규범적 논의를 통해 보다 분명해질 수 있습니다. 이 보고서는 바로 망 중립성을 통신비밀의 보호라는 형사정책적 관점에서 검토한 선도적 연구라고 할 수 있을 것입니다. 이 보고서를 토대로 앞으로 망 중립성에 관한 더욱 활발한 논의가 규범적 관점에서 펼쳐질 수 있기를 기대합니다.

2014년 2월

한국형사정책연구원

원장 곽상욱

CONTENTS

표 차례

그림 차례

국문요약

통신비밀보호법 제2조 제7호[1]와 제3조 제1항[2]그리고 제16조 제1항 제1호[3]에 의하면, 전기통신의 송·수신을 방해하는 자는 특별한 정당화 사유가 없는 한 10년 이하의 징역과 5년 이하의 자격정지로 처벌되어야 한다. 그런데 현재 우리 통신사는 기업의 이익을 극대화하기 위하여 DPI(Deep Packet Inspection)와 같은 기술적 방법을 이용하여 가입자의 통신을 실시간으로 확인하고 분류하여 선택적으로 차단하거나 전송속도를 제한한다. 이는 바로 망 중립성(Network Neutrality)을 침해하는 것이 된다. 망 중립성이란 통신망 관리자가 인터넷상의 모든 컨텐츠를 동등하게 취급해야 한다는 의미이다. 특정 패킷을 선별적으로 취급하려면 논리적으로 당연히 전체 패킷, 즉 이용자의 모든 인터넷 사용 내용에 대한 실시간 "감시"가 전제되어야만 한다. "감시"와 "방해"는 바로 통신비밀보호법상 감청의 구성요건에 포섭되는 행위이다. 그러므로 법률에 열거된 특별한 정당화 사유가 없는 한 망 중립성 저해 행위는 바로 불법감청의 구성요건에 해당하며 위법한 행위가 된다. 그러나 지금까지 우리나라에서 망 중립성과 관련하여 통신비밀보호법상 불법감청이 형사법상 주요 이슈가 된 적은 단 한 번도 없다.

행정법적 또는 민사법적 프레임에서 보면 망 중립성을 둘러싼 분쟁들은 결국 기업과 기업 또는 기업과 개인 사이의 비용전가 문제인 것처럼 보인다. 그래서

---

1) 제2조(정의) 이 법에서 사용하는 용어의 정의는 다음과 같다. 7. "감청"이라 함은 전기통신에 대하여 당사자의 동의 없이 전자장치·기계장치 등을 사용하여 통신의 음향·문언·부호·영상을 청취·공독하여 그 내용을 지득 또는 채록하거나 전기통신의 송·수신을 방해하는 것을 말한다.

2) 제3조(통신 및 대화비밀의 보호) ① 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.

3) 제16조(벌칙) ① 다음 각호의 1에 해당하는 자는 10년 이하의 징역과 5년 이하의 자격정지에 처한다. 1. 제3조의 규정에 위반하여 우편물의 검열 또는 전기통신의 감청을 하거나 공개되지 아니한 타인간의 대화를 녹음 또는 청취한 자

방송통신위원회나 공정거래위원회는 단기적이고 미시적인 손익형량의 문제로 판단하였고, 망 중립성 분쟁들은 대체로 통신사에게 유리한 방향으로 결정되었다. ① 빠른 정보통신기술의 발전으로 망 중립성에 대한 규범적 가치기준이 아직 보편적으로 자리 잡지 못하고 있기 때문에, ② 선택적 인터넷 차단 행위를 감청이라는 규범적, 거시적 관점에서 바라보지 못하고 있으며, ③ 규범의 부재로 인해 기업과 기업, 기업과 개인의 이해관계의 충돌가능성은 훨씬 높아지는 반면, ④ 정작 납득 가능한 정당한 해결책을 찾는 것에 실패할 수밖에 없으므로, ⑤ 결국 더 힘이 강한 자, 즉 네트워크를 장악하고 있는 통신회사의 이해관계가 관철되고 있는 것이다. 그래서 모호한 망 중립성 원칙은 오히려 강자의 면죄부가 되기도 한다.

그러나 현대 정보사회에서 자유로운 인터넷 접속은 표현의 자유에 대한 전제조건으로 공론장 형성의 필수요소이다. 우리는 전기통신의 등장과 함께 이미 이와 유사한 경험을 경험한 적이 있으며, 그래서 통신의 자유에 대한 강력한 보호가 필요하다는 사회적 합의는 현재 통신비밀보호법상의 강력한 형사처벌 구성요건으로 남아있다. 더욱이 통신비밀보호법 입법자들은 현명하게도 제정당시부터 앞으로의 기술발전을 포섭할 수 있도록, 명확성을 침해하지 않는 범위 내에서 미래를 향해 열려있는 “전기통신”, “송·수신 방해”와 같은 개념을 사용하였다. 다만 통신의 방식이 음성 중심에서 데이터 기반으로 변화하고 있는 지금, 법을 적용하는 과정에서 규범과 현실의 인지부조화를 겪고 있는 것일 수도 있다. 그렇기 때문에, 우리는 전통적인 법치국가 형법원칙에 근거하여 이러한 현상에 대한 정당한 해결방안을 논증할 수 있다. 망 중립성의 정책방향의 문제는 법익보호에 관한 형사정책적 관점에서 논의하면 비로소 분명해진다.

물론 인터넷을 이용한 데이터 통신은 자동화된 정보처리장치를 통해 이루어진다는 점으로 인해 음성기반의 통신과는 근본적으로 다른 특성을 갖는다. 그래서 불법적인 목적의 인터넷 이용에 대한 사전 예방적 조치가 필수적인 것으로 여겨지기도 한다. 또한 물리적인 통신망은 유한한 자원으로 망에 부하를 발생시키는 이용자에게 이에 비례하여 적절한 요금이 청구될 수 있어야 한다. 현실적으로 누가 비용을 부담할 것인가, 즉 적절한 손익분배의 관점을 떠나서는 인터넷 자체가 유지·개선되기 어려울 수도 있다. 그러므로 인터넷 서비스 제공자의 “합

리적인 트래픽 관리"가 필요하다. 그런데 형법이론적 관점에서 "합리적인 트래픽 관리"는 바로 불법감청 구성요건 해당행위의 정당화 사유가 된다. 그러나 이러한 특성은 통신비밀보호법 구성요건을 해석함에 있어서도 고려되어야 한다. DPI를 이용한 패킷 분석이 사람에 의한 내용의 지득을 전제하고 있지는 않지만, 자동적으로 "채록"되어 필요한 기간 동안 저장·분석된 후, 결국 사람이 내용을 지득하였다면 하였을 행위인 "전기통신의 송·수신을 방해"하기 위하여 이용된다. 게다가 통신비밀보호법상 감청 구성요건은 내용의 지득을 필수적인 요소로 하고 있지 않다. 또한 이용자의 "동의"는 통신사가 일방적으로 정한 "약관"을 승인하는 방식으로 이루어진다. 정당화 사유로 볼 수 있는 적법한 법익처분이라고 보기 어려운 것이다.

결국 망 중립성 정책은 통신비밀보호법상 감청구성요건 해당행위의 정당화 가능성을 검토하는 것을 통해 확인될 수 있다. 이를 위해 보고서의 전반부에서는 왜 망 중립성을 형법적 관점에서 검토해야 하는지, 그 필요성과 필연성을 설득력 있게 제시하기 위하여 노력을 기울였다. 우선 제2장에서는 현재 규범의 공백상태에 놓여있는 망 중립성 정책은 망 관리가 아니라 망 이용자의 권리 침해라는 관점에서 접근해야 보다 분명해 질 수 있음을 논증하였으며, 이러한 관점에서 선별적 접속 제한과 통신비밀보호법상 감청구성요건 해당성을 법리적으로 검토하였다. 제3장에서는 망 중립성에 대한 국외의 논의현황을 폭넓게 검토하여 정당화의 가능성과 한계를 제시하기 위한 기초자료를 제공하고자 하였다. 우선 인터넷의 자유로운 이용과 합리적인 망 관리간의 균형을 강조하는 캐나다를 중심으로, 통신사업자 친화적인 북미지역의 망 중립성과 통신비밀보호에 관한 논의의 전개 과정을 검토하였다. 북미식의 접근방법, 즉 다양한 이해관계자의 주장과 논증을 통해 직간접적으로 구체화되는 "합리적 트래픽 관리"의 조건에 관하여 살펴볼 수 있을 것이다. 또한 EU차원의 망 중립성 법제화 정책의 영향 아래 있는 영국의 망 중립성과 프라이버시 관련 문제 해결에 대한 논의를 통해서, 망 중립성 저해행위의 "감청" 해당 여부에 대한 법적 판단과, "동의" 등 정당화를 위한 절차에서 고려해야 할 규범적 요소들, 그리고 사실상 네트워크를 지배하고 있는 통신회사에 대한 법 집행상의 어려움을 확인할 수 있을 것이다.

제4장에서는 통신비밀보호법상 불법감청 구성요건에 해당하는 행위의 불법을

조각하기 위한 요건을 크게 “동의”와 “정당행위”의 관점에서 구체적으로 살펴보았다. 통신비밀보호법상 감청 동의는 형법이론상 이른바 “양해”에 해당하며, 구성요건 해당성을 배제하는 것으로 보아야 한다. 다만 통신의 비밀과 자유는 원칙적으로 법원이 발부한 허가장을 통해서만 제한될 수 있는 것으로 동의가 허가장을 우회하는 수단이 되어서는 안 되며, 따라서 설령 양해에 해당한다 하더라도 그 요건은 형법 제24조에서 규정하고 있는 피해자의 승낙에 준하여 엄격하게 검토되어야 한다. 또한 2011년 제정된 우리나라의 당시 방송통신위원회의 “망 중립성 및 인터넷 트래픽 관리에 관한 가이드라인”과 2013년 말 만들어진 “통신망의 합리적 관리·이용과 트래픽 관리의 투명성에 관한 기준(안)”의 내용에 대한 논의를 토대로 “합리적 트래픽 관리”가 업무로 인한 정당행위가 되기 위한 요건을 확인하였다. 제5장에서는 결론을 대신하여 망 중립성 침해행위에 대한 합리적인 형사정책의 방향을 제시하였으며, 첨예한 이해관계의 대립 속에서 이 기준이 준수되도록 하기 위한 절차적, 제도적 보장 방안을 모색하였다.

제1장

서론

전 현 욱

01 서론

제1절 연구의 목적

1. 왜 망 중립성을 형사정책적 관점에서 검토해야 하는가?

통신비밀보호법[4] 제2조 제7호[5]와 제3조 제1항[6]그리고 제16조 제1항 제1호[7]에 의하면, 전기통신의 송·수신을 방해하는 자는 특별한 정당화 사유가 없는 한 10년 이하의 징역과 5년 이하의 자격정지로 처벌되어야 한다. 그런데 현재 우리 통신사는 다양한 이유와 목적을 위하여, 특히 경쟁서비스를 차단하고 기업의 이익을 극대화하기 위하여 가입자의 "전기통신의 송·수신을 방해"하고 있다. 통신사들은 DPI(Deep Packet Inspection)와 같은 기술적 방법을 기반으로 가입

4) 통신비밀보호법의 문제점에 대해서는 배종대, 형법각론, 제8전정판, 2013, 58/6 참조.

5) 제2조(정의) 이 법에서 사용하는 용어의 정의는 다음과 같다. 7. "감청"이라 함은 전기통신에 대하여 당사자의 동의 없이 전자장치·기계장치 등을 사용하여 통신의 음향·문언·부호·영상을 청취·공독하여 그 내용을 지득 또는 채록하거나 전기통신의 송·수신을 방해하는 것을 말한다.

6) 제3조(통신 및 대화비밀의 보호) ① 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.

7) 제16조(벌칙) ① 다음 각호의 1에 해당하는 자는 10년 이하의 징역과 5년 이하의 자격정지에 처한다. 1. 제3조의 규정에 위반하여 우편물의 검열 또는 전기통신의 감청을 하거나 공개되지 아니한 타인간의 대화를 녹음 또는 청취한 자

자의 통신을 실시간으로 확인하고 분류하여 선택적으로 차단하거나 특정 어플리케이션에서 이용하는 패킷을 식별하여 이를 일부 차단하는 방법으로 전체적인 전송속도를 제한한다.

통신의 선택적 차단은 바로 망 중립성(Network Neutrality)을 침해하는 것이 된다. 망 중립성이란 2003년 팀 우(Tim Wu) 교수가 처음 본격적으로 제기하기 시작한 개념[8]으로, 네트워크 사업자들이 인터넷상의 모든 컨텐츠를 동등하게 취급해야 한다는 의미이다.[9] 데이터를 패킷으로 전송하는 인터넷의 구조를 고려하면, 모든 패킷을 동등하게 취급하지 않는다는 것은 결국 특정 목적으로 이용되는 패킷만을 기술적으로 식별해서 전부 또는 일부를 선택적으로 "방해"하는 것을 의미한다. 그런데 특정 목적 패킷을 선별적으로 취급하려면 논리적으로 당연히 전체 패킷[10], 즉 이용자의 모든 인터넷 사용 내용에 대한 실시간 "감시"가 전제되어야만 한다. 이용자가 인터넷을 이용해 무엇을 하고 있는지 알아야, 특정한 서비스의 이용을 방해할 수 있기 때문이다. "감시"와 "방해"는 바로 위에 인용한 통신비밀보호법상 감청의 구성요건에 포섭되는 행위이다. 그러므로 법률에 열거된 특별한 정당화 사유가 없는 한 통신사의 망 중립성 저해 행위는 바로 불법감청의 구성요건에 해당하며 위법한 행위가 된다. 그러나 지금까지 우리나라에서 망 중립성과 관련하여 통신비밀보호법상 불법감청이 주요 이슈가 된 적은 단 한 번도 없다.

물론 최근 망 중립성과 관련하여 "법적" 분쟁이 전혀 없었던 것은 아니다. 2012년 2월 KT는 스마트 TV가 인터넷 트래픽을 과도하게 발생시킨다는 이유로 삼성전자의 스마트 TV에 대한 인터넷 접속을 차단한 바 있다.[11] 이 사건에 대하여 당시 방송통신위원회는 차단되지 않은 LG전자의 스마트 TV 이용자에 비해 부당한 차별이기 때문에 전기통신사업법 제50조 제1항 제5호를 위반한 위법을 확인하였으나, 망 중립성 원칙이 아직 정립중이라는 이유로 단지 경고 처분을

8) Tim Wu, Network Neutrality, Broadband Discrimination, Journal of Telecommunications and High Technology Law, Vol. 2, 2003, 141쪽 이하.

9) 상세한 내용은 Tim Wu의 웹사이트 (http://www.timwu.org/network_neutrality.html) 참조.

10) 최소한 전체 패킷 중에서 기술적으로 사용 패턴을 파악하고 차단하기 위해 충분한 비율의 불특정 패킷.

11) 연합뉴스 2012년 2월 9일자 "KT "스마트TV 연결 인터넷망 즉시 차단"(1보)" 참조.

부과하는데 그쳤다. 또한 모바일 인터넷 전화(mobile Voice over Internet Protocol; mVoIP) 서비스를 제공하고 있는 카카오톡이 발표하고 있는 데이터 현황 기상도[12]에 따르면 현재 SKT와 KT는 사실상 통화가 불가능할 수준으로 mVoIP 서비스를 차단하고 있는 것으로 확인된다. 해당 사안에 대하여 시민단체가 SKT와 KT를 대상으로 공정거래위원회에 제소하였으나 2013년 7월 17일 소비자 후생저하효과를 인정하기 어렵다고 판단하여 무혐의 처분이 내려졌다.[13] 2013년 9월 30일 같은 사안에 대해 서울중앙지방법원에 통신사를 상대로 하는 손해배상 청구 소송이 제기된 상태이다.

그러나 위의 사례에서 알 수 있듯이, 행정법적 또는 민사법적 프레임에서 보면 망 중립성을 둘러싼 분쟁들은 결국 기업과 기업 또는 기업과 개인 사이의 단순한 비용전가의 문제인 것처럼 보이는 것이 사실이다. 그래서 방송통신위원회나 공정거래위원회는 장기적인 관점에서 망 중립성 또는 감청에 대한 규범적 고려가 전제된 객관적인 기준과 원칙에 의해서 판단한 것이라기보다는, 단기적이고 미시적인 손익형량의 문제로 본 것이다. 그렇기 때문에 이러한 분쟁들은 결국 대체로 통신사에게 유리한 방향으로 마무리되었다.

이는 ① 너무나도 빠른 정보통신기술의 발전으로 인해 망 중립성에 대한 정당한 규범적 가치기준이 사회의 법 인식에 아직 보편적으로 자리 잡지 못하고 있기 때문에[14], ② 아직 선택적 인터넷 차단 행위를 (감청이라는) 규범적, 거시적 관점에서 바라보지 못하고 있으며, ③ 동시에 규범의 부재로 인해 인터넷의 이용과 관련하여 기업과 기업, 기업과 개인의 이해관계의 충돌가능성은 훨씬 높아지는 반면, ④ 정작 이에 관하여 누구나 납득 가능한 정당한 해결책을 제시하는 것에 실패할 수밖에 없으므로, ⑤ 결국 더 힘이 강한 자, 즉 네트워크를 장악하고 있는 통신회사의 이해관계가 관철될 가능성이 높기 때문이다. 그래서 모호한 망 중립성 원칙은 오히려 강자의 면죄부가 되기도 한다. 이러한 이유로, 망 중립성 보호의 관점에서 보면 상당히 잘 만들어진 통신비밀보호법상 감청 금지 규

12) 카카오톡 홈페이지(http://www.kakao.com/services/talk/voices) 참조.

13) 전자신문, 2013년 7월 17일자 "공정위, 이통사 mVoIP 차단 관련 무혐의 결론" 참조.

14) 기술발전과 법인식의 간극으로 인한 규범의 부재 현상에 관한 분석은 전현욱, 개인정보 보호에 관한 형법정책, 고려대학교 박사학위논문, 2010, 53-55쪽 참조.

정에도 불구하고 우리나라의 인터넷 서비스 제공자들은 상당히 폭넓은 자유를 가지고 컨텐츠를 동등하게 취급하지 않는 것으로 보인다.

그러나 망 중립성은 단순한 단기적 손익분배의 관점으로만 접근할 수 있는 문제가 아니다. 현대 정보사회에서 자유로운 인터넷 접속은 그 무엇보다 중요한 시민의 기본적 자유권의 내용이며 표현의 자유에 대한 전제조건으로 공론장 형성에 없어서는 안 되는 필수적인 요소이다.[15] 그런데 우리는 통신기술의 발전, 즉 전기통신의 등장과 함께 이미 이와 유사한 경험을 경험한 적이 있으며, 그래서 사생활의 비밀과 통신의 자유에 대한 강력한 보호가 필요하다는 사회적 합의[16]는 현재 통신비밀보호법상의 강력한 형사처벌 구성요건으로 남아있다. 더욱이 우리의 통신비밀보호법 입법자들은 현명하게도 구성요건의 제정당시부터 앞으로의 기술발전을 포섭할 수 있도록, 명확성을 침해하지 않는 범위 내에서, 미래를 향해 열려있는 개념인 "전기통신", "송·수신 방해"와 같은 개념을 사용하였다. 다만 통신의 방식이 음성 중심에서 데이터 기반으로 변화하고 있는 지금, 법을 적용하는 과정에서 규범과 현실의 인지부조화를 겪고 있는 것일 수도 있다.

그렇기 때문에, 우리는 이미 가치에 대한 기존의 사회적 합의와 전통적인 법치국가 형법원칙에 근거하여 이러한 현상에 대한 정당한 해결방안을 논증할 수 있다. 그러므로 망 중립성의 정책방향의 문제는 이해관계의 충돌이라는 프레임에서 벗어나, 중대한 기본권, 즉 법익보호에 관한 형사정책적 관점에서 논의하면 비로소 분명해진다고 할 것이다. 통신의 비밀과 인터넷의 자유로운 이용에 관한 권리는 형법상 보호법익이며 관련 정책과 법제화의 방향은 기업의 이해관계가 아니라 개인적 법익의 관점에서 출발해야 한다. 동시에 망 중립성에 관한 국가정책적 가치기준을 관철하기 위한 법적 강제수단도 역시 형벌이 되어야 할 것이다. 따라서 망 중립성에 대한 형사법적 이해가 선행되어야 하며 이를 토대로 규범적 기준을 마련하고 국가정책의 기본방향이 결정되어야 한다.

---

15) Francesca Musiani/Maria Löblich, Net Neutrality from a Public Sphere Perspective, The Value of Network Neutrality for the Internet of Tomorrow, (원문은 Dynamic Coalition on Network Neutrality 홈페이지 http://nebula.wsimg.com/c65488b3edff49adc2dba84e344591bd?AccessKeyId=B45063449B96D27B8F85&disposition=0), 2013, 36-43쪽 참조.

16) 1993년 12월 27일 제정된 통신비밀보호법(법률 제4650호) 제정 이유 참조.

그러나 아직 이러한 관점의 선행연구는 국내외적으로 찾기가 쉽지 않은 것이 현실이다.[17] 이 보고서는 정책보고서로서, 망 중립성 정책에 있어서 형사정책적 고려가 필요하다는 점을 지적하고, 이에 대한 논의에 필요한 자료를 가능한 한 폭넓게 제공하는 것을 일차적인 목표로 한다.

2. 정책 방향 제시

물론 규범과 현실의 괴리가 발생하게 된 원인과 과정에 대해서는 보다 깊이 있는 검토가 있어야 할 것이다. 인터넷을 이용한 데이터 통신은 자동화된 정보처리장치를 통해 이루어진다는 점으로 인해 통신비밀보호법의 제정 배경이 된 음성기반의 통신과는 근본적으로 다른 특성을 갖는 것이 사실이기 때문이다. 그래서 자동화된 정보처리장치를 통한 악성 코드 유포나 특정 서비스의 과다 이용이 망 전체에 장애를 야기하기도 하며, 장애 발생시 이로 인해 광범위한 피해가 야기될 가능성이 높을 수밖에 없다. 그럼에도 불구하고 사실상 사후적 대응이 어렵기 때문에, 불법적인 목적의 인터넷 이용에 대한 사전 예방적 조치가 필수적인 것으로 여겨지기도 한다.

또한 물리적인 통신망은 유한한 자원으로 이를 구축하고 유지하는 것에는 막대한 비용이 소요되며, 이 비용을 감당하고 새로운 기술개발을 위한 신규투자에 필요한 자금을 마련하기 위하여, 망에 부하를 발생시키는 이용자에게 이에 비례하여 적절한 요금이 청구될 수 있어야 한다. 그러나 데이터 통신의 자동성으로 인해 음성통신과는 달리 소수의 이용자, 또는 컨텐츠 제공자가 막대한 트래픽을 발생시키는 것도 가능한 구조로 되어있다. 그러므로 현실적으로 누가 비용을 부담할 것인가, 즉 적절한 손익분배의 관점을 떠나서는 인터넷 자체가 유지·개선되기 어려울 수도 있는 것이다. 그래서 이렇게 만들어진 정보통신망은 공공재가

17) 망 중립성 저해행위를 감청의 관점에서 보는 국내의 선행연구로는 오길영, 인터넷 감청과 DPI, 민주법학, 제41호, 2009, 391쪽 이하; 오길영, 감청의 상업화와 그 위법성, 민주법학, 제43호, 2010, 419쪽 이하; 박희영, DPI 기술의 운영과 ISP의 형사책임, Internet and Information Security, 제2권 제1호, 2011, 105쪽 이하.

아니라 사유재라는 주장도 일견 설득력이 있다.

그러므로 인터넷을 유지하고 효율적으로 운영하기 위하여 물리적인 통신망을 구축하고 소유하며 관리하는 인터넷 서비스 제공자의 "합리적인 트래픽 관리"가 필요한 것이다. 그런데 형법이론적 관점에서 "합리적인 트래픽 관리"는 바로 불법감청 구성요건 해당행위의 정당화 사유가 된다. 이러한 이유로 인하여 사용자들은 각종 통신서비스에 가입할 때 통신사가 정한 약관에 따라 통신사의 망 관리 행위에 동의하는 절차를 필수적으로 거치게 되며, 이러한 동의는 별다른 논의 없이 통신비밀보호법 제2조의 "동의"에 해당하는 것으로 간주된다. 게다가 DPI 장비를 이용한 디지털 통신의 패킷 식별은 자동화된 정보처리장치에 의해 자동적으로 수집·분석·분류되며 그 과정에서 사람이 통신의 내용을 "지득"하는 일은 없는 경우가 대부분이다. 따라서 통신사들은 DPI 장비 활용에 관하여 애초에 통신비밀보호법 구성요건 해당성 자체를 부인하고 있다.

그러나 데이터 통신의 음성 통신과의 차이점, 즉 자동성은 "합리적인 트래픽 관리"의 필요성에 대한 논거가 되기도 하지만, 동시에 통신비밀보호법 구성요건을 해석함에 있어서도 고려되어야 한다. DPI를 이용한 패킷 분석이 음성통신의 감청과는 달리 사람에 의한 내용의 지득을 전제하고 있지는 않지만, 자동화된 정보처리장치를 통한 패킷의 처리를 위한 것이며, 이를 통해 자동적으로 "채록"되어 필요한 기간 동안 저장·분석된 후, 결국 "전기통신의 송·수신을 방해"하기 위하여 이용된다. 또한 현재 통신비밀보호법상 감청 구성요건은 내용의 지득을 필수적인 요소로 하고 있지 않다는 점에 주목할 필요가 있다. 게다가 이용자의 "동의"는 각종 통신 서비스에 가입할 때 구체적인 내용을 모르는 상태에서 통신사가 일방적으로 정한 "약관"에 동의하는 방식으로 이루어진다. 형법이론적으로 정당화 사유로 볼 수 있는 적법한 법익의 처분이라고 보기 어려운 것이다.

결국 국가의 미래를 위한 망 중립성 정책, 즉 통신비밀보호법상 감청 구성요건 해당행위의 정당화 가능성과 한계는 적법한 법익 처분으로서의 "동의"는 어떠한 요건 아래에서 인정될 수 있는지, 그리고 "합리적인 트래픽 관리"의 범위는 어떻게 설정되어야 하는지를 검토하는 것을 통해 확인될 수 있다. 이 보고서는 우선 법제도적, 기술적 측면에서 정당화를 위해 고려해야 할 요소들을 검토하고, 이를 토대로 망 중립성에 대한 형사정책적 방향을 제시하는 것을 목표로 한다.

이를 위해 망 중립성과 관련하여 상반되는 양측의 논거를 열린 시각에서 폭넓게 검토하고, 꼭 지켜져야 할 법익이 무엇이고 이를 지키기 위해 고려해야 할 점과 필요한 절차는 어떠해야 하는가를 검토해 보고자 한다. 동시에 또한 인터넷을 통한 디지털 통신 환경에서 "합리적인 트래픽 관리"의 범위를 준수하였는지 여부를 법제도적으로 확인하기 위해 필요한 요건을 정책대안으로 제시하겠다.

제2절 연구의 범위와 방법

그러므로 이 보고서는 망 중립성 관련 통신정책 전반을 다루기 위한 글이 아니다. 오로지 망 중립성 저해행위가 통신비밀보호법상 감청에 해당하는지 여부에 한정하여 형사정책적 관점에서 정당화 가능성을 검토하고 "합리적인 트래픽 관리", 즉 정당화 사유에 대한 정책적 판단에 필요한 범위 내에서만 논의하고자 한다. 그러나 국내외를 막론하고 망 중립성은 불과 1~2년 정도 사이에 논의되기 시작한 개념으로, 아직은 형사정책적 관점에서 참고할만한 문헌자료가 그리 다양하지 못한 것이 현실이다.

그래서 이 보고서를 작성하기 위해 국내외 망 중립성 관련 기술적, 정책적 연구 자료, 단행본, 논문 및 연구보고서 등 다양한 자료를 수집하여 종합적으로 검토하고, 실제 발생하고 있는 망 중립성 분쟁 사건 및 이에 관련된 기관 및 단체의 움직임 등에 대한 구체적 사례를 확인하여, 이를 토대로 국내에서 제기되고 있는 망 중립성 관련 문제 현상을 파악하였으며, 이를 통해 형사정책적 관점에서 필요한 내용을 선별하여 그 근본적인 원인을 분석하고자 하였다. 그 과정에서 문헌으로 기록된 자료에 국한되지 않고, 망 관리 업무 담당자는 물론 정보통신 보안기술 전문가와 민간 운동가등 다양한 입장의 전문가들로부터 상호간의 관점을 교류할 수 있도록 지속적인 자문을 구하였다.

이러한 노력을 통해 보고서의 전반부에서는 왜 망 중립성을 형법적 관점에서 검토해야 하는지, 그 필요성과 필연성을 설득력있게 제시하기 위하여 많은 노력을 기울였다. 이를 위해 제2장에서는 우선 현재 규범의 공백 상태에 놓여있는 망 중립성 정책은 망 관리가 아니라 망 이용자의 권리 침해라는 관점에서 접근

해야 보다 분명해 질 수 있음을 설명하였으며, 이러한 관점에서 선별적 접속 제한과 통신비밀보호법상 감청구성요건 해당성을 법리적으로 검토하고자 한다. 실제 문제가 된 사례를 상세하게 살펴보고 실제 기술을 적용하는 행위가 불법감청의 구성요건에 해당하는지를 구체적으로 확인해 본다. 이를 위해 통신 내용을 실시간 감시하는데 이용되고 있는 기술적 방법과 원리를 형사정책적 검토를 위해 필요한 범위 내에서 살펴본다. 더 나아가 보호법익으로서 통신비밀의 성격, 그리고 정보적 자기결정권과 인터넷 접속의 자유에 관해서도 검토해 보겠다.

제3장에서는 망 중립성에 대한 국외의 논의현황을 폭넓게 검토하여 정당화의 가능성과 한계를 제시하기 위한 기초자료를 제공하고자 한다. 이 과제의 연구기획 단계에서 본의 아니게 국제공동연구에 선정된 사정이 있어, 국외의 전문가와 함께 연구할 수 있었다. 우연하게 주어진 기회를 충분히 이용하고자 국외의 역량 있는 연구자를 선정하려 하였으나, 수개월간의 노력에도 불구하고 아쉽게도 결국 형사정책적 관점에서 망 중립성을 직접적으로 연구한 학자는 찾을 수 없었다. 망 중립성에 관해서는 다른 나라에서도 논의가 이제 비로소 전개되기 시작했으며, 형사정책적 관점에서 학문적인 성과로 참고할만한 것은 찾기 어려웠기 때문이다.

그러나 다행히 망 중립성 법정책 연구자 중에서 프라이버시 및 정보적 자기결정권에 대한 이해가 깊은 전자상거래법 전문가(캐나다 오타와 대학교 마이클 가이스트 교수[18])와 미디어법 전문가(영국 서섹스 대학교 크리스 마스든 교수[19])를 찾을 수 있었으며, 제한된 예산과 기간의 범위 내에서 연구 주제 및 방향에 대한 지속적인 의사소통을 통해 비록 형사정책에 직접 논의의 초점이 맞춰진 것은 아니지만 충분히 참고할 만한 그들의 연구 성과를 얻을 수 있었다.

---

18) Michael Geist 교수는 캐나다 인터넷과 전자상거래법 연구소 소장으로 프라이버시와 지적재산권에 관하여 활발한 연구를 수행하였으며, 약 2008년 이후부터는 망 중립성과 이에 대한 법정책에 관하여 적극적인 연구를 수행하고 있다. 캐나다의 프라이버시 커미셔너의 자문위원이며, 블로그 및 언론에 망 중립성 칼럼을 발표하는 등 다양한 분야에서 활발하게 활동하고 있다.

19) Chris Marsden 교수는 최근까지 Essex 대학교에 재직하다 올해 초 Sussex 대학 미디어법 교수로 임용되었으며 인터넷상의 규제에 관하여 다수의 연구성과를 발표한 바 있다. 최근에는 망 중립성을 인터넷 공간의 거버넌스 문제의 차원에서 접근하면서 각 이해관계 당사자들이 모두 참여할 수 있는 공동규제 시스템을 만드는 것이 가능한 해결책이 될 수 있을 것이라는 의견을 제시하였다.

제3장에서는 이를 번역하여 소개한다. 우선 인터넷의 자유로운 이용과 합리적인 망 관리간의 균형을 강조하는 캐나다를 중심으로, 통신사업자 친화적인 북미지역의 망 중립성과 통신비밀보호에 관한 논의의 전개 과정을 검토한다. 북미식의 접근방법, 즉 다양한 이해관계자의 주장과 논증을 통해 직간접적으로 구체화되는 "합리적 트래픽 관리"의 조건에 관하여 살펴볼 수 있을 것이다. 또한 EU차원의 망 중립성 법제화 정책의 영향 아래 있는 영국의 망 중립성과 프라이버시 관련 문제 해결에 대한 논의를 통해서, 망 중립성 저해행위의 "감청" 해당 여부에 대한 법적 판단과, "동의" 등 정당화를 위한 절차에서 고려해야 할 규범적 요소들, 그리고 사실상 네트워크를 지배하고 있는 통신회사에 대한 법 집행상의 어려움을 확인할 수 있을 것이다.

그리고 연구기간 말미에 호주에서 망 중립성과 프라이버시에 관련한 논의가 상당히 전개된 것을 확인하고 긴급히 자료를 수집하여 이를 추가하였다. 이로 인해 제3장이 다소 비대해진 면이 있지만, 현재 망 중립성과 통신비밀보호에 관하여 정리된 논의나 논거로 삼을만한 권위 있는 참고문헌을 찾기가 어려웠기 때문에, 논증의 근거를 제시하기 위하여 망 중립성 정책과 관련한 실제 논의의 전개 현황을 면밀하게 살펴볼 필요가 있었다. 특히 이 보고서에서는 자료제공의 의미를 담아 외국의 논의를 가능한 한 상세하게 소개하였으며, 그 중 형사정책적 논의에 직접 닿아있는 부분은 바로 프라이버시와 감청에 관한 각 이해당사자들의 주장과 이에 대한 각국 정부 및 국제기구의 입장이 될 것이다.

제4장에서는 이러한 논의들을 토대로 선별적 접속 제한 행위에 대한 정당화의 가능성과 한계를 검토한다. 구체적으로는 우선 이용자의 "동의"가 구성요건 해당성 배제사유로서 양해에 해당하는지, 또는 위법성 조각사유로 피해자의 승낙으로 보아야 하는지를 살펴보고, 실제로 불법을 조각하기 위해 필요한 동의의 요건을 확인한다. 또한 감청의 궁극적인 정당화 사유로 판단되는 합리적 트래픽 관리의 기준과 관련하여 특히 우리나라 미래창조과학부가 주관하여 제정하려 하고 있는 "통신망의 합리적 관리·이용과 트래픽 관리의 투명성에 관한 기준(안)"의 내용을 중심으로 기준(안)이 제시하고 있는 각각의 사유에 대하여 위법성 조각 사유로서 형사법적 의미를 고찰해 보도록 하겠다. 제5장에서는 결론을 대신하여 지금까지의 논의를 토대로 망 중립성 침해행위에 대한 합리적인 형사정책

의 방향을 제시하고자 한다. 합법적으로 가능한 “망 관리”의 범위를 제시하고, 첨예한 이해관계의 대립 속에서 이 기준이 준수되도록 하기 위한 절차적, 제도적 보장 방안을 모색해 본다.

제2장

망 중립성에 대한 형법적 이해

전 현 욱

02

망 중립성에 대한 형법적 이해

제1절 통신비밀보호법상 감청과 망 중립성

1. 통신비밀보호법상 감청 구성요건

가. 내 용

현행 통신비밀보호법은 감청의 구성요건을 다음과 같이 규정하고 있다.

> **제2조(정의)** 이 법에서 사용하는 용어의 정의는 다음과 같다. (중략) 7. "감청"이라 함은 전기통신에 대하여 당사자의 동의 없이 전자장치 · 기계장치 등을 사용하여 통신의 음향 · 문언 · 부호 · 영상을 청취 · 공독하여 그 내용을 지득 또는 채록하거나 전기통신의 송 · 수신을 방해하는 것을 말한다. (후략)
>
> **제3조(통신 및 대화비밀의 보호)** ① 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. (후략)
>
> **제16조(벌칙)** ① 다음 각호의 1에 해당하는 자는 10년 이하의 징역과 5년 이하의 자격정지에 처한다. 1. 제3조의 규정에 위반하여 우편물의 검열 또는 전기통신의 감청을 하거나 공개되지 아니한 타인간의 대화를 녹음 또는 청취한 자 (후략)

통신비밀보호법 제2조 제7호와 제3조 제1항 그리고 제16조 제1항 제1호에 의하면, 당사자의 동의 없이 전기통신의 송 · 수신을 방해하는 자는 누구든지 제3

조 제1항에 제한적으로 열거된 법률의 규정에 의한 정당화 사유나, 형법총칙 제20조 내지 제24조에 의한 위법성 조각 사유가 없는 한 10년 이하의 징역과 5년 이하의 자격정지로 처벌되어야 한다. 이 구성요건은 헌법 제18조에서 보장하고 있는 "통신의 비밀"을 침해하는 자를 처벌하기 위한 것으로, 사생활의 비밀과 통신의 자유는 자유로운 민주사회의 전제조건이 되므로[20] 예외적으로 감청이 정당화 될 수 있는 경우를 극히 제한적으로 열거하고 있다.

나. 적용 범위 - 전기통신, 청취, 공독, 지득, 채록, 송·수신 방해

또한 우리 헌법은 통신의 도구를 제한하고 있지 않으며[21] 통신비밀보호법 제2조 제3호[22]는 전자적 방식에 의한 모든 음향·문언·부호·영상의 송·수신을 전기통신으로 정의하고 있으므로 통신비밀보호법의 통신은 당연히 음성 통신은 물론 데이터 통신을 포함하여 모든 유형의 전자적 방식으로 운영되는 통신을 포함하는 개념으로 해석된다.[23] 특히 우리의 통신비밀보호법 입법자들은 당시 데이터 통신에 대한 이해가 깊지 않았을 것임이 분명함에도 불구하고, 현명하게도 통신비밀보호법 제2조 제7호에서 감청에 대한 정의를 일반적인 언어사용례보다 비교적 넓게 정하였다. 국어사전은 감청의 의미를 "기밀을 보호하거나 수사 따위에 필요한 참고 자료를 얻기 위하여 통신 내용을 엿듣는 일"이라고 설명한다.[24] 즉 본래 우리말에서 일반적으로 사용되는 감청이라는 단어는 감청을 하는 사람이 통신의 내용을 파악하는 것을 의미하는 것이다.

그러나 통신비밀보호법상 감청은, 물론 "청취·공독하여 그 내용을 지득 또는 채록"하는 행위라고 정의되긴 하지만, 이에 부수하여 "전기통신의 송·수신을 방

20) 국회정치관계법심의특별위원장, 통신비밀보호법안(대안), 1993. 12, 1쪽.

21) 차진아, 사이버범죄에 대한 실효적 대응과 헌법상 통신의 비밀 보장, 공법학연구, 제14권 제1호, 2013, 41쪽.

22) 통신비밀보호법 제2조 제3호 "전기통신"이라 함은 전화·전자우편·회원제정보서비스·모사전송·무선호출 등과 같이 유선·무선·광선 및 기타의 전자적 방식에 의하여 모든 종류의 음향·문언·부호 또는 영상을 송신하거나 수신하는 것을 말한다.

23) 김형준, 현행 통신비밀보호법의 문제점과 개선방안 - 통신제한조치와 대화감청을 중심으로 -, 형사법연구, 제24호, 2005, 216-217쪽.

24) 국립국어원 표준국어대사전(http://stdweb2.korean.go.kr/main.jsp)에서 인용

해하는 것"까지도 포함한다. 추정컨대, 통신비밀보호법 제5조 제1항에서 법적으로 허용되는 감청에 대하여 "통신제한조치"라는 용어를 사용하고 있는 것으로 보아, 당시 입법자들은 데이터 통신에 대한 자동화된 처리를 염두에 두고 있지는 않았지만, 음성 통신이라 하더라도 내용의 지득 없는 단순한 송·수신 방해를 법이 허용하는 강제수사의 범위에 넣고자 했던 것으로 보인다. 범인의 검거뿐만 아니라 범죄의 예방을 위해 통신제한조치가 허가될 수 있다는 점을 고려한다면, 단지 내용을 지득할 수만 있고 통신을 방해할 수 없게 되는 경우 범죄목적의 정보전달을 막지 못하게 될 수도 있는 불합리를 피하고자 했던 것으로 생각된다.

그러므로 본래 통신비밀보호법상 감청은 일반적인 국어 사용례와는 다른 개념이며, 내용의 지득 없이 송·수신을 방해하는 경우도 이에 포함되는 것으로 보아야 한다. 그래서 결과적으로 우리 통신비밀보호법은 제정될 당시부터 디지털 통신은 물론 앞으로의 통신기술발전을 포섭할 수 있도록, 명확성을 침해하지 않는 범위 내에서 열려있는 구성요건 표지를 사용하는 미래지향적 구조를 갖게 되었다. 특히 "전기통신", "송·수신 방해"는 음성통신 이외의 거의 대부분의 통신행위를 포섭할 수 있는 개념이며, 또한 내용의 지득을 필수적인 구성요건 요소로 하고 있지 않아, 자동화된 장비를 이용하여 데이터 통신을 식별하여 분류하고, 특정 패킷을 골라내어 전송하지 않는 행위에 대해서도 구성요건 해당성을 인정할 수 있는 것이다.

다만 현행 통신비밀보호법은 "청취·공독하여 그 내용을 지득 또는 채록"한 경우라고 규정하고 있으므로 청취·공독 없는 기계적 채록의 경우에는 감청이 성립되지 않는다는 견해가 있다.[25] 이 견해에 따르게 되면 전화통화의 내용을 듣지 않고 단순히 기계장치를 부착하여 녹음하기만 하는 경우와 마찬가지로 사람의 인지 없이 자동화된 정보처리기기(DPI 장비 등)를 이용하여 패킷의 패턴을 분석하는 경우, 이어지는 송·수신 방해 행위가 없다면 감청 구성요건에 해당하지 않게 된다. 그러나 아래에서 설명하는 바와 같이 망 중립성 저해 행위는 필

25) 김형준, 현행 통신비밀보호법의 문제점과 개선방안 - 통신제한조치와 대화감청을 중심으로 -, 형사법연구, 제24호, 2005, 221-222쪽. 이는 입법의 불비이므로 "청취·공독 하거나 지득·채록하여"로 개정하는 것이 바람직하다고 한다.

수적으로 송·수신 방해를 수반하게 되므로, 이러한 지적은 이 보고서의 논지에 영향을 주지 않는다. 게다가 후술하겠지만, 정보기술의 발전으로 사람이 직접 그 내용을 청취·공독한 바가 없다 하더라도 만약 내용을 알았다면 하고자 하는 업무를 미리 프로그래밍된 자동화된 장치를 통해 수행하고 있다면, 내용을 청취·공독한 것과 실질적으로 차이가 없으며, 따라서 통신의 비밀과 자유는 이미 침해된 것으로 보아야 할 것이다.

다. 적용상의 한계

그러나 이처럼 강력한 구성요건에도 불구하고 우리나라의 인터넷 서비스 제공자들은 최근 상당히 폭넓은 자유를 가지고 전기통신의 송·수신을 차별적으로 방해하고 있는 것으로 보인다. 전 세계의 주요 국가의 인터넷 서비스 제공 회사들을 상대로 2009년부터 2012년 1사분기까지 진행된 한 조사[26]에 따르면, 우리나라의 최대 유무선 통신사업체 중 하나인 KT는 2009년과 2010년 사용자의 Bittorrent[27]의 전송을 차단하거나 DPI 장비를 이용한 패킷 분석과 속도제한을 가장 많이 한 통신사로 선정된 바 있다. 또한 이하에서 살펴볼 바와 같이 2012년에는 우리나라 통신사들이 공개적으로 스마트 TV[28]와 mVoIP와 같은 타사의 경쟁서비스를 선별하여 차단한 일도 있었다.

이처럼 실제 우리나라의 유무선 인터넷 사업자들은 인터넷의 효율적 운영과

---

26) M-Lab(http://www.measurementlab.net/)의 조사. 이에 관해 상세한 내용은 본 조사 결과를 인터넷상에 공개하고 있는 시라큐스 대학교 "The Network is Aware" 연구팀 홈페이지 (http://dpi.ischool.syr.edu/Topthrottlers.html) 참조. 이 연구는 미국 국립 과학연구재단의 연구지원으로 수행되었다. 물론 M-Lab의 조사는 모든 통신사를 조사한 결과가 아니며 통계학적으로 적절하게 설계된 것이라고 하기는 어려울지도 모른다. 우리나라 통신사 중에서는 유일하게 KT만이 조사대상에 포함되었으며, 2011년에는 10건 이하의 테스트만이 집계되었기에 발표에서 배제되었다. 12회의 테스트가 집계된 2012년 1사분기에는 세계 10위권에 포함되었다. KT는 조사기간 중 총 137회의 조사에서 127번 속도를 제한한 것이 확인되었으며, 제한비율은 93퍼센트에 이른다.(홈페이지 발표내용 재가공) 조사방법론에 대해서는 연구팀 홈페이지 "Surveying internet surveillance"(http://dpi.ischool.syr.edu/DPI-flyer-small.pdf) 참조.

27) 가장 널리 이용되는 P2P 파일 전송 서비스 중 하나이다.

28) 통신사들이 제공하고 있는 IPTV 서비스와 경쟁관계에 있다.

망 관리를 이유로 데이터의 종류에 따라 전송을 차단하거나 속도를 차별하기도 하며, 더 나아가 기업의 이윤을 극대화하기 위하여 자사가 제공하는 유료 서비스의 수익에 영향을 줄 수 있는 경쟁 서비스를 차별적으로 방해하고 특정한 서비스에 대해서는 별도의 요금체계에 따른 이용료를 청구하기도 한다. 이를 위해 통신사들은 거액을 투자하여 DPI장비를 도입하였으며, 이 장비를 활용하여 통신의 내용을 확인하고 분류하여 선택적으로 차단하거나, 특정 어플리케이션에서 이용하는 패킷을 식별하여 이를 일부 차단하는 방법으로 전체적인 전송속도를 제한하고 있다.

즉, 통신사들은 다양한 목적과 이유로 가입자의 "전기통신의 송·수신을 방해"하고 있는 것이다. 그럼에도 불구하고 통신사의 전기통신 송·수신 방해 행위가 통신비밀보호법상 불법감청에 해당하는 것으로 보아 형사법적 문제가 제기된 사례는 지금까지 단 한 번도 없다. 통신사의 차별적 통신방해에 대하여 통신사들은 언제나 예외적인 정당화 사유가 있는 것으로 주장하고 있으며, 이에 대한 구체적인 검증은 이루어진 바 없는 상태에서 구성요건 해당성조차 검토되지 않고 있는 것이 현실이다.

2. 망 중립성(Network Neutrality)의 개념과 "전기통신의 송·수신 방해"

가. 망 중립성의 개념

그런데 통신의 선별적 차단은 바로 망 중립성(Network Neutrality)을 침해하는 행위가 된다. 망 중립성이라는 용어는 2003년 콜롬비아 로스쿨(당시 버지니아 로스쿨)의 팀 우(Tim Wu) 교수가 "망 중립성, 광대역 망에서의 차별"[29]이라는 논문에서 오픈 액세스(Open Access) 및 광대역 망에서의 차별(Broadband Discrimination)과 구별하면서 처음 본격적으로 제기한 개념으로, 네트워크 사업자들은 인터넷상의 모든 컨텐츠를 동등하게 취급해야만 한다는 원칙을 말한다.[30] 초기에는 세

29) Tim Wu, Network Neutrality, Broadband Discrimination, Journal of Telecommunications and High Technology Law, Vol. 2, 2003, 141쪽 이하.

부적으로 비차별(non-discrimination), 상호접속(interconnection), 접근성(access)의 세 가지 원칙을 기본적 내용으로 하였으나, 망 중립성에 관한 논의가 계속됨에 따라, 최근에는 불합리한 차별금지(No Unreasonable Discrimination), 차단금지(No Blocking), 투명성(Transparency)이 강조되고 있다.[31]

가장 엄격한 의미의 망 중립성은 인터넷 사업자들이 망에서의 정보 흐름에 대하여 어떠한 방해도 하지 않을 것을 요구하는 것이다.[32] 그러나 망 중립성 원칙의 개념과 규범적 의미에 관한 논의는 아직 진행 중이며, 다양한 관점과 다양한 주장이 전개되고 있다. 망 중립성 지지자들은 개방된 네트워크의 성격을 유지하기 위하여 망 중립성 정책을 뒷받침 하는 것이 정부의 중요한 역할이라고 주장한다. 반면 이러한 규제는 오히려 광대역망의 발전에 해가 되기 때문에 불필요하다고 주장하는 반대 입장도 찾을 수 있다.[33]

나. 통신의 차별적 취급과 통신비밀보호법

본래 망 중립성은 인터넷의 설계 원리이자 구조적 본질인 단대단(end-go-end) 원칙[34]에 따라 당연히 인정되는 개념이었다. 단대단 원칙이란 네트워크는 단지 정보의 전달을 위한 것이므로 가장 간단하게 설계하여 전송에 소요되는 비용을 최소화해 한다는 원칙으로, 인터넷의 정보처리는 네트워크에 연결된 최종이용자(end user)에게 맡겨져야 하며, "먼저 도착한 자료를 먼저 처리하여 최선의 노력

30) Tim Wu 교수는 망 중립성을 달성해야 하는 목표로, 오픈 액세스와 차별 금지를 망 중립성을 보호하기 위한 수단으로 설명하고 있다. 망 중립성의 개념과 관련된 논의를 폭넓게 검토하는 것은 이 보고서의 목표가 아니며 가능하지도 않으므로, 형사정책적 관점에서 설명이 필요한 부분만을 다루기로 한다. 망 중립성에 관하여 상세한 내용은 Tim Wu의 웹사이트 (http://www.timwu.org/network_neutrality.html) 참조.

31) 한국방송통신전파진흥원, 글로벌 모바일 망 중립성 현황과 전망, 2012. 7. 24, 1쪽 참조. 이는 FCC의 오픈 인터넷 규칙의 내용이기도 하다. 망 중립성 세부원칙의 개념변화, 특히 투명성의 강조 필요성에 대해서는 제4장에서 상술한다.

32) 최승재, 경쟁법의 관점에서 본 망 중립성에 대한 연구, 언론과 법 제10권 제2호, 2011, 372쪽 참조.

33) 망 중립성에 관한 찬반 논의에 대해서는 임영덕, 미국 미디어 규제와 망 중립성에 대한 고찰, 미국헌법연구, 제21권 제3호, 2010, 76쪽 참조. 그러나 이 보고서는 후술하는 바와 같이 망 중립성을 시민의 권리에 대한 불법적인 침해라는 차원에서 접근해야 그 실질에 대한 이해가 분명해 질 수 있음 논증하고자 한다.

34) 단대단 원칙은 망 중립성 이용자 포럼 김보라미 변호사의 자문을 기초로 작성되었다.

(best efforts)을 다하는 네트워크"[35]가 되어야 한다는 것이다. 즉 인터넷은 단지 정보전달을 위한 도구이므로 가장 단순한 구조를 통해 최선의 효율성을 달성하면 되는 것이고, 그 도구를 어떻게 이용하는가는 전적으로 망의 양쪽 끝단에 연결된 사용자의 자율이라는 것이다.

그러나 1990년대 이후 통신 회사의 규모가 커지고 방송과 통신이 융합하면서 그리고 이해관계가 서로 다른 망 관리자들이 물리적 통신망을 구축하고 관리하기 시작하면서 당연히 지켜질 것으로 생각했던 단대단 원칙이 위협받기 시작하였고, 이러한 과정에서 망 중립성을 정책적으로 보호할 필요가 있다는 논의가 제기되었다.[36] 서비스 및 컨텐츠의 제작에서 전송에 이르기까지 전 과정의 수직계열화가 진행되는 과정에서 컨텐츠 제작사를 거느리게 된 통신회사가 자사의 통신망을 통해 전송되는 정보의 유형과 내용에 이해관계를 갖기 시작하였고, 자사의 컨텐츠를 우대하기 위해 경쟁관계에 있는 통신을 차별적으로 취급하는 기술적 수단들을 도입하여 활용했기 때문이다.[37] 그런데 인터넷에서 데이터의 전송을 차별적으로 취급한다는 것은 특정 내용을 가진 정보를 식별하여 전송을 전부 차단하거나, 일부를 차단하여 해당 컨텐츠의 전체적인 전송 속도를 낮추는 것을 의미한다.

그런데 이는 바로 "전기통신의 송·수신을 방해하는 것"으로 현행 통신비밀보호법 제2조 제7호가 정의하고 있는 감청의 개념에 해당하는 행위가 된다. 즉 정당한 이유 없이 망 중립성을 저해하는 행위는 정보통신 기술의 발전으로 인해 새롭게 발생한 프라이버시 침해이며 당연히 형사불법에 해당한다. 별도의 논증 없이도 프라이버시에 대한 적법한 제한은 그보다 더 중대한 이익을 위해서만 정당화될 수 있으며, 사적 이익을 위해 타인의 프라이버시를 침해하는 것은 원칙적으로 정당화되기 어렵다. 따라서 이러한 주장은 충분히 합리적인 논증과 함께

35) 정영철, 인터넷접속서비스와 망 중립성 - 사업자권한과 국가권련간 균형을 중심으로, 정보법학, 제14권 제2호, 2010, 145쪽.

36) 인터넷의 단대단 원칙과 망 중립성에 관한 논의는 Mark A. Lemley/Lawrence Lessig, The End of End-to-End: Preserving the Architecture of the Internet in the Broadband Era, UCLA Law Review, Vol. 48, 2001, 925쪽 이하 (원문은 http://papers.ssrn.com/sol3/papers.cfm?abstract_id=247737) 참조.

37) 망 중립성 논쟁의 배경으로는 최승재, 경쟁법의 관점에서 본 망 중립성에 대한 연구, 언론과 법 제10권 제2호, 2011, 376쪽 이하.

제기되어야 한다. 형사소송절차에서도 검사에 의해 구성요건해당사실이 입증되면 피고인이 위법성 조각사유에 해당하는 사실이 부존재하는지 여부에 대하여 법관이 의심을 품을 정도로 입증해야 하는 부담을 지게 되는 것이 원칙이다.[38] 그러나 상술한 바와 같이 지금까지 우리나라에서 망 중립성 저해행위가 형사불법의 차원에서 사회적으로 주요 이슈가 되거나, 이에 관하여 형사법적 절차가 개시된 적은 단 한 번도 없었다. 아직까지 이에 대한 불법의식이 자리 잡고 있지 못하고 있는 것이다.

다. 「전기통신사업법」 및 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 위반

이 외에도 전기통신사업법 제83조 제1항은 "누구든지 전기통신사업자가 취급중에 있는 통신의 비밀을 침해하거나 누설하여서는 아니 된다"고 하여 전기통신사업자가 취급하는 통신의 비밀의 보호를 선언하고 있다. 이를 위반하면 같은 법 제95조 제7호에 의해 3년 이하의 징역 또는 1억 5천만원 이하의 벌금으로 처벌된다. 또한 전기통신사업법 제83조 제2항은 "전기통신업무에 종사하는 자 또는 종사하였던 자는 그 재직 중에 통신에 관하여 알게 된 타인의 비밀을 누설하여서는 아니 된다"고 선언하고 있으며, 역시 이를 위반하는 경우 같은 법 제94조 제4호에 의해 5년 이하의 징역 또는 2억원 이하의 벌금으로 처벌된다. 그러나 제83조 제1항과 제2항의 구성요건은 비밀의 누설을 그 행위양태로 하고 있어 선별적 송·수신 차단에 직접 적용하기 어려울 것으로 판단된다.

오히려 망 중립성 저해행위는 같은 법 제3조 제1항의 정당한 사유 없는 전기통신역무제공 거부나 같은 조 제2항의 공평의무 위반[39], 같은 법 제50조 제1항 제1호의 불합리한 차별 금지, 또는 같은 항 제5호의 이용자 이익에 대한 현저한 침해[40]에 해당하는 것으로 보인다. 제3조에 해당하는 경우 제92조에 의해 미래

38) 배종대/이상돈/정승환/이주원, 신형사소송법, 제5판, 홍문사, 2013, 54/30 참조.

39) 전기통신사업법 제3조(역무의 제공 의무 등) ① 전기통신사업자는 정당한 사유 없이 전기통신역무의 제공을 거부하여서는 아니 된다. ② 전기통신사업자는 그 업무를 처리할 때 공평하고 신속하며 정확하게 하여야 한다.

창조과학부장관 또는 방송통신위원회가 그 시정을 명할 수 있고, 통신사업자가 이를 따르지 않으면 제104조 제4항에 의해 1천만원 이하의 과태료 부과처분을 받는다. 또한 제3조 제1항 위반인 경우 제95조 제1호에 의해 3년 이하의 징역 또는 1억5천만원 이하의 벌금으로 처벌된다. 제50조 제1항을 위반하는 경우 제52조에 의해 방송통신위원회는 금지행위의 중지 등 시정명령을 내릴 수 있고, 제53조에 의해 매출액의 100분의 3 이하에 해당하는 금액을 과징금으로 부과할 수 있다. 특히 제50조 제1항 제1호의 위반에 대해서는 제99조에 의해 3억원 이하의 벌금으로 처벌되기도 한다.

전기통신사업법 제99조는 "이용자의 차별적 취급"을 금지하는 것이며 통신비밀보호법 제16조는 "통신의 비밀"을 보호하기 위한 것이다. 그러므로 형법적 관점에서 합리적인 이유 없는 선별적 송·수신 방해는 통신비밀보호법 제16조 위반과 전기통신사업법 제99조 위반의 경합범이 성립하는 것으로 볼 수 있다. 그러나 모든 이용자의 특정 서비스에 대한 송·수신 방해는 이용자에 대한 차별적 취급으로 보지 않을 가능성이 있으며, 또한 경쟁 사업자의 망 이용에 대한 취급은 비용부담의 관점에서 정당화 될 가능성이 높은 것으로 보인다.

망을 통해 전송되는 "정보"와 "비밀"을 보호하는 구성요건으로는 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제49조가 있다. 이 규정은 "누구든지 정보통신망에 의하여 처리·보관 또는 전송되는 타인의 정보를 훼손하거나 타인의 비밀을 침해·도용 또는 누설하여서는 아니 된다"고 선언하고 있다. 이 규정을 위반하면 같은 법 제71조 제11호에 의해 5년 이하의 징역 또는 5천만원 이하의 벌금으로 처벌된다. 만약 망 관리자가 망 중립성 원칙을 위반하여 맞춤광고를 하기 위한 목적으로 자신의 망을 통해 전송되는 패킷에 내용을 변조하는 행위를 하는 경우 타인의 정보에 대한 "훼손"이 되어 이 구성요건에 해당하는 것으로

---

40) 제50조(금지행위) ① 전기통신사업자는 공정한 경쟁 또는 이용자의 이익을 해치거나 해칠 우려가 있는 다음 각 호의 어느 하나에 해당하는 행위(이하 "금지행위"라 한다)를 하거나 다른 전기통신사업자 또는 제3자로 하여금 금지행위를 하도록 하여서는 아니 된다. 1. 설비등의 제공·공동활용·공동이용·상호접속·공동사용·도매제공 또는 정보의 제공 등에 관하여 불합리하거나 차별적인 조건 또는 제한을 부당하게 부과하는 행위 (중략) 5. 이용약관(제28조제1항 및 제2항에 따라 신고하거나 인가받은 이용약관만을 말한다)과 다르게 전기통신서비스를 제공하거나 전기통신이용자의 이익을 현저히 해치는 방식으로 전기통신서비스를 제공하는 행위 (후략).

볼 수도 있을 것이다.

그러나 이 구성요건은 행위객체를 "정보"와 "비밀"로 구분하고 있기 때문에, 해석상 여기서 말하는 비밀은 단지 남에게 알려지지 않았다는 표지만으로는 부족하며, 따라서 알려지지 않아야 할 비밀가치가 구체적으로 침해되는 경우에만 적용 될 수 있을 것으로 생각한다.[41] 이 경우 타인에 의한 내용의 지득 없는 자동화장치를 통한 패킷 분류가 비밀의 침해에 해당하는지가 모호해질 여지가 있다. 게다가 전송중인 타인의 통신 내용을 침해하는 경우는 통신비밀보호법이 이 법에 대하여 법조경합 중 특별관계에 있는 것으로 보아야 한다. 그러므로 이 글은 구성요건 해당성이 보다 명확한 통신비밀보호법상 불법감청 구성요건으로 논의의 대상을 한정하고자 한다.[42]

제2절 국내의 망 중립성 침해 사례

물론 최근 망 중립성과 관련하여 "법적" 분쟁이 전혀 없었던 것은 아니다. 오히려 망 중립성 정책을 둘러싼 극심한 이해관계의 충돌로 인하여, 최근 몇 년간 크고 작은 분쟁이 지속적으로 발생하고 있다. 그런데 명확한 망 중립성 관련 정책이 아직 제시되지 못하고 있으며, 이에 기반한 구체적이고 보편적인 규범적 기준을 찾지 못하였기 때문에 이해관계의 충돌은 대체로 통신사에게 유리한 방향으로 결론내려지고 있는 것이 현실이다. 모호한 망 중립성 정책이 네트워크를 지배하고 있는 통신회사에 의해 불법 조각사유로 원용되고 있는 것이다. 이와 관련하여 가장 대표적인 분쟁 사례인 스마트 TV 차단 사건과 mVoIP 차단 사건의 사례를 통해 우리나라의 선별적 인터넷 접속 방해 행위에 대한 논의 현황을 살펴본다.

41) 그렇지 않은 정보의 경우 개인정보인 경우에만 개인정보보호법으로 보호된다.

42) 전기통신사업법과 정보통신망 이용촉진 및 정보보호 등에 관한 법률 위반에 관해서는 제4장에서 정당화 사유를 검토함에 있어 필요한 범위 내에서 서술한다.

1. KT의 삼성전자 스마트 TV 차단

가. 사건의 경과

2012년 2월 스마트 TV가 인터넷 트래픽을 과도하게 발생시킨다는 이유로 삼성 스마트 TV에 대한 인터넷 접속제한조치를 시행한 바 있다.[43] 이로 인해 KT 초고속 인터넷 가입자 약 782만명 중 삼성 스마트 TV 이용자 약 2만 4000명의 스마트 TV를 이용한 인터넷 접속이 5일간 차단되었다. KT 측은 이 차단조치에 앞서 법률검토를 마쳤으며[44] 약관에 근거한 적법한 조치라고 주장하였다. 그러나 이번 사건으로 통신사들이 특정 서비스를 겨냥해 언제든 임의로 네트워크를 차단할 수 있다는 사실이 확인되었으며, 컨텐츠 및 서비스 제공 기업과 통신기업 사이의 갈등이 표면화되는 계기가 되었다.

망 중립성 정책에 공동대응하기 위하여 '구글코리아', '다음커뮤니케이션', '야후코리아', 'NHN' 등 인터넷 컨텐츠 및 서비스 사업자들이 모여 결성한 협의체인 오픈인터넷협의회(Open Internet Alliance; OIA)는 KT의 삼성 스마트 TV 접속 차단 조치는 망 중립성 가이드라인에 대한 명백한 위반이라고 의견을 밝혔다. 2011년 채택된 망 중립성 가이드라인에 따르면 인터넷 접속제공사업자는 합법적인 컨텐츠, 애플리케이션, 서비스나 망에 위해가 되지 않는 장치를 차단해서는 안 된다고 규정하여 통신사에 대해 차단금지 의무를 명시적으로 선언하고 있으며, 따라서 KT의 접속 차단 조치는 이 같은 의무를 위반해 합법적 기기 접속에 대한 이용자의 기본 권리를 침해한 행위라는 것이다.[45]

나. 배 경

추후 조사에 따르면 당시 삼성 스마트 TV 서비스를 제공하는 서버의 하루 평균 데이터 통신 량은 불과 50GB 정도에 그쳤으며, 이는 KT의 인터넷 서비스에

43) 연합뉴스 2012년 2월 9일자 "KT "스마트TV 연결 인터넷망 즉시 차단"(1보)" 참조.
44) 아시아경제 2012년 2월 9일자 "김효실 KT 상무 "법률검토 마쳤다"" 참조.
45) 파이낸셜, 2012년 2월 16일자, "OIA "KT, 삼성 스마트TV 접속 차단 망 중립성 위반""

장애를 야기하기에 턱없이 부족한 트래픽 수준이었던 것으로 드러났다. 그럼에도 불구하고 KT가 전격적으로 삼성전자 스마트 TV의 인터넷 접속을 차단한 조치를 단행한 배경에는 국내 거대 기업 간의 이익 다툼이 있었다. 국내 통신 시장의 거의 대부분을 장악하고 있는 통신 3사(KT, SKT, LG U+)는 이미 2011년부터 스마트 TV 제조회사인 삼성전자와 LG전자 측에 망 사용료를 지불할 것을 요청하였고, 정부의 망 중립성에 대한 입장이 명확하지 않다는 이유로 삼성전자측이 협상을 거부함에 따라 KT측이 전격적으로 인터넷 접속을 차단하게 된 것이다. 스마트 TV 제조사 측은 즉각 KT의 조치가 부당하다는 입장을 밝혔고, PC에서 이용하는 고화질 동영상 스트리밍 서비스나 IPTV 등과 비교하여 형평성에서 어긋난다고 주장했다.[46] 이에 삼성전자는 서울중앙지방법원에 KT의 스마트 TV 인터넷 접속 차단을 막아달라는 가처분을 신청했으며, 당시 방송통신위원회는 법 위반여부를 검토하여 엄중하게 제재하겠다고 밝힌 바 있다.[47]

다. 방송통신위원회의 결정

그러나 3개월이 지난 5월 4일 방송통신위원회는 "이용약관과 달리 삼성 스마트 TV 가입자의 인터넷 접속을 제한하고 접속제한 시 이용제한 일시 및 기간 등을 사전통지하지 않은 행위"가 전기통신사업법 제50조 제1항 제5호[48] 후단 및 같은 법 시행령 제42조[49]의 규정을 위반하여 이용자의 이익을 침해한 것에 해당

46) 아시아경제 2012년 2월 9일자 "삼성·LG "KT, 스마트TV 차단 부당"" 참조.

47) 디지털 데일리 2012년 2월 10일자 "삼성전자, KT 스마트TV 접속차단에 가처분 신청으로 맞불" 참조.

48) 제50조(금지행위) ① 전기통신사업자는 공정한 경쟁 또는 이용자의 이익을 해치거나 해칠 우려가 있는 다음 각 호의 어느 하나에 해당하는 행위(이하 "금지행위"라 한다)를 하거나 다른 전기통신사업자 또는 제3자로 하여금 금지행위를 하도록 하여서는 아니 된다. (중략) 5. 이용약관(제28조제1항 및 제2항에 따라 신고하거나 인가받은 이용약관만을 말한다)과 다르게 전기통신서비스를 제공하거나 전기통신이용자의 이익을 현저히 해치는 방식으로 전기통신서비스를 제공하는 행위.

49) 제42조(금지행위의 유형 및 기준) ① 법 제50조제3항에 따른 금지행위의 유형 및 기준은 별표 4와 같다. ② 방송통신위원회는 특정 전기통신 분야 또는 특정 금지행위에 적용하기 위하여 필요하다고 인정하는 경우에는 제1항에 따른 금지행위의 유형 및 기준에 대한 세부기준을 정하여 고시할 수 있다. (별표 4의 내용 중 5. 마. 1)은 "전기통신서비스의 요금, 번호, 전기통신설비 또는 그 밖의 경제적 이익 등을 다른 이용자에 비하여 부당하게 차별적으로 제공하거나 이를 제안하는 행위"를 부당한 이용자 차별에 해당하는 행위로 본다.)

하므로 KT의 삼성전자 스마트 TV 차단행위는 위법하다고 판단했다.[50] 망 중립성 원칙에 대한 판단은 유보한 채, KT가 망 이용 대가 협상에 계속 임하고 있는 LG전자의 스마트 TV는 인터넷 접속을 차단하지 않았기 때문에 이용자 차별에 해당한다고 본 것이다.

하지만 방송통신위원회는 당초 엄중 제재방침을 밝힌 것과는 달리 망 중립성 논의가 아직 진행 중이며, 망 구축 비용 부담 문제에 관하여 논의 중에 있으므로 사회적 합의를 통해 현행 법령이 개정될 가능성이 있다는 점, 그리고 KT가 접속 제한조치를 조기 해제해 이용자 피해규모가 크지 않은 점 등을 고려해 법 위반에도 불구하고 단순 경고 조치를 처분하는데 그쳤다. 이 사건과 관련하여 방송통신위원회 관계자는 당시 언론 인터뷰를 통해 "과징금이나 더한 제재를 가할 경우 시장에 잘못된 시그널을 줄 수 있다"고 밝혀 선택적 접속 차단 자체를 문제삼고자 하는 것이 아님을 분명히 밝혔다. 이러한 분위기 속에서 2013년 6월 26일에는 KT의 회장이 기자회견을 통해, 유튜브 등 특정 서비스를 거론하면서 "네트워크 트래픽을 규격화하고 과부하를 불러일으키는 사업자에게는 별도 요금을 부과해야 한다"고 말하여 망 중립성에 관한 논란이 다시 제기되기도 하였다.[51]

2. mVoIP 차단

가. 사건의 경과

2012년 6월 4일 카카오톡의 모바일 인터넷 전화(mobile Voice over Internet Protocol; mVoIP)[52] 서비스인 "보이스톡 베타서비스"를 개시하며 망 중립성 관련 논의가 확산되었다.[53] 우리나라 이동통신사들은 이미 2009년 스마트폰이 보

50) 뉴시스 2012년 5월 4일자, "방통위 "KT 삼성 스마트TV 접속 차단 위법이나 경고"" 참조.

51) 한겨레, 2013년 6월 26일자, "망 과부하 초래 사업자에 추가비용 받아야" 참조.

52) 상세한 법리적 분석은 장윤정, m-VoIP 서비스에서의 망 중립성에 대한 법적 검토, Ewha Law Review 제2권 제2호, 2012, 27쪽 이하 참조.

53) 방송통신위원회는 2012년 7월 13일 "통신망의 합리적 관리 및 이용에 관한 기준(안)"에 mVoIP에

급되고 스카이프, 바이버 등의 외국산 mVoIP 서비스가 활성화되기 시작할 당시부터 여러 가지 기술적 수단을 동원하여 이를 차단해 왔으나[54], 국내 mVoIP 서비스 이용자의 절대적인 수가 많지 않아 문제가 수면 위로 떠오르지 않았다. 그러나 카카오 보이스톡을 계기로 mVoIP에 대한 인식이 확산됨에 따라 관련 논의도 함께 증폭된 것이다.

이 사건을 통해 인터넷 접속 서비스를 제공하는 통신기업과 컨텐츠를 제공하는 인터넷·포털 기업 사이의 대립 구도 속에서 유선 인터넷을 중심으로 전개되던 망 중립성 논쟁이 무선 통신 분야로 넘어가게 되면서 비로소 이용자의 인터넷 이용에 대한 권리라는 관점이 조금 더 부각되게 되었다.[55] 특히 이 문제는 지난 대통령 선거를 위한 선거운동기간에 확산됨으로써 대통령 선거 주요 쟁점으로 부각되었다. 정치권의 압박으로 인하여 결국 이동통신사들은 새로운 요금제를 신설하였고, 요금제에 따라 제한된 용량을 mVoIP로 사용할 수 있도록 부분적으로 허용되었다.

그럼에도 불구하고 카카오 보이스톡의 트래픽 손실률 등으로 미루어 짐작하건데, 우리나라의 SKT와 KT는 여전히 의도적으로 mVoIP를 위한 데이터 통신을 기술적으로 선별하여 품질을 낮추고 있는 것으로 의심받고 있는 것이 현실이다. 카카오톡이 자사의 서비스 이용 현황을 기반으로 통계를 만들어 발표하고 있는 mVoIP 서비스 데이터 현황 기상도[56]에 따르면 2013년 11월 23일 현재 SKT와 KT는 대략 10% 이상의 패킷 손실률을 보이고 있는데, 이는 일본이나 미국에서 카카오 보이스톡에 접속하는 경우보다 무려 10배 이상 높은 수치이다. 반면 LG U+는 대략 0.6% 이하의 패킷만이 손실되고 있다. 이는 논리적으로 SKT와 KT가 인위적 수단을 투입하여 카카오 보이스톡 서비스 이용만을 선별적으로 식별하여 차단하고 있음을 의미한다.[57] 카카오톡 홈페이지에 따르면 음성 데이터의 특성

관한 내용을 포함하여 발표하는 계기가 되었으며, 이로 인해 기준(안)에 대하여 합의를 이루지 못하고 논란이 오히려 촉발된 면이 있다. 기준(안)의 내용에 관한 상세한 해설은 제4장 참조.

54) 아시아경제, 2009년 4월 7일자, "이통사 vs 인터넷 업계 '공짜 전화' 격돌" 참조.

55) 전자신문, 2012년 9월 17일자, "모바일 인터넷전화(mVoIP) 허용 논란" 참조.

56) 카카오톡 홈페이지(http://www.kakao.com/services/talk/voices) 참조.

57) 2013년 4월 9일자, 이투데이 "이통사, 인터넷 무료통화 확대…보이스톡 품질불량은 그대로?" 참조.

상 기술적으로 손실률이 10%가 넘으면 사실상 음성으로의 복원이 불가능하여 통화가 거의 불가능하게 된다고 한다. SKT와 KT의 차단 비율은 사실상 통화가 불가능해지는 수준으로 의도적으로 맞춰져 있는 것으로 추정된다.

나. 경제적 트래픽 관리

이에 관하여 2013년 10월 10일 미래창조과학부 주관 정보통신정책연구원에서 주최로 열린 "통신망의 합리적 트래픽 관리기준 마련을 위한 토론회"에서 SKT 정태철 상무는 "경제적 트래픽 관리 차원"에서 mVoIP을 차단하고 있다고 밝힌 바 있다. 즉, mVoIP이 유발하는 트래픽 양이 유무선 인터넷에 미치는 영향은 크지 않지만, 이동통신사의 음성통화를 대체하는 경쟁서비스가 될 수 있기 때문에 통신회사의 음성통화 매출이 줄어들 것을 우려하여 의도적으로 차단하고 있다는 것이다. 즉, 현재 최소한 SKT와 KT는 자사의 이동통신망에서 그 외의 다른 법률적 근거나 합리적 이유가 없음에도 불구하고 오로지 기업의 경제적 이익을 극대화하기 위하여 인터넷 이용을 선택적으로 "전기통신의 송·수신을 방해"하고 있음을 확인할 수 있다.

음성통화요금은 일반적으로 초당 1.8원이고 이를 환산하면 시간당 6,480원이 부과된다. 이에 반해, mVoIP 서비스 제공자들이 밝힌 mVoIP의 데이터 소모율은 분당 약 0.4~0.6MB여서 시간당 약 24~36MB가 소요되며 이를 일반적인 데이터 요금으로 환산하면 시간당 약1,224~1,836원이 데이터 이용 요금으로 부과된다고 한다. 게다가 통신사가 만든 음성·데이터 통합 요금제에 포함된 기본제공 데이터량 중 매월 소진하지 못하고 사라져버리는 부분[58]을 이용하는 경우라면 추가적인 부담을 최소화할 수 있다. 더욱이 국제전화를 이용하는 경우라면 평균적으로 요금이 가장 싼 미국을 기준으로 계산하더라도 음성통화를 이용하는 경우 국제전화 사업자별로 국제전화 요금이 분당 100원에서 200원이 추가되기 때문에, 결과적으로 이용자는 시간당 음성통화 요금에 추가로 6,000~12,000원의 국제전

58) 우리나라 통신사의 음성·데이터 통합요금제는 대부분 사용자로부터 일정 금액을 받고 미리 정한 음성과 데이터 통화량을 매월 제공하는 형식으로 계약되며, 월중 소진하지 못한 부분은 이월되지 않고 사라지도록 되어있다.

화 요금을 더 부담해야 한다.[59] 우리나라의 이동통신회사들은 대체로 자회사를 통해 국제전화 서비스까지 유료로 제공하여 수익을 거두고 있다.

다. 공정거래위원회의 판단

이동통신사의 mVoIP 차단에 관하여 이미 2011년 시민단체가 이동통신사를 공정거래위원회에 제소한 바 있다. 그러나 2013년 7월 17일 공정거래위원회는 아직 망 중립성과 관련하여 명확한 정책적 판단이 내려지지 않은 상황에서 법률위반 여부를 판단하기는 불가능하며, 또한 이동통신사들이 음성 무제한 등 새로운 요금제를 출시하였고, 최근에는 일부 저가 요금제에 대해서도 mVoIP을 허용하고 있기 때문에 소비자 후생저하효과를 인정하기 어렵다고 판단하여 무혐의 처분을 내렸다.[60] 그러나 통신사들은 mVoIP을 허용하는 요금제에서도 요금수준에 따라 용량의 제한을 설정하고 있다. 이 말은 통신사가 이동전화 가입자가 자사의 통신망을 이용해 전송하는 모든 패킷을 실시간으로 식별, 분류하여, 그 중 mVoIP으로 추정되는 패킷의 양을 측정하고 있으며, 지정한 용량을 초과하는 순간 송·수신을 방해한다는 것을 의미한다. 즉, 통신사는 자동화된 설비를 이용하여 가입자의 스마트폰 데이터 통신 내역을 항상 감시하고 있으며, 통신사가 원치 않는 방식의 데이터 사용이 식별되면 언제든지 이를 차단할 수 있다는 것이다. 그래서 공정거래위원회의 판단이 대기업의 일반 소비자에 대한 거래상 지위남용행위 중 불이익 제공행위이며, 소액 요금제에서는 여전히 mVoIP 이용이 전면 금지되고 있다는 점을 간과한 잘못이 있다는 이유를 들어, mVoIP이 차단된 요금제를 사용한 이용자들은 2013년 9월 30일 서울중앙지방법원에 SKT와 KT를 상대로 손해배상을 청구하는 소를 제기하여 심리중이다.

---

59) 요금에 대한 계산은 mVoIP 차단을 이유로 2013년 9월 30일 서울중앙지방법원에 손해배상을 청구한 소장에서 인용함.

60) 전자신문, 2013년 7월 17일자 "공정위, 이통사 mVoIP 차단 관련 무혐의 결론" 참조.

제3절 형법적 접근의 필요성

1. 규범과 현실의 괴리

가. 규범 인식의 부재

통신사의 삼성전자 스마트 TV와 mVoIP 서비스에 대한 접속차단 사례에서 알 수 있듯이, 망 중립성을 둘러싼 분쟁들은 행정법적 또는 민사법적 프레임에서 보면 통신사의 선택적 송·수신 방해행위는 기업과 기업 또는 기업과 개인 사이의 단순한 비용전가의 문제인 것처럼 보이기도 하는 것이 사실이다. 그래서 망 중립성 원칙은 망 관리자가 컨텐츠 제공자에게 망 이용에 대한 비용을 부담하게 하거나, 통신서비스 가입자에게 더 비싼 요금을 과금할 수 있는 서비스를 사용하도록 강제하게 만드는 통신사의 영업전략[61]을 어디까지 허용하는 것이 공정한 것인가에 관하여 정부의 규제수준을 정하는 문제로 이해되기도 한다. 정부의 규제가 산업의 발전을 위축시킨다는 신자유주의적 주장은 바로 이러한 관점에 서 있는 것이다. 그래서 현재까지 망 중립성 정책과 관련하여 국내에서는 이동통신사의 시장지배력의 남용문제와 통신망 개방의 범위가 주된 관심사였다.[62]

아직 우리사회는 망 중립성에 대하여 장기적인 관점에서 규범적 고려가 전제된 객관적인 원칙을 보편적 기준으로 받아들이지 못하고 있다. 그래서 선별적 통신 차단문제에 관하여 결정을 내려야 했던 방송통신위원회나 공정거래위원회는 해당 사안을 단기적이고 미시적이고 개별적인 손익형량의 문제로 볼 수밖에 없었으며, 다른 이용자와의 차별대우 또는 소비자 후생 감소 여부를 결정의 근거로 제시한 것이다. 또한 그렇기 때문에, 우리나라에서 망 중립성 저해행위에 대한 분쟁은 대부분 상대적 강자인 통신회사에 유리한 방향으로 정리되고 있다. 네트워크 운영과 관리에 관한 권한과 정보를 독점하고 있는 통신사는 언제나 자

61) 김성환, 망 중립성의 개념과 쟁점의 이해, 정보통신포럼 2007, 법원사, 2008, 80면.

62) 임규철, 망 중립성, 비교법연구 제11권 제2호, 2011, 39면. 이러한 과정에서 소비자의 권리 보호를 위한 이용자의 인터넷 접속권이나 무차별성 보장은 부차적인 논의대상이었다. 그러나 이 문제는 기업과 기업 간의 이해관계에 그치지 않는다. 가장 큰 피해자는 바로 일반 시민이 될 수 있다는 데에 문제의 심각성과 논의의 필요성이 있다.

신에게 유리한 방향으로 망 관리 방법을 선택하고 있으며, 이에 관련한 정보는 객관적인 원칙, 즉 법률을 통해 강제하지 않는 한 자신들에게 유리한 것만을 선택적으로 공개한다. 게다가 통신사들은 막대한 자금력을 동원하여 자신들의 이윤을 극대화하기 위해 만든 요금제와 망 관리 수단의 "공정성"과 "정당성"을 적극적으로 홍보하고 있는 것이 사실이다. 이익형량 다툼에서 통신사의 수천억에 달하는 영업이익에 비해 가입자의 몇 천원에 이하에 불과한 추가비용부담은 항상 작은 것으로 보이며, 소소하게 분산된 망 중립성 원칙 지지 측의 이해관계에 비해, 독과점의 지위를 유지하고 있는 통신사의 망 중립성 반대의 이익은 너무나도 크다. 통신시장의 이러한 현실은 구조적으로 규범적 판단을 가로막는 원인이 된다. 이러한 현상은 법이론적으로 다음과 같이 분석할 수 있을 것이다.

나. 구조적 분석 - 보편적 규범의 부재와 이해관계의 충돌

① 너무나도 빠른 정보통신기술의 발전으로 하루가 다르게 등장하고 있는 새로운 현상들은 각자의 이해관계에 직접적인 영향을 주는 현실의 변화를 초래하지만, 이를 둘러싸고 서로의 이해가 충돌하는 경우 이를 어떻게 해결하는 것이 정당한 것인지, 즉 사회의 구성원으로써 해도 되는 것과 해서는 안 되는 것을 판단하는 기준이 되는 규범의 대응 속도는 현실의 변화를 쫓아가지 못할 수밖에 없다.[63] 망 중립성에 대해서도 규범적 가치기준이 사회의 법 인식에 아직 보편적으로 자리 잡지 못하고 있는 것이다. 행위기준으로 삼을 만한 보편적 규범을 찾을 수 없는 관련 당사자들은 자신의 이해관계에 따라 행동하게 된다.

② 그런데 현실에 대한 규범적 인식의 틀이 되는 가치기준이 아직 보편적으로 승인되지 않은 상황에서, 통신사의 선별적 인터넷 접속 차단처럼 직접적이고 가시적인 손해가 즉시 야기되지 않는 경우, 또는 권리의 침해가 발생했다는 사실을 당사자가 인지조차하기 어려운 경우에는 해당 행위에 대한 규범적 평가가 자리 잡기가 훨씬 더 어려울 수밖에 없다. 통신사의 선택적 접속 차단은 충분히 알려지지 않은 채 통신사가 장악하고 있는 네트워크상에서 기술적으로 이루어지

63) 기술발전과 법인식의 간극으로 인한 규범의 부재 현상에 관한 분석은 전현욱, 개인정보 보호에 관한 형법정책, 고려대학교 박사학위논문, 2010, 53-55쪽 참조.

며, 가입자가 겪는 불편을 통해 추정할 수 있을 뿐이다. 또한 망 중립성을 저해하기 위해 사용하는 기술의 작동 구조나 이를 위해 침해되는, 또는 침해될 것으로 추정되는 가입자의 프라이버시에 대한 정보는 통신사에 의해서 적극적으로 은폐된다. 그렇기 때문에 우리 시민 사회는 아직 선택적 인터넷 차단 행위를 감청이라는 규범적, 거시적 관점에서 바라보지 못하고 있다.

③ 규범적 인식 부재는 보다 적극적인 이해관계의 추구로 이어질 수밖에 없다. 그래서 당사자들은 자신의 이익을 보다 극대화하기 위해 행위방향을 설정하며, 따라서 인터넷을 통한 정보의 전송과 관련하여 기업과 기업, 기업과 개인 등 관련 당사자의 이해관계 충돌가능성은 훨씬 높아졌다. 이러한 상황에서 이해관계에 보다 민감한 쪽, 즉 망 이용의 대가가 주된 수입원인 통신사의 이익추구가 보다 적극적일 수밖에 없으며, 그래서 통신사는 경제적으로 조금이라도 불리한 내용의 통신을 최대한 찾아내서 차단하고자 한다. 이러한 과정에서 역시 스마트 TV 제조사나 mVoIP 서비스 제공자처럼 이해관계가 직접 침해된 컨텐츠 및 서비스 제공 기업이 가장 먼저 통신사의 망 중립성 저해행위에 대하여 문제를 제기하였던 것이다. 이때 인터넷 서비스 제공자나 컨텐츠 사업자 모두 “공정경쟁”을 주장했다는 사실은 공정함에 대하여 서로 승인할 수 있는 기준이 아직 자리잡지 못하였다는 점을 방증하고 있는 것으로 보인다.

④ 그러나 이 문제를 해결해야 할 것으로 기대되는 권한 있는 행정기관은 정작 이해관계의 충돌을 해결할 수 있는 규범을 발견하지 못하고 있다. 규범적 인식이 결여된 상태에서 이해관계의 충돌이라는 프레임에 갇힌 시각으로는 보편적이고 객관적인 기준에 의거한 정당한 해결책을 제시하는 것에 실패할 수밖에 없는 것이다. 오히려 망 중립성 정책을 제시해야 하는 미래창조과학부 역시 이해관계 충돌 프레임 속에서 다양한 당사자들의 의견을 모으는데 에너지를 소진하고 있는 것으로 보인다. 그래서 우리나라는 2011년 12월 망 중립성 및 인터넷 트래픽 관리에 관한 가이드라인을 선언해 놓고도 여전히 “합리적 트래픽 관리”에 대한 구체적이고 세부적인 기준을 제시하는데 실패하고 있다.[64]

⑤ 이러한 이유로 망 중립성을 둘러싼 분쟁을 이해관계의 충돌로 바라보는

64) 합리적 트래픽 관리기준에 관하여는 제4장에서 상술한다.

한, 결국 더 힘이 강한 자, 즉 네트워크를 장악하고 있는 통신회사의 이해관계가 관철될 가능성이 높다. 모호한 망 중립성 원칙이 오히려 강자의 면죄부 또는 불법 조각사유 되기도 하는 것이다. 오히려 이러한 가운데에서 망 중립성의 논의 속에는 상대적 약자인 시민의 기본권이 적절하게 고려되고 있지 못한 실정이다. 심지어 이미 망 중립성에 대한 기본 원칙을 선언하고 있는 전기통신사업법과 가이드라인의 내용을 의도적으로 축소하는 새로운 기준에 대한 논의가 전개되는 웃지 못할 일도 벌어졌던 것이 현재 우리나라 망 중립성 정책의 현실이다. 이러한 이유로 망 중립성 보호의 관점에서 보면 상당히 잘 만들어진 통신비밀보호법상 감청 금지 규정에도 불구하고 우리나라의 인터넷 서비스 제공자들은 상당히 폭넓은 자유를 가지고 컨텐츠를 동등하게 취급하지 않는 것으로 보인다.

2. 논의 방향의 전환 – 망 관리에서 망 이용자의 권리로

이처럼 단순한 단기적 손익분배, 또는 망 유지·개선의 비용분담 차원의 이해는 망 중립성 원칙의 규범적 실질을 파악하고 미래를 위한 정책의 방향을 제시하는데 도움이 되지 않을 뿐만 아니라, 때로는 특정한 이해관계의 입장에서 이를 방해하는 원인이 되기도 한다. 객관적이고 보편적 가치기준이 분명하지 않은 곳에서 각 당사자의 손해와 이익을 평가하고 이를 서로 비교하는 것은 애초에 실패할 수밖에 없는 일이다. 그러나 우리는 통신의 비밀에 관하여 이미 사회 구성원으로서 이미 최소한의 넘어서는 안되는 선에 대한 규범적 가치기준을 가지고 있다. 단지 이 규범을 선별적 인터넷 차단 행위에 연결시키지 못하고 있을 뿐이다. 이는 망 관리라는 관점은 인터넷이 바로 의사소통을 위한 수단이라는 사실을 적절하게 드러내지 못하기 때문이다. 그러나 망 이용자의 권리라는 측면에서 바라보면 통신비밀의 관점에서 망 중립성을 바라볼 수 있게 된다.

인터넷의 본질은 “관리”에 있는 것이 아니라 “정보의 전달”에 있다. 현대 정보사회에서 자유롭게 인터넷에 접속하여 정보를 소통하는 것은 가장 중요한 시민의 자유권적 기본권이며 표현의 자유를 구체적으로 실현하기 위한 전제조건이기 때문에 민주적 공론장 형성에 없어서는 안 되는 필수적인 요소이다.[65] 하버마스

(Habermas)에 의하면 공론장이란 여론의 형성을 통해 시민과 권력을 연결시켜 주는 것으로, 적절하게 기능하기 위해서는 모든 시민들의 참여하여 자유롭게 의사소통을 할 수 있어야 한다.[66] 오늘날 상당부분의 정보 획득과 의사표현이 바로 인터넷을 통해 이루어지고 있다는 사실을 고려하면, 인터넷을 통한 정보 소통에 대한 개입과 간섭, 즉 "송·수신을 차단하는 것"은 기본권에 대한 심각한 침해가 될 뿐만 아니라, 우리사회의 민주적 발전을 저해하는 중대한 범죄가 될 것이다.

그런데 우리는 역사적으로 통신의 자유에 대한 부당한 침해를 경험한 적이 있으며, 이러한 경험에 대한 가슴 아픈 반성을 담아[67] 통신비밀보호법을 제정하였다. 그래서 사생활의 비밀과 통신의 자유에 대한 강력한 보호가 필요하다는 사회적 합의[68]는 현재 통신비밀보호법에 매우 강력한 형사처벌 구성요건으로 남아 있다. 더욱이 상술한 바와 같이 우리의 통신비밀보호법상의 감청에 대한 개념정의는 정보처리장치를 통한 자동화된 감청도 충분히 포섭할 수 있도록 규정되어 있다. 다만 현재 정보기술의 발전으로 인하여 통신의 방식이 음성 중심에서 데이터 기반으로 변화하고 있는 지금, 규범으로부터 행위방향을 설정하는 과정에서 규범과 현실의 인지부조화를 겪고 있는 것일 뿐이다. 그렇기 때문에, 우리는 이미 가치에 대한 기존의 사회적 합의와 전통적인 법치국가 형법원칙에 근거하여 망 중립성과 관련된 분쟁에 대한 정당한 해결방안을 논증할 수 있을 것이다.

물론 그 과정에서 이미 현실의 변화의 정도가 패러다임을 바꿀 정도에 이르렀기 때문에 이에 상응하여 가치기준을 바꿀 필요가 있다는 사실이 적절하게 논증된다면, 통신비밀보호법의 개정이나 데이터 통신의 감청에 관한 특별법의 제정

---

65) 민주적 공론장과 망 중립성에 관한 상세한 논의는 Francesca Musiani/Maria Löblich, Net Neutrality from a Public Sphere Perspective, The Value of Network Neutrality for the Internet of Tomorrow, (원문은 Dynamic Coalition on Network Neutrality 홈페이지 http://nebula.wsimg.com/c65488b3edff49adc2dba84e344591bd?AccessKeyId=B45063449B96D27B8F85&disposition=0), 2013, 36-43쪽 참조.

66) 1984, 49쪽; 공론장에 관한 하버마스의 분석에 관한 해설은 이상돈/홍성수, 법사회학, 박영사, 2000, 160쪽 이하 참조.

67) 박상천 의원 외 93인, 통신비밀보호법안, 1993. 5, 2쪽.

68) 국회정치관계법심의특별위원장, 통신비밀보호법안(대안), 1993. 12, 1쪽.

을 논의할 수도 있을 것이다. 그러므로 망 중립성의 정책방향의 문제는 이해관계의 충돌이라는 망 관리의 프레임에서 벗어나, 망 이용자의 권리라는 중대한 기본권 침해, 즉 법익보호에 관한 형사정책적 관점에서 논의하면 비로소 분명해진다고 할 것이다.

3. 선별적 접속 제한의 이중적 구조 - 감시와 방해

선별적 송·수신 방해는 크게 두 개의 행위로 나누어 이해할 수 있다. 우선 망 관리자는 자동화된 정보처리장치를 이용하여 ① 망을 통해 전송되는 모든 패킷의 패턴을 분석한다. 그 다음 분석된 내용을 토대로, 역시 자동화된 정보처리장치를 이용하여 ② 특정 패킷의 송·수신을 방해한다. 모든 인터넷 이용 내역에 대한 실시간 감시와 그 감시를 토대로 한 송·수신 차단이라는 통신제한조치가 동시에 일어나는 것이 망 중립성 저해행위인 것이다. 전자는 "통신의 비밀"을 침해하는 것이라고 할 수 있고, 후자는 "통신의 자유"를 침해하는 것이라고 할 수 있다.

가. 모든 인터넷 이용 내역에 대한 실시간 감시

상술한 바와 같이 망 중립성 정책은 통신비밀보호법상 불법감청 구성요건, 즉 망 이용자의 권리침해와 법익보호의 관점에서 보면 보다 명백해진다. 그렇다면 과연 망 중립성 저해행위, 즉 통신사가 자사의 망을 통해 전송되는 컨텐츠의 유형을 식별하고 선별적으로 이를 방해하는 행위가 실제로 이용자의 통신비밀에 대한 권리를 침해하는지, 그리고 그 심각성이 형법적 보호가 필요한 정도라고 할 수 있는지, 아니면 데이터 통신과 자동화 기기의 특성으로 인하여 음성 통신에 대한 감청과는 근본적인 차이가 있는 것인지를 구체적으로 확인해 볼 필요가 있다.

모든 데이터를 패킷으로 분할하여 전송하는 인터넷의 기본적인 작동원리를 고려하면, 망 사업자가 자사의 망을 통해 전송되는 모든 패킷을 동등하게 취급하지 않는다는 것은, 결국 특정 목적으로 이용되는 패킷만을 기술적으로 식별해서

전부 또는 일부를 선택적으로 “방해”하는 것을 의미한다. 그런데 특정 목적 패킷을 선별적으로 취급하려면 논리적으로 당연히 전체 패킷 또는 최소한 전체 패킷 중에서 기술적으로 사용 패턴을 파악하고 구분하여 차단하기 위해 충분한 비율의 불특정 패킷을 식별해야 하며, 이는 이용자의 모든 인터넷 사용 내용에 대한 실시간 “감시”를 의미한다. 이용자가 인터넷을 이용해 무엇을 하고 있는지를 즉시 탐지해 낼 수 있어야, 특정한 서비스의 이용을 개시하는 순간 이를 방해할 수 있기 때문이다.

예컨대 이동통신사가 mVoIP 어플리케이션을 이용한 인터넷 음성전화 서비스만을 골라 차단하는 경우, 이동통신사는 사용자가 mVoIP 어플리케이션을 이용할 때에만 통신에 개입하는 것이 아니라, 단순한 웹서핑이나 이메일 전송, 동영상 스트리밍 등 가입자가 스마트폰과 이동통신망을 이용해서 송·수신하는 모든 패킷을 실시간으로 감시해야 한다. 그래야 mVoIP 패킷을 골라낼 수 있기 때문이다. 이는 실제 음성 통신에 대한 통신제한조치가 집행되는 경우에도 마찬가지인데, 피의자 또는 피내사자가 언제 범죄사실에 관한 통신을 할 것인지 미리 확정적으로 알 수는 없기 때문에, 통신비밀보호법상 통신제한조치는 최대 2개월의 이내에서 기간을 정하여 허가된다.[69]

나. 기간 제한 없는 통신제한조치

다만 음성통신에 대한 감청은 일반적으로 수사기관의 담당자가 실시간으로 내용을 청취하고 이를 지득할 것을 전제로 한 개념이라는 점에서 자동화된 정보처리기기를 이용하는 데이터 통신의 차별적 취급과는 차이가 있는 것이 사실이다. 그러나 법원의 통제 아래에서 제한적으로 열거된 중대범죄에 관한 수사목적을 달성하기 위하여 수사기관에 의해 한정된 기간만 인정되는 통신제한조치와 인터넷 서비스 제공자가 가입자의 모든 통신을 언제나 실시간으로 감시하는 것과는

69) 통신비밀보호법 제6조 제7항 통신제한조치의 기간은 2월을 초과하지 못하고, 그 기간 중 통신제한조치의 목적이 달성되었을 경우에는 즉시 종료하여야 한다. 다만, 제5조제1항의 허가요건이 존속하는 경우에는 제1항 및 제2항의 절차에 따라 소명자료를 첨부하여 2월의 범위안에서 통신제한조치기간의 연장을 청구할 수 있다

분명 논의의 지평이 전혀 다르다. 또한 상술한 바와 같이 통신비밀보호법상 음성 통신에 대한 통신제한조치 역시 내용의 지득 없는 송·수신 방해를 포함하는 것으로 해석해야 할 것이다. 그러므로 통신비밀보호법은 법리적으로 음성 통신과 데이터 통신 모두 차이 없이 규정하고 있는 것으로 보아야 한다. 그리고, 비록 현행 통신비밀보호법상 "통신제한조치"가 패킷 감청에 대해서도 적용될 수 있는지에 관해서는 논의의 여지가 있다 하더라도[70], 감청 금지규정은 당연히 데이터 통신에 대해서도 적용될 수 있다.

통신사업자가 패킷의 내용에 따라 선별적으로 접속을 제한하는 경우, 법원의 허가장 없이 가입자의 모든 통신 패킷을 기간 제한 없이 언제나 감시하고, 특정 목적의 통신 패킷을 구분해서 송·수신을 방해해야 한다. 이처럼 "감시"와 "방해", 이는 바로 통신비밀보호법상 감청의 구성요건에 정확하게 포섭되는 행위이다. 그러므로 이 외의 특별한 정당화 사유가 없는 한 통신사의 망 중립성 저해 행위는 바로 불법감청의 구성요건에 해당하며 이에 상응하는 불법행위가 된다고 할 것이다. 더 나아가 현대 정보사회에서 모든 인터넷 데이터 송·수신 내역에 대한 실시간 감시는 사실상 이용자의 프라이버시 또는 개인정보에 대한 자기결정권과 통신의 비밀에 대한 권리를 완전히 박탈하는 것과 다름없는 대한 심각한 침해이며, 인터넷 서비스 제공자가 이러한 권한을 이용하여 이용자를 실질적으로 지배하는 또 다른 빅브라더가 될 수도 있는 위험이 된다.

---

70) 통신비밀보호법상 통신제한조치가 패킷 감청에 적용될 수 없으며 적용되어서도 안 된다는 주장으로 오길영, 인터넷 감청과 DPI, 민주법학, 제41호, 2009, 391쪽 이하. 그러나 현행 통신비밀보호법을 문리적으로 해석하면, 통신제한조치가 음성 통신에만 제한되는 것으로 보기는 어려울 것으로 생각된다. 그러나 패킷 감청에 대한 통신제한조치 허가의 합헌성은 별개의 문제이며, 이 논문의 주장처럼 궁극적으로는 디지털 매체의 특성을 반영하여 "새 틀"을 짜는 것이 합리적인 해결방안이 될 것으로 생각된다. 이 연구보고서는 통비밀의 보호에 관한 것이며, 디지털 증거에 대한 통신제한조치는 이 글의 목적과 논의의 범위에서 명백히 벗어나므로, 관련 논의는 다음의 연구 기회로 미루기로 한다.

4. 망 중립성 원칙의 한계와 감청의 정당화 필요성

가. 데이터 통신의 특성 - 자동화된 정보처리

그러나 다른 모든 구성요건 해당행위들과 마찬가지로 통신비밀을 침해하는 행위도 기본권 제한의 일반원칙인 비례성 원칙[71]에 의해 정당화될 수 있다. 그러므로 선별적 인터넷 접속 차단행위에 대한 정당화의 기준과 한계를 확인하기 위해서는, 상술한 바와 같은 규범과 현실의 괴리가 발생하게 된 근본적인 원인과 과정에 대한 보다 깊이 있는 검토를 통해, 송·수신 방해로 인해 침해되는 법익과 이로 인해 달성하고자 하는 목표의 크기를 신중하게 평가하고 비교해야 할 것이다. 인터넷을 이용한 데이터 통신의 제한과 관련된 이해관계는 분명 본래 통신비밀보호법의 제정 배경이 되었던 음성기반의 통신과는 근본적으로 다른 특징이 있는 것이 사실이기 때문이다.

자동화된 정보처리장치를 통한 데이터 통신은 음성 통신에 비하여 타인에게 훨씬 광범위하고 심각한 피해를 야기할 수 있다. 인터넷은 타인의 법익을 직접 공격하는 도구로 이용되기도 하고, 특정 서비스의 단순한 과다 이용이 전체 통신망의 속도 저하를 야기하기도 한다. 그런데 이러한 피해는 사후적 대응을 통해 해결하는 것이 사실상 거의 불가능하기 때문에, 불법적이거나 부당한 목적의 인터넷 이용에 대한 사전 예방적 조치가 필수적일 수밖에 없다.[72] 그러므로 이러한 데이터 통신의 남용 행위에 대해서는 음성 통신과는 다른 차원의 기본권 제한조치가 필요하며, 보다 높은 수준의 기본권 제한을 요구하는 수단도 정당화될 가능성이 있다. 게다가 데이터 통신은 음성 통신과는 달리 정보처리기기에 의한 자동화된 제한조치가 가능하다. 즉, 정보처리절차를 적절하게 설계하면 통신 비밀의 실질적 침해의 정도를 최소화하면서 망 관리의 목표를 달성할 수 있게 되는 것이다.

---

71) 비례성 원칙의 의의 및 내용은 배종대, 보안처분과 비례성원칙, 배종대/김일수 편, 법치국가와 형법, 세창출판사, 1998, 46쪽 참조.

72) 예방적 조치(정보보안)의 필요성에 대한 분석은 본장 제4절에서 검토한다.

나. 인터넷의 효율적 운영

더욱이 인터넷은 기술의 발전과 자본의 투입 정도에 종속되는 유한한 자원이며 따라서 전체 이용자에게 합리적으로 배분되어야 한다. 물리적인 통신망은 이를 구축하고 유지하는 것에는 막대한 비용이 소요되기 때문에, 이 비용을 감당하고 새로운 기술개발을 위한 신규투자에 필요한 자금을 마련하기 위하여 망에 부하를 발생시키는 이용자에게 이에 비례하여 적절한 요금이 청구될 수 있어야 하는 것이다. 특히 최근 급격히 확산되고 있는 무선통신망은 전파자원의 희소성으로 인하여 이러한 측면이 더욱 강한 것이 사실이다.

하지만 데이터 통신의 자동성으로 인해 음성 통신과는 달리 소수의 이용자, 또는 컨텐츠 제공자가 막대한 트래픽을 발생시키는 것도 가능하다.

그러므로 현실적으로 누가 비용을 부담할 것인가, 즉 적절한 손익분배의 관점을 떠나서는 인터넷 자체가 유지·개선되기 어려울 수도 있는 것이다. 그래서 이렇게 만들어진 정보통신망은 공공재가 아니라 사유재라는 주장도 일견 설득력이 있다. 이러한 관점에서 통신망 구축을 위해 투여된 기술과 자본은 사적 재산권에 종속된 이윤추구의 수단이며, 따라서 처벌 위주의 단순한 법적 규제만으로는 효율성을 달성할 수 없다는 점 또한 고려되어야 한다.[73] 보편적으로 납득 가능한 규범을 확인하기 어려운 새로운 문제영역에서 제재를 통한 규범의 내면화는 달성하기 어려우며, 규범을 위반한 자는 처벌을 단지 손해로 받아들일 가능성이 높기 때문이다.[74] 특히 통신사가 금전적 제재를 받는 경우, 결국 통신사는 해당 제재에 소요되는 비용을 통신요금을 통해 이용자에게 전가하게 될 수밖에 없다는 주장도 현실적인 타당성을 갖는다.

그러므로 인터넷을 유지하고 효율적으로 운영하는 것은 통신 사업자뿐만 아니라 전체 인터넷 이용자의 효용을 높이기 위해한 것이기도 하다. 그래서 물리적인 통신망을 구축하고 소유하며 관리하는 인터넷 서비스 제공자의 트래픽 관리

73) 사회국가이념에 지향된 형법의 한계에 대해 자세한 내용은 이상돈, 법학입문, 법문사, 2009, 262쪽 이하 참조.

74) 이러한 관점에 대한 상세한 설명은 전현욱, 개인정보 보호에 관한 형법정책, 고려대학교 박사학위논문, 2010, 26쪽.

가 필요한 것이다. 형법이론적 관점에서 합리적인 트래픽 관리는 바로 비례성 원칙에 의한 정당한 통신제한, 즉 법익침해행위의 정당화 사유가 된다. 이러한 이유로 인하여 사용자들은 각종 통신서비스에 가입할 때 통신사가 정한 약관을 통해 통신사의 망 관리 필요성에 동의하는 절차를 필수적으로 거치게 되며, 현재 이러한 동의는 별다른 논의 없이 통신비밀보호법 제2조의 "동의"에 해당하는 것으로 여겨지고 있는 것으로 생각된다. 통신비밀에 대한 자기결정권의 취지로 입법된 동의절차가 합리적 트래픽 관리를 정당화하는 절차적 수단으로 변용되고 있는 것이다.[75]

다. 인터넷 서비스 제공자의 관점

특히 통신비밀보호법에 대한 통신사의 입장은 상당히 강경한 것으로 보인다. DPI 장비를 이용한 디지털 통신의 패킷 식별은 자동화된 정보처리장치에 의해 자동적으로 분석되어 분류되며 그 과정에서 사람이 통신의 내용을 "지득"하는 일도 없는 경우가 대부분이다. 게다가 거의 모든 통신사들은 특정한 통신 내용을 선별하여 차단할 수 있다는 약관조항을 통해 이미 모든 가입자의 동의를 받고 있다. 따라서 통신사들은 DPI 장비 활용에 관하여 애초에 통신비밀보호법 구성요건 해당성 자체를 부인하고 있다. 이 연구보고서의 작성을 위하여 통신사의 실무담당자와 면담하는 과정에서 통신사측의 의견을 확인하는 기회를 가질 수 있었다. 이 자리에서 실무담당자는 망 관리 차원에서 통신 내역을 자동화된 정보처리기기(예컨대 DPI 장비)를 통해 처리할 뿐이며, 사람이 그 내용을 전혀 인지하지 않은 상태에서 전체 인터넷 서비스의 품질을 유지하기 위해 일부 이용자의 인터넷 접속을 선택적으로 제한하는 것은 프라이버시 침해와 전혀 무관한 것임을 강조하였다.

특히 인터넷 사용량 관리는 결과적으로 용도에 따라 다른 요금체계를 적용하는 전기요금 과금과 같은 것으로, 기술적 방법을 통해 인터넷의 사용 용도를 구

75) 그러나 전적으로 "동의"에 의지하는 정당화 방법은 애초의 입법의도를 벗어난 것이다. 동의는 인터넷 사업자의 설명의무를 구체화하여 송수신 방해라는 수단의 기본권 침해적 성격을 축소하기 위한 절차적 수단으로 이용되는 것이 바람직하다. 동의를 통한 정당화에 대해서는 제4장에서 상술한다.

별해서 파악하는 것은 마치 한국전력공사가 산업용과 주거용 전기의 요금을 구별하기 위하여 계량기를 따로 설치하는 것과 같으며, 또한 도시가스 업체가 난방용과 취사용의 요금을 따로 계산하는 것과 같다고 주장하였다. 같은 맥락에서 일부 사용자의 전송속도 제한이나 접속 차단도 블랙아웃을 막기 위한 부분적으로 단전하는 것과 유사한 것이라고 하였다. 게다가 해킹이나 악성 코드 유포와 같은 보안 위해요소를 사전에 차단하여 망에 장애가 발생하지 않도록 하는 것은 투자비용을 부담하고 물리적인 통신망을 설치한 망의 소유자로서 당연한 권리이며, 더 나아가 망의 관리자로서 의무이기도 하다는 것이다.

또한 선택적 인터넷 접속 차단이 통신비밀보호법 위반으로 10년 이하의 자유형으로 처벌될 수 있는 중대한 범죄라는 지적에 대해서도 이는 정보기술의 발전으로 인하여 법률이 현실을 반영하지 못하고 있는 문제이므로 적절하게 개정되어야 할 것이며, 오히려 본 연구를 통해 합법적으로 망 관리를 할 수 있는 적절한 기준을 제시하여 법률 개정에 힘써 줄 것을 부탁하였다. 이처럼 통신업계에서는 망 중립성 관련 문제를 단지 망 관리 업무의 하나로 받아들일 뿐이며, 인터넷 이용자의 프라이버시라는 관점에서 접근하는 시각에 대하여 강한 방어적 입장을 보이고 있다.

라. 소 결

1) 패턴 분석과 송·수신 차단은 별개의 문제

망 중립성 정책과 관련하여 논의를 어렵게 만드는 가장 대표적인 원인은, 아직까지 망 중립성 원칙에 관한 논의가 시민사회나 학계 전반에 활성화되지 않고 있기 때문에 이용자의 권리 측면의 논의는 상대적으로 부족한 반면, 높은 이해관계를 갖고 있는 통신사는 적극적으로 망 관리 옹호논리를 주장하고 있기 때문에 이에 대하여 적절하게 반박하는 것이 쉽지 않다는 점이다. 그러나 형사정책적 관점에서 바라보면 이러한 주장의 허와 실이 분명하게 드러난다. 망 중립성 저해행위는 크게 DPI 장비를 이용한 패턴 분석이라는 선행행위와, 분석된 패턴 정보에 기반한 차별적 송·수신 차단 행위로 나뉘어진다.

특히 정보의 내용을 지득한 바 없으므로 통신의 비밀을 침해한 바 없다는 논

변은 이미 우리 통신비밀보호법상 불법감청죄의 구성요건이 내용의 인식을 요구하지 않는다는 점만으로도 의미가 없는 주장임을 알 수 있다. 또한 감청 구성요건 해당 가능성을 인정한다면, 가입자의 동의의 의미도 분명해진다. 불법을 배제하기 위해서는 형법이론이 제시하는 요건을 갖춘 유효한 법익처분이어야 하는 것이다. 내용도 모르고 한 약관에 대한 동의는 이러한 요건을 충족시키기 어려울 것으로 보인다. 그러므로 통신사가 주장하는 인터넷 관리를 적법하게 하기 위해서는 법익침해를 정당화시키기 위한 별도의 근거가 필요한 것이다.

2) 합리적 트래픽 관리와 비례성 원칙

물론 자동화된 정보처리장치를 이용하여 타인에게 중대한 피해를 야기하는 불법적 통신의 경우 당연히 비례성 원칙에 따라 통신의 비밀과 자유가 제한될 수 있으며, 보다 경미한 침해를 야기하는 기술적 수단을 적절하게 선택하고 이를 통제할 가능성만 확보할 수 있다면 보안이나 범죄 예방 목적을 위해 서비스 제공자가 가입자의 송·수신을 방해하는 것이 합리적인 망 관리로서 일정부분 정당화 될 수 있다. 그러므로 형법이론적 관점에서 통신비밀보호법이 미처 법률에 명시적으로 예정하고 있지 않은 구성요건 해당성 배제사유 또는 정당화 사유에 해당하는 것으로 어떠한 경우에 이러한 정당화가 필요한가에 대하여 신중하게 살펴보고 적합성, 필요성, 균형성을 검토하여 합리적인 기준을 제시하는 것이 바로 망 중립성에 대한 정책방향을 구체화하는 것이 된다. 목적과 수단의 비례관계를 확인하고 비교하기 위해서는 우선 통신에 대한 차별적 취급이 구체적으로 누구의 어떠한 권리를 침해하며, 동시에 어떠한 목표를 달성할 수 있는지에 대한 이해가 전제되어야 한다.

제4절 DPI(Deep Packet Inspection) 기술에 대한 검토[76]

수단, 즉 선별적 송·수신 방해가 어떠한 권리를 침해하고 이를 통해 무엇을 달성할 수 있는지를 이해하기위해 우선 망 중립성을 침해하는데 사용되는 DPI 기술의 구체적인 작동 원리를 검토해 본다. 최근 ISP 업체들은 네트워크 관리 및 보호를 위하여 DPI 기술의 활용을 검토하거나 이미 이용하고 있다. 하지만 DPI 기술을 활용함으로서 발생할 수 있는 개인정보 침해에 대한 사실은 아직 부각되지 않고 있으며, 이에 관한 사회적, 이론적 논의도 아직은 그리 풍부하지 못한 것이 우리나라의 현실이다. 이는 통신사들이 선별적 접속 제한에 이용하는 기술적 수단에 대한 정보를 공개하지 않고 있기 때문이며, 더 나아가 기술적이고 규범적이며 동시에 정책적인 다양한 관점에 대한 폭넓은 이해가 선행되어야 비로소 문제의 실질에 접근할 수 있기 때문이다.

선별적 접속 제한이 통신비밀보호법 구성요건에 해당하는지 여부에 관하여 보다 명확한 판단을 내리기 위해서는 우선 DPI기술에 대한 이해가 전제되어야 한다. 본래 기술은 가치중립적인 것이어서 사용 방법에 따라 피해를 야기하기도 하지만 이익을 가져다주기도 한다. DPI 기술의 활용 역시 반드시 안 좋은 영향만을 미치는 것이라고는 할 수 없으며, 보안 등을 위해서는 꼭 필요한 부분도 있는 기술이기 때문에 합리적인 정책방향을 제시하기 위해서는 DPI기술의 실질에 관하여 충분히 고려해야 하는 것이다. 그러므로 이 보고서에서는 DPI에 대한 기술적 특징, 논의 동향 및 개인정보 침해 가능성을 가능한 지면과 능력이 허용하는 범위 내에서 비교적 상세하게 알아보고 이를 바탕으로 향후 DPI의 합리적인 활용 방안에 대한 논의의 출발점으로 삼으려 한다. 이를 위해 DPI라는 새로운 기술로 인하여 ISP가 침해 할 수 있는 프라이버시의 범위 및 가능성을 알아보며 해당 사실이 개인정보 침해에 어떠한 영향을 미치는지 검토하고 이에 대한 바람직한 정책방향을 제시하고자 한다.

---

76) DPI 기술에 대한 부분은 디지털 포렌식 및 컴퓨터 보안 전문가인 딜로이트 컨설팅 기업리스크 자문본부의 이영훈 컨설턴트와 한국 유닉의 김광훈 컴퓨터공학박사의 자문을 토대로 작성되었다.

1. DPI 기술 개관

SK 컴즈 개인정보 유출(3500만건), 넥슨 개인정보 유출(1320만건) 등 지난 2년간 유출된 개인정보는 널리 알려진 것만 거칠게 더해도 약 6000만건이 훨씬 넘는다. 최근 이러한 사건, 사고를 통해 개인정보보호에 대한 인식이 높아지고 그 중요성 또한 높아지고 있다. 이러한 상황에서 DPI 기술은 개인정보를 침해하는 수단이 되기도 하며 반대로 이를 지키기 위한 도구가 되기도 한다. 현재 우리는 과학 기술의 발전으로 인터넷을 통해 Google 또는 Naver 등의 웹사이트를 검색하여 정보를 수집하고 E-mail을 주고받으며 인터넷으로 일반 전화 및 화상 전화도 나누고, 스마트폰을 통해 영화 감상, 게임, 및 음악을 들으며 SNS(Social Network Service)로 다른 사람과 소통하는 등 오늘날 인터넷은 우리 생활에 없어서는 안 될 존재가 되었다. 이러한 것이 가능한 것은 ISP(Internet Service Provider)(또는 인터넷접속중개자)가 정보통신의 기반을 갖추며 해당 기반시설에 대한 안전성을 유지하고 있기 때문이다.

ISP는 안전한 네트워크 관리를 위해 DDoS의 공격을 예방하거나 스팸메일이나 악성 소프트웨어(악성코드 또는 멀웨어)를 차단하고 인터넷 트래픽을 관리하는 등의 업무를 수행하고 있다. 하지만 앞으로 ISP는 전통적인 업무인 인터넷 접속 서비스와 네트워크의 안정성을 위한 보호조치를 넘어서 웹사이트의 내용 필터링이나 차단은 물론 웹 내용 조작도 가능하게 되었다. 최근에는 이용자 맞춤광고를 시도하고 있어 사설 도청의 문제까지 제기되고 있고 SKT와 KT가 카카오 보이스톡을 선별적으로 부분 허용하는 등 특정 앱이나 서비스에 대한 관리가 가능하게 되었다. 이러한 ISP의 활동 범위를 확대시켜 준 것은 다름 아닌 DPI 기술이다.

ISP들은 이미 개인정보보호, 즉 보안 등을 이유로 DPI장비를 도입하여 활용하고 있다. 전병헌 민주통합당 의원이 지난해 10월 국정감사 때 제출한 자료에 따르면 KT와 SKT가 각각 11대씩, LGU+가 6대의 DPI 장비를 보유하고 있다고 한다. 그러나 이 장비들이 개인정보를 보호하기 위한 목적으로만 사용되고 있는 것은 아닌 것 같다. 지난 6월 KT가 카카오의 무료 인터넷 전화 보이스톡의 통화 품질을 떨어뜨려 논란이 됐을 때도 바로 DPI 장비가 사용된 것으로 알려진

것이다. 더 나아가 지금 미래창조과학부가 마련하고자 하는 "통신망의 합리적 트래픽 관리기준[77]"은 원칙적으로 DPI 기술의 활용을 전제로 하고 있는 것으로 보인다.

2. DPI의 기술적 이해

DPI 기술은 쉽게 말해 패킷의 내부 컨텐츠까지 확인하는 기술이라고 할 수 있다. DPI는 인터넷 패킷감청이라는 용어와도 혼용될 정도로 비슷한 개념이라고 볼 수 있다. 인터넷 패킷 감청과 DPI는 그 목적이 전혀 다르지만 사용되는 기술은 유사하기 때문에 해당 용어는 사용 목적에 따라 달라질 수 있다. 실 예로 국가정보원이 DPI 장비를 이용하여 인터넷 통신을 감청해 온 사실이 밝혀지면서 사회적인 이슈가 된 예가 있다. DPI 기술을 이해하고 문제의 소재를 확인하기 위해서는 우선 패킷의 구조, OSI 계층 구조 및 관련 기술과 원리에 대하여 살펴볼 필요가 있다.

가. 패킷(Packet)의 구조와 OSI 계층 구조

아래의 〈그림 1,2〉은 패킷의 구조 및 IP 패킷의 헤더 구조를 보여준다. 패킷은 크게 헤더(Header)부와 데이터 영역(Data Field)으로 구분된다. 헤더 부분은 기본적인 프로토콜 정보인 출발지 주소(Source Address)와 목적지 주소(Destination Address) 등을 담고 있는데, 이를 조사하면 IP주소(IP Address)나 저수준의 네트워킹 정보(Low-Level Connection States) 등을 파악할 수 있다. 한편 데이터 영역에는 소스 어플리케이션에 대한 정보(Identity of the Source Application)와 메시지 자체의 내용, 예를 들어 이메일 메시지, VoIP통화 및 웹서핑 세션등을 구성하는 모든 Bit가 담겨져 있다. 쉽게 말해서 이렇듯 크게 두 부분으로 나누어져 있는 패킷의 구조는, 비유를 통해 설명하면 우편으로 송달되는 편지를 비유

77) 상세한 내용은 미래창조과학부 주최, 정보통신정책연구원 주관 "통신망의 합리적 트래픽 관리기준 마련을 위한 토론회"(2013. 10. 10) 자료집 참조

하여 설명하기도 한다. 헤더 부분은 편지봉투에 해당하여 그 겉봉에 발신자의 정보와 수신자의 정보 및 도착지의 정보가 기재되어 있으며, 데이터 영역은 봉투 속에 들어있는 편지지로써 바로 우편을 통해 전달되어야 할 내용물인 것이다.

패킷이 전송될 때는 특별한 과정을 거치게 된다. 첫 번째로 패킷이 분할되고 암호화되며 압축 및 포장되어 전달이 된 후 포장을 풀고 암호를 풀고 압축을 풀어 분할된 것들을 다시 조립하여 원래의 패킷을 만드는 과정을 거친다. 이러한 과정은 다음 [표1][78]와 같이 일반적으로 OSI(Open System Interconnection) 계층으로 불리는 네트워크 참조 모델로 표현할 수 있다.

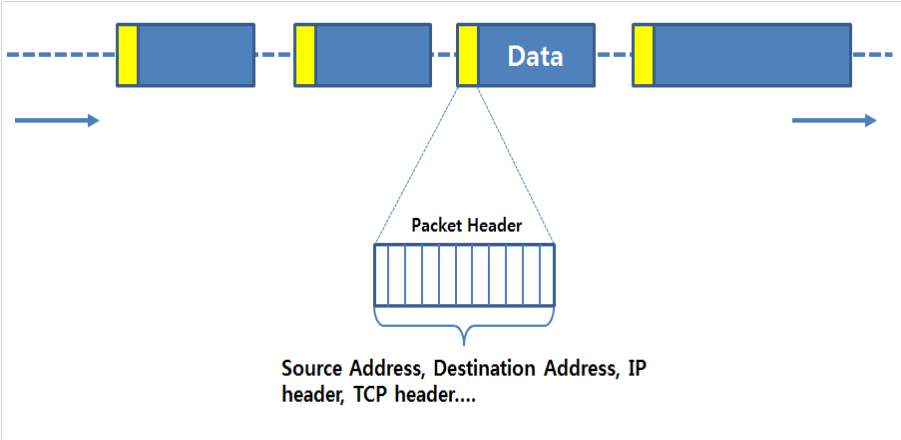

그림 1 패킷 구조도

78) 강유리, "인터넷 트래픽 관리와 DPI" 방송통신정책 제 25권 8호 통권 553호 pp. 23~48 May 2013 28페이지 표1 인용

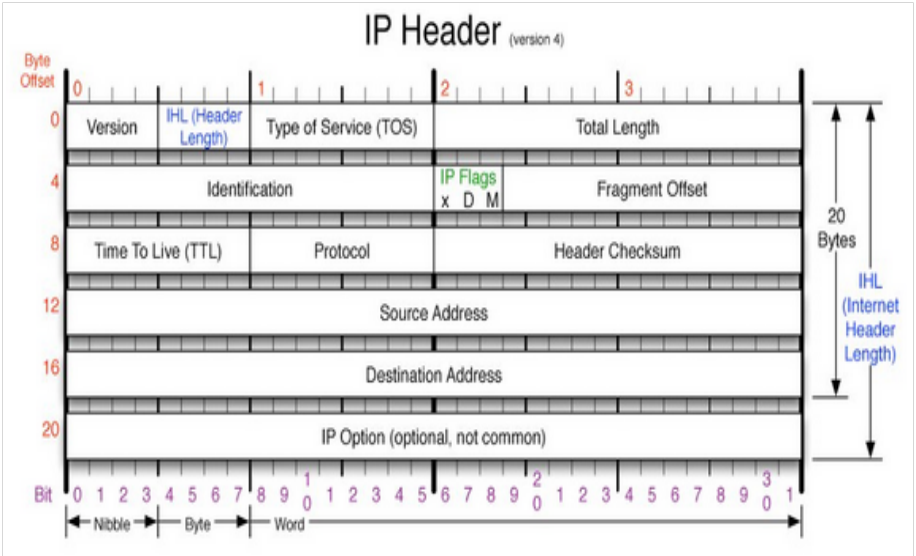

그림 2 IP Header 내부 구조도

표 1 OSI 계층

계층	OSI 계층	기능	Payload/ Header 구분
7	애플리케이션 계층 (Application Layer)	사용자가 사용하는 층으로 HTTP, FTP, 이메일 등 서비스 의미	페이로드 (Payload)
6	프리젠테이션 계층 (Presentation Layer)	정보의 표현방식 관리, 암호화, 정보압축	
5	세션 계층 (Session Layer)	응용 프로세서간 대화 관장	
4	트랜스포트 계층 (Transport Layer)	한 컴퓨터 안에서 포트 번호로 프로그램들을 구분	TCP 헤더 (TCP Header)
3	네트워크 계층 (Network Layer)	IP 주소를 통해 바이너리 집합체 전송	IP 헤더 (IP Header)
2	데이터링크 계층 (Data Link Layer)	MAC 주소를 통해 바이트들로 나열된 집합체 전송 및 데이터 전송상의 에러 확인	
1	물리 계층 (Physical Layer)	전자 신호 전송(비트정보 전달)	

나. DPI 관련 기술

DPI의 개념과 동작을 알기 전에 DPI 기술이 나오기 이전의 기술인 SPI(Stateful Packet Inspection or Shallow Packet Inspection)을 알아볼 필요가 있다. 인터넷 네트워크 환경을 통해 수많은 패킷들이 이동하고 있는 현실에서 네트워크 트래픽을 관리할 필요성이 생기게 되었다. 네트워크 환경을 통해 패킷이 이동하는 기본 원칙은 헤더부에 적힌 주소(출발지와 목적지)에 의해 전송되는 방식이다. 따라서 헤더부의 정보가 없다면 패킷을 원하는 곳으로 이동 시킬 수 없게 되는 것이다. 따라서 우체국에서 편지를 배송할 때 편지 봉투를 확인하여 분류하고 배송하듯이 때로는 헤더부분을 검사해 볼 필요가 있다. 이 우편물이 발송인이 원하던 주소대로 잘 배송되고 있는 것인지, 또는 우편 번호가 잘못 적힌 것은 아닌지 말이다. 이렇듯 헤더부에 명시된 다양한 내용을 검사하는 행위가 SPI이다. 패킷의 헤더 계층 (~Layer4)까지만 검사하여 비정상 패킷을 검출하는 기술이다. 패킷의 헤더부분에 특정 데이터를 넣거나 헤더부분의 내용을 조작하여 악의적인 목적으로 이용이 가능하나 IPv4에서는 추가할 수 있는 데이터의 범위나 양이 적어서 데이터 영역에 대한 위변조에 비해서 그 위험성이 적다고 볼 수 있다. 즉 집배원이 우송의 목적으로 겉봉의 내용을 살피는 것이 문제되지 않는 것처럼, SPI가 불법인 이유는 없다.

그동안의 SPI 기술은 네트워크 방화벽(Firewall) 시스템을 위해서 개발되어 왔고 현재도 사용되고 있는 기술이다. 즉 기업이나 조직의 차원에서, 기업·조직의 내부를 구성하고 있는 컴퓨터의 정보보안을 위해 외부에서 내부, 내부에서 외부의 네트워크에 침입하는 것을 차단하는 기술로 사용된다. 하지만 DPI는 앞에서 서술한 것과 마찬가지로 SPI 기술과 달리 데이터 영역까지 살펴보는 검사를 말한다. NIDS Evasion, DDoS 등 SPI로는 탐지할 수 없는 네트워크 공격이 생겨나면서, 패킷의 내용 계층(~Layer7, Payload(데이터영역))까지 검사하는 기술이 필요하게 되었다.

다. SPI와 DPI의 차이점

새로운 네트워크 분석 기술의 필요성에 따라 개발된 DPI는 기존의 SPI기술과 큰 차이점을 보인다. 아래의 〈그림3〉은 OSI 계층 구조에 대한 DPI와 SPI의 차이점을 보여주는 그림이다.

아래의 그림은 Parsons[79]의 분류 기준 바탕으로 그려진 그림으로 3단계의 패킷 분석이 나온다. 기존의 설명한 SPI와 DPI의 중간단계인 MPI로 표현되고 있으나 이하에서는 논의의 편의를 위하여 MPI(Medium Packet Inspection)는 제외하도록 한다.

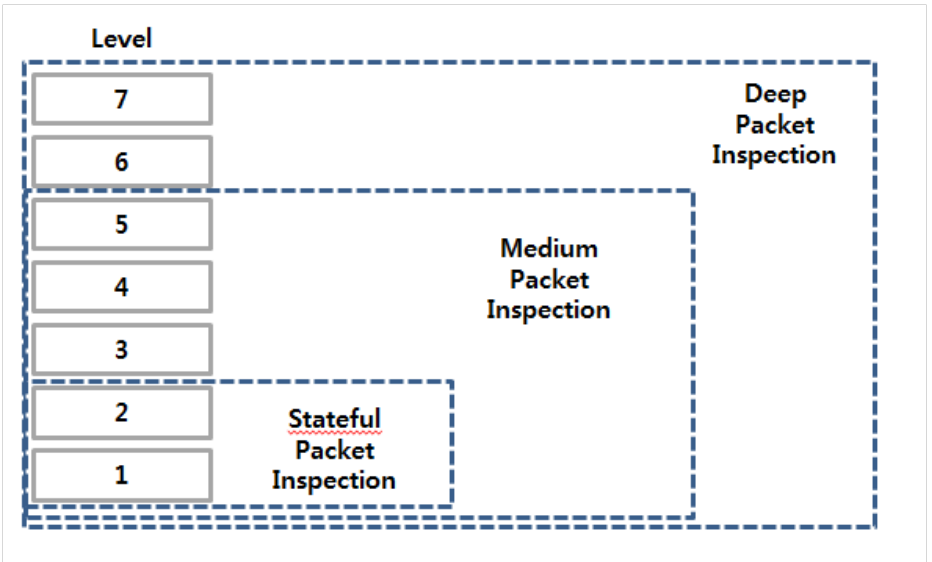

그림 3 OSI계층과 패킷 검사 수준

그림에서 보는 것과 같이 SPI는 세션 및 프리젠테이션이나 애플리케이션 계층을 읽을 수 없고, 이는 패킷의 데이터 영역까지 들여다 볼 수 없음을 의미한다. 패킷의 헤더 정보만을 통해 분석하고 판단하기 때문에 패킷에 대한 정교한 분석(특히, 애플리케이션 관련 추론)은 어렵다. 하지만 DPI에 비해 대용량의 트래픽

79) Parsons, C. . "DPI in perspective: tracing its lineage and surveillance potential." thenewtransparency surveillance and social sorting. Working paper. 2008

을 매우 빠르게 처리할 수 있다.

DPI는 SPI와 달리 모든 계층을 읽을 수 있고 이는 패킷의 데이터 영역까지 들여다 볼 수 있음을 의미한다. 하지만 이를 어떻게 구현하는지는 DPI 벤더 간 차별화 요소로 대부분 밝혀지지 않고 있다. 애플리케이션 식별에 한계가 있는 SPI와 달리 DPI는 매초에 수십만 건을 실시간으로 처리하며, 무슨 프로그램이 어떠한 패킷을 생성하는지 판단할 수 있도록 고안되었기 때문에 대규모 네트워크 환경에서 사용 될 수 있다. 예를 들어, 이메일과 금융거래, 음성통화 등을 포함한 인터넷 트래픽을 모니터링하면서 보통의 일반적인 트래픽과 그렇지 않은 트래픽(악의적 목적을 가진 트래픽)인가 을 구분하고 패킷을 바로 전송할 것인지 지연시킬 것인지를 결정하는데 쓰인다고 볼 수 있다.

일반적으로 알려진 DPI 장비는 패킷을 분석하기 위해 이미 식별된 패킷의 종류에 매칭 시킬 수 있는 충분한 정보를 가질 때까지 수십만의 패킷을 검사 장비의 메모리에 저장하여 패턴을 분석하게 된다. 일단 새로운 패킷이 장비에 의해 식별된 패턴과 매칭되면, 장비는 무슨 애플리케이션이 패킷을 생성하고 보내는지를 알게 되고 패킷 전송을 허용할지 말지의 규칙을 적용한다. 예를 들어 애플리케이션 사업자가 자신 서비스의 패킷 헤더 정보를 속이거나 패킷의 데이터부분을 추가적으로 암호화함으로써 패킷 검사 장비가 자신의 패킷을 식별하는 것을 우회한다 하더라도 서비스를 진행하기 위해 반드시 발생되는 공통적인 패턴을 발견하여 이를 통해 ISP는 식별된 애플리케이션의 패킷에 대한 우선순위를 주어 관리 할 수 있게 된다.

라. DPI의 특징과 기술적 분석

새로운 모바일 기기들이 끊임 없이 개발되고 LTE (Long-term Evolution)를 비롯한 4G 네트워크가 확장되면서 데이터 트래픽이 폭발적으로 증가하고 있다. 아울러, 보안 공격 발생률의 지속적인 증가로 인해 데이터 패킷에 대한 검사를 수행해야 할 필요성도 점차 높아지고 있기 때문에 패킷 처리 성능을 높임과 동시에 더욱 강력한 보안성을 보장하며 보다 지능적으로 데이터를 처리할 수 있는 네트워크 장비에 대한 요구가 그 어느 때보다 높아졌다.

따라서 DPI 기능은 데이터 스트림과 패킷 검사를 통해 악성 컨텐츠를 찾아내는 역할을 수행하는 네트워크 보안 애플리케이션의 필수 요소로 인식되고 있다. 악성 코드의 위협이 더욱 교묘해지고 있기 때문에, 성능 저하를 일으키지 않으면서도 수신되는 데이터에 대한 보다 세부적인 검사를 수행할 수 있는 네트워크 장비가 요구되고 있다. 소프트웨어 기반 DPI 접근 방식은 네트워크 보안 시장의 변화하는 요구에 맞춰 진화 가능하도록 비용 효과적이며 확장 가능한 솔루션을 유연성 있게 제공한다. 패킷 헤더만 검사하는 기존의 방화벽 및 IDS(Intrusion Detection Systems)와 달리, DPI는 각 패킷의 모든 헤더와 페이로드를 검사할 수 있기 때문에 보다 강력한 보안 애플리케이션의 기반을 제공 한다. 기존의 연구논문[80]을 보면 DPI기술의 발전 과정에 따른 특징을 볼 수 있다.

DPI는 발전과정에서 다음과 같은 두 가지 특징을 갖게 되었다. 첫째, DPI 기술은 실시간으로 인터넷 트래픽을 분석하여 차별적으로 처리할 수 있도록 진화하였다. 해당 특징의 경우 보안 기술 측면에서 보면 발전해가는 공격기술에 대응하기 위한 필수 불가결한 요소라고 볼 수 있다.

둘째, 다양한 기능들을 하나의 장비에 구현할 수 있도록 발전하였다. 이로 인해서 보안, 트래픽 관리, 유해 컨텐츠 차단, 맞춤 광고 제공 등 다양한 목적을 위해 사용될 수 있다. 해당 특징을 우리는 자세히 확인해야 할 것이다. 그 이유는 DPI 기술을 통해 활용되는 다양한 방법 중 네트워크 관리를 위한 방법이 아닌 것들이 존재하기 때문이다. 이는 우리들이 원하지 않는 서비스 및 활동이 ISP 업자들을 통해 이루어 질 수 있음을 의미한다.

일반적으로 네트워크를 관리하기 위한 활용 예로는, 가입자단의 대역폭 확대에 한계를 느끼는 네트워크 사업자들이 멀웨어나 대용량 트래픽을 유발하는 애플리케이션 관리를 통해 네트워크 운영의 효율성을 도모하는 것이 있다. 하지만 추가적으로 수입을 창출하길 원하거나 애플리케이션 사업자의 음성전화 또는 VoD 등으로부터 자사 서비스의 수익 보전 차원에서 DPI 기술을 사용하여 자사 서비스와 타 서비스 간 품질 차이를 발생 시킬 수도 있다. 컨텐츠 사업자들도

80) 강유리, "인터넷 트래픽 관리와 DPI" 방송통신정책 제 25권 8호 통권 553호 2013, 23~48쪽. 아래 표는 이 논문에서 인용함.

자신들의 지적 자산이 허가 없이 불법적으로 유통되는 것을 필터링하기 위해 DPI에 관심을 갖고 있다. 다음 표는 DPI의 다양한 이용 목적을 표를 통해 보여주는 것이다.

표 2 DPI의 다양한 이용 목적

목적	내용
네트워크 보안	바이러스, 멀웨어 및 위해 트래픽 차단
네트워크 관리	희소한 주파수 자원을 효율적으로 운영하기 위해 P2P와 같이 원치 않는 트래픽의 속도를 저하차단하거나 트래픽 종류에 따른 라우팅 최적화
컨텐츠 규제	아동 학대부터 국가 및 사회 안정성을 해칠 수 있는 불법 또는 유해 컨텐츠 차단
저작권 보호	P2P 등을 통해 저작권이 보호된 컨텐츠의 유통 방지
맞춤형 광고 제공	개별 이용자가 발생하는 인터넷 트래픽에 기반한 맞춤형 광고 제공

이러한 목적과 관련하여 DPI 기술의 구조를 정의해보면 다음과 같다. 앞에서 설명한 것과 같이 일반적으로 네트워크를 통해 데이터를 전송할 때 데이터를 효율적인 크기로 분할하여 전송하게 된다. 이렇게 분할된 조각들을 패킷이라고 하며, 패킷에는 헤더부분에 각 조각들의 목적지 주소와 앞으로 패킷을 재조립하기 위해 필요한 번호들이 저장되어 있게 된다. DPI 기술은 이와 같은 패킷들을 메모리에 저장하여 각 조각들에 대해서 패턴을 찾기도 하며 각 조각들을 모아서 해당 내용을 분석하는 기술이라고 볼 수 있다. 기존의 SPI기술이 패킷을 조립하기 위한 헤더부분의 정보만으로 패킷을 분석하고 관리하였다면 DPI는 헤더 정보뿐만 아니라 조각난 데이터 부분까지도 확인하여 패턴을 만들고 분석하기 때문에 기존의 SPI기술에서 할 수 없던 많은 일을 할 수 있게 되는 것이다. 패킷의 조각은 기본적으로 암호화 단계를 거쳐 전송되게 된다. 하지만 패킷을 모아서 각 헤더 부분과 데이터 부분의 내용 및 패턴을 분석해 보면 어플리케이션 사업자가 추가적인 암호화 기술을 적용하지 않는 이상 복호화 하는 것은 그리 어려운 일이 아니다. 이것은 DPI기술이 아닌 와이어샤크 (WireShark)와 같은 상용 프로그램을 통해서도 패킷을 분석하고 내용을 파악할 수 있는데 해당 패킷들의

목적지가 어디고 어떠한 포맷으로 되어 있는가에 대한 정보가 헤더 또는 데이터 부분에 있기 때문에 관련 정보를 바탕으로 적용된 암호화 기술을 유추하고 복호화를 진행하면 어렵지 않게 패킷의 내용을 파악 할 수 있게 된다.

간단한 예로, 커피숍 등 무선인터넷을 많이 쓰는 공공장소에서 해커가 노트북을 통해 해당 공간에서 이동하는 패킷을 수집하여 분석하게 되면 해당 공간에서 인터넷을 이용한 사람들의 ID나 비밀번호, 채팅내용 및 해당 컴퓨터의 화면을 똑같이 보는 것과 같은 해킹이 가능하다. 즉 DPI는 이러한 일련의 과정을 해당 통신망을 지나가는 모든 패킷을 대상으로, 대량으로 광범위하게 처리할 수 있게 만드는 기술이라고 할 수 있다.

마. DPI 보안 활용 필요성

지금까지의 네트워크 보안 장비는 4계층까지의 정보를 이용해 파이어월이나 VPN, 웹서버를 로드밸런싱하거나, 캐시서버에 대한 리다이렉션 기능을 활용하는 것이 대부분이었다. 하지만 최근에는 다계층 스위치를 이용한 보안 기능에 많은 관심을 가지게 되었으며, 많은 기업에서 이를 도입하여 활용하고 있다. 실제로 DPI 기술은 IDS/IPS 기술의 미래 모습이라고 봐도 무방하다. 따라서 보안 분야의 관점에서 본다면 DPI의 목적은 네트워크의 트래픽을 효율적으로 운영하고 보안 리스크를 없애기 위한 기술로 개발된 기술이라고 볼 수 있다.

그렇다면 DPI 기술은 이러한 목적과 현실에 따라 보안을 위해서 반드시 필요한 기술인가라는 의문을 가질 수 있게 된다. 유럽에서의 경우, 통신사업자들과 설비 제조업자들은 DPI 기술이 트래픽 관리행위를 위한 필수적인 전제조건은 아니라는 입장을 보였다.[81] 앞에서 이야기한 DPI 기술의 장점으로 기존에 대응하기 힘든 네트워크 공격 기법 및 앞으로 일어날 공격 기법에 대한 대응이 효율적으로 가능하다는 것은 알 수 있었다. 하지만 DPI 기술이 이러한 모든 문제의 오직 한 가지 해결방안은 아니라는 것은 분명하다. 다만 여러 가지 해결 방안 중 가장 효율적이고 정확한 방법임은 틀림이 없는 것이다.

81) 황주연, "유럽에서의 망 중립성 논의 경향" 정보통신정책 제 23권 6호, 2011, 12~13쪽

DPI 기술은 약이 될 수도 있지만 대부분의 효과가 강한 약이 그러하듯이 남용할 경우 그 해로움이 크다. 이를 통제하기 위한 법정책이 바로 망 중립성에 대한 형사정책이 될 것이다. 이하에서는 절을 바꿔 기술 활용의 규범적 의미를 통해 DPI 기술을 이용한 불법감청을 통해 침해되는. 법익의 실질을 분석해 보도록 하겠다.

제5절 선별적 송·수신 방해 행위가 침해하는 법익

1. 통신비밀보호법상 불법감청 구성요건의 보호법익

가. 형법상 비밀 개념

통신비밀보호법은 그 법률의 명칭에서부터 통신의 비밀을 보호하기 위한 법임을 명시하고 있다. 또한 이 법 제1조[82]는 통신비밀을 보호하고 통신의 자유를 신장하는 것을 목적으로 하고 있음을 선언하고 있으며, 불법감청 구성요건의 일차적 보호법익은 통신의 비밀이 된다. 우리말에서 "비밀"이란 "숨기어 남에게 드러내거나 알리지 말아야 할 일" 또는 "밝혀지지 않았거나 알려지지 않은 내용"을 의미한다. 형법상 보호법익으로서 비밀이란 "사생활 평온의 핵심이 되는 '개인의 비밀'"을 말한다.[83]

그러나 비밀의 가치에 대한 평가는 극도로 주관적인 것으로 별다른 설명이나 제한 없이 비밀을 바로 구성요건의 행위객체로 하는 것에는 명확성 원칙에 대한 부담이 있다. 그래서 우리 형법상 비밀침해죄는 객관적으로 확인 가능한 "봉함 기타 비밀장치"를 보호되는 행위객체의 표지로 하여 구성요건의 명확성을 확보하고 있다. 또한 형법 제316조 제1항의 비밀침해죄는 그 내용이 공개되거나 타인에 의해 인식될 것을 요하지 않으며, 단지 비밀장치를 해제하여 누설될 위험

82) 통신비밀보호법 제1조(목적) 이 법은 통신 및 대화의 비밀과 자유에 대한 제한은 그 대상을 한정하고 엄격한 법적 절차를 거치도록 함으로써 통신비밀을 보호하고 통신의 자유를 신장함을 목적으로 한다.

83) 배종대, 형법각론, 제8전정판, 홍문사, 57/2.

을 야기하는 것만으로도 구성요건에 해당하는 것이 된다. 그러므로 본래 우리 형법은 비밀침해죄를 위험범으로 구성하고 있다. 객관적으로 확인 가능한 방법인 비밀장치 등을 통해서 드러난 정보주체의 비밀로 하고자 하는 의도를 보호하고 있는 것이다. 비밀의 내용을 식별했는지 여부는 비밀침해죄의 구성요건에서 고려대상이 아니다.

나. 자동화된 패턴 분석과 통신비밀 침해

다만 우리 형법 제316조 제2항은 기술적 수단에 의한 비밀침해죄를 규정하면서 전자기록 등 특수매체기록의 경우 기술적 수단으로 그 내용을 알아낼 것을 행위양태로 하고 있어 침해범의 구성요건을 취하고 있다. 이 구성요건은 정보기술의 발전으로 인해 기존의 비밀침해죄의 행위객체에 포섭되지 않는 현상이 발생하였기 때문에 이에 대응하기 위하여 신설된 것이다. 전자기록 등 특수매체기록은 본래 인간의 오감으로 내용을 식별할 수 없는 것이어서 그 내용을 파악하기 위해서는 별도의 장치가 필요하며, 따라서 기술적 수단이 투입되면 비로소 인간이 인지할 수 있는 형태로 변화한다. 그러므로 논리적으로 이미 비밀장치를 해제하기 위한 기술적 수단의 이용이 성공하였다면 해당 전자기록의 내용은 다소의 차이는 있더라도 행위자의 인지가 가능한 상태에 놓이게 되며, 기술적 수단을 이용하였음에도 불구하고 여전히 그 내용을 알아내지 못한 경우라면 결과적으로 이는 비밀장치를 개봉하지 못한 것과 다름없는 것으로 볼 수 있다.

그러나 1995년 형법 개정으로 제316조 제2항을 신설한 이후로도 벌써 20년에 가까운 시간이 흘렀으며 그 동안 “기술적 수단”은 더 빠른 속도로 발전하였다. 그래서 오늘날 특수매체기록에 대해서는 사람이 그 내용을 지득하지 않는다 하더라도 자동화된 정보처리기기를 활용하여 얼마든지 이용할 수 있는 상황이 되고 있다. DPI 장비를 통해 분석된 패킷의 내용을 인간이 인지하지 않았다 하더라도, 이미 자동화된 정보처리장치는 DPI 장비를 투입한 자의 의도에 맞는 정보처리를 수행할 수 있다. 이는 마치 사기죄의 구성요건이 인간의 기망을 요구하고 있기 때문에, 은행 컴퓨터를 이용한 자동화된 정보처리과정에 해킹 등의 방법으로 불법적으로 개입하여 계좌 잔액을 증가시키는 행위를 포섭할 수 없게 되

는 처벌의 공백이 발생하여, 컴퓨터 사용 사기죄 구성요건을 신설한 것과 유사한 상황이라 할 수 있을 것이다. 즉 현대의 업무 처리는 인간의 인지를 필수적인 요건으로 하지 않으며 오히려 인간의 구체적인 인지가 전혀 없이 이루어지는 것이 훨씬 더 많다고 할 수 있다. 그러므로 패킷의 내용을 실제로 인간이 전혀 지득한 바가 없다 하더라도, DPI 장비를 설치한 자가 만약 그 내용을 인지했다면 처리했을 업무를 정보처리장치가 자동으로 처리하게 된다는 점을 고려하면, 역시 선별적 송·수신 차단을 위해 DPI 장비를 설치하고 이를 이용하는 행위는, 비록 이것이 자동화된 패턴 분석에 불과하다고 항변한다 할지라도, 통신비밀의 근본적인 침해를 야기하는 것으로 보아야 한다.

다. 보호법익의 범위 확대 - 자유로운 통신의 권리

설령 백보 양보하여 자동화된 패턴분석을 통한 선별적 송·수신 차단 행위가 통신비밀의 본질을 침해하는 것은 아니라 하더라도 여전히 통신비밀보호법상 불법감청 구성요건에 해당한다. 오히려 1993년 제정된 통신비밀보호법은 사기죄 구성요건의 경우와는 달리, 그리고 상술한 바와 같이 입법자가 의도했는지 여부와는 상관없이, 매우 다행스럽게도 이러한 현상까지도 적절하게 포섭할 수 있도록 미래를 향해 열려있는 구성요건 구조를 갖고 있기 때문이다. 즉 기술발전에 따라 통신 비밀의 보호영역이 확대되고 있으며, 통신비밀보호법상 불법감청 구성요건의 보호하는 법익의 범위도 점차 확장되고 있는 것이다. 그러므로 우리 통신비밀보호법상 불법감청죄의 보호법익은 내용의 지득 여부와 관계없이 침해된다. 이미 통신비밀보호법이 보호하는 영역은 단지 비밀 유지의 이익에서 멈추는 것이 아니라, 자유롭게 통신할 수 있는 권리에 이르고 있기 때문이다. 통신비밀보호법 제1조[84]는 "통신 및 대화의 비밀과 자유"를 보호하기 위한 목적을 갖고 있음을 제정 당시부터 분명하게 선언하고 있다. 인터넷통신과 관련하여 특히 이러한 사실은 이용자의 권리라는 관점에서 바라보면 보다 명확해진다.

84) 통신비밀보호법 제1조(목적) 이 법은 통신 및 대화의 비밀과 자유에 대한 제한은 그 대상을 한정하고 엄격한 법적 절차를 거치도록 함으로써 통신비밀을 보호하고 통신의 자유를 신장함을 목적으로 한다.

패턴분석을 통해 데이터 송·수신을 선별적으로 방해하는 것은 단지 통신비밀을 침해하는 것에서 그치지 않고 인터넷 이용자의 인터넷을 이용권의 본질적인 내용을 침해하는 것이라 할 수 있을 것이다. 물론 아직까지 우리나라에서 인터넷 이용자의 권리는 단지 인터넷 접속 서비스 제공자와의 계약상 권리로 여겨지는 경우가 많으며, 더 나아가 시민의 인터넷 이용에 관한 권리라는 개념은 아직 기본권적 차원에서 폭넓게 논의되고 있는 것으로 보이지 않는다. 그러나 상술한 바와 같이 본래 인터넷은 단대단 원칙을 설계의 기본 원칙으로 하고 있는 통신망으로, 오히려 망 관리자의 내용에 따른 송·수신 차별 권리 또는 권한이라는 개념이 훨씬 낯선 것이다. 스마트폰 등 휴대용 단말기를 통해 인터넷이 삶의 구석구석에까지 연결되어있는 현대 정보사회에서 인터넷을 이용한 정보획득과 의사표현의 자유는 이미 인간다운 삶을 위해 없어서는 안 되는 필수적인 가치가 된 것으로 보인다. 동시에 통신의 비밀에 대한 권리의 중요성도 이에 상응하여 더욱 부각되고 있으며, 그 개념의 범위를 점차 넓혀가고 있다.

2. 인터넷의 본질과 권리 주체로서 최종 이용자

망 중립성을 저해하는 행위는 바로 인터넷 이용자의 자유로운 인터넷 이용권을 침해하는 것이다. 그러므로 망 중립성에 관하여 통신비밀보호법의 보호법익의 실질을 확인하기 위해서는 인터넷 이용자의 권리를 보다 구체적으로 확인할 필요가 있다. 이하에서는 인터넷의 단대단 원칙을 논의의 출발점으로 하여 우선 최종 이용자의 규범적 개념을 구체화하고 이를 토대로 망 중립성 저해행위가 침해하는 망 이용자의 권리와 이익, 즉 통신비밀보호법상 불법감청 구성요건이 보호하고자 하는 법익의 실질을 확인해 본다.[85]

85) 이하에서 서술하고 있는 인터넷 이용자의 권리에 관한 내용은 망 중립성 이용자포럼 김보라미 변호사의 자문을 토대로 작성되었다.

가. 단대단 원칙과 최종 이용자

단대단 원칙에서 "사람"과 그의 권리가 직접적으로 도출되는 것은 아니다. 그러나 단대단 원칙에서 논의되는 "끝단에 있는 컴퓨터"를 실행시키고, 기능을 수행하도록 하는 주체가 존재한다는 점에서, 우리는 "사람"과 연결되어 논의를 진행할 수밖에 없다. 실제로 이러한 이 끝단에 있는 컴퓨터와 관련된 규범화는 오늘날 최종 이용자(end user)라는 개념으로 전환되어 논의되고 있다. 최종 이용자란 개념은 우리법상에서는 아직 생경하지만 국제적으로는 이미 일반적으로 활용되어 여러 법제에서는 도입된 개념이다.

그렇다면 최종 이용자란 무엇인가. 네트워크의 끝단에 있는 컴퓨터를 통해 인터넷 커뮤니케이션을 하는 사람, 단체 또는 그 무엇인가가 될 수 있을 것이다. 단대단 원칙에 기반한 기술적인 측면에서 생각해 보면 최종이용자 안에는 우리법에서 일반적으로 사용하는 용어인 소비자가 포함될 수도 있을 것이고, 컨텐츠 사업자들, 어플리케이션사업자들은 물론, 심지어 가장 광범위하게는 "법인격이 부여되지 않는 기술적인 장치"까지 포함할 수 있을 것이다.[86] 예를 들어, 2009년 서울버스 앱을 만들어 화제를 불러 일으켰던 당시 고등학교 2학년이었던 유주완군[87]은 소비자로 볼 수는 없을 수 있으나 네트워크 끝단에서 네트워크를 이용하여 서비스를 제공하는 최종 이용자에는 포함할 수 있게 된다.

86) 이 보고서에서는 최종이용자 논의를 규범적 의미로 한정하려고 하므로 법인격이 부여되지 않는 기술적인 장치는 제외하여 논의하도록 한다.

87) 서울버스 어플리케이션은 서울시와 경기도에서 홈페이지를 통해 실시간으로 제공하는 버스 위치정보를 끌어와 이용편리성을 높이기 위해 다시 가공한 후 사용자의 스마트폰에서 확인할 수 있도록 해준 무료 프로그램이었다. 그러나 경기도는 정보를 무단으로 이용했다는 이유로 정보제동을 차단하였고, 이미 어플리케이션을 이용하고 있던 시민들의 거센 반발로 인하여 당시 도지사가 직접 나서 차단 조치를 해제하였다. 이러한 상황은 망 중립성을 둘러싼 이해관계의 대립이 매우 다양한 차원에서 발생하고 있으며, 때로는 중립성의 개념이 단순한 통신망의 이용을 넘어 정보이용 플랫폼이나 공공정보에 대해서도 확장하고 있음을 보여준다. 그러나 망 중립성의 개념확장에 관한 논의는 이 보고서의 연구대상이 아니며, 상세한 논의는 보고서의 목적을 명확히 하는 것에도 도움이 되지 않는다고 생각되므로, 여기서는 단지 소개를 하는데 그치기로 한다.

나. 최종 이용자 개념의 구성

인터넷의 장점은 인터넷 프로토콜을 통해서 인터넷의 통제권을 망사업자들이 아닌 최종이용자에게 준 데에서 시작한다. 그러나 상술한 바와 같이 오늘날 망 사업자들은 기업 이윤의 극대화를 위해 망에 대한 감시기술을 발전시켜왔고, 그 감시기술을 이용하여 자신이 "소유"하는 망을 통제하고 있다. 망 사업자들은 또한 최종 이용자들의 선택권을 부당하게 제한하고, 통신요금을 차별하고, 특정 컨텐츠를 차단하는 수단으로 이 기술을 악용하곤 한다. 특히 시민의 인터넷 이용권리에 대한 인식이 아직 뒤처진 우리나라에서는 스카이프나 보이스톡과 같은 mVoIP을 차단하는 일들이 일상적으로 당연하다는 듯이 계속되고 있으며, 통신사는 가입자가 mVoIP을 사용하고 싶으면 추가요금을 내는 요금제를 선택하도록 강요하고 있다. 이러한 상황에서, 최종 이용자들은 타인에게 불법적인 피해를 야기하지 않는 한 자유롭게 인터넷을 이용할 수 있는 권리가 있으며, 망 사업자의 간섭 없이도 직접 컨텐츠와 어플리케이션을 만들고, 소비하고, 인터넷상에서 돌아다니는 문화를 선택할 수 있다는 의미를 갖는 단대단 원칙은, 오늘날 망 사업자의 적극적인 간섭으로 사실상 형해화 되어버렸다.

따라서 변화된 현실에서, 이제는 망 중립성 침해행위에 대한 규범적 고려는 단대단 원칙이나 인터넷 디자인 원칙만으로 설명하기 보다는, 이 끝단의 이용자들의 권리와 규범을 체계화시켜 나가는 데에서 논의가 시작될 수밖에 없을 것이다. 이미 다른 나라들에서는 "최종 이용자" 개념과 그 권리를 법제화하고 있고, 그 인권적 논의는 최근 다양하게 이루어지고 있다. 논의의 중심을 망 관리자에서 최종 이용자로 옮기는 것은 인터넷 이용권이라는 새로운 시각에서 망 중립성 문제를 바라볼 수 있는 문을 열어준다. 따라서 이런 측면에서 우리의 법체계에 대한 논의를 시작해 보는 것은 의미 있는 일이라고 생각된다.

다. 최종 이용자의 규범적 의미

최종 이용자의 법적 개념에 대한 정의 조항은 이에 대하여 여러 개념들을 모아 정의하고 있는 EC 전자 커뮤니케이션 네트워크와 서비스를 위한 공통규제

프레임워크 지침(이하 "EC 프레임워크"[88]) 지침을 참조하는 것이 바람직할 것으로 보인다. 이 EC 프레임워크 제2조 (h)호에서는 이용자를 공중이 이용할 수 있는 전자통신서비스를 이용 또는 요청하는 법인 또는 자연인으로, 같은 조 (i)호에서는 소비자를 공중이 이용할 수 있는 전자통신서비스를 자신의 거래, 사업 또는 직업 외의 목적으로 이용 또는 요청하는 자연인으로, 같은 조 (j)호에서는 가입자를 그 서비스의 공급을 위하여 공중이 이용할 수 있는 전자통신서비스를 제공하는 자와 계약한 상대방인 자연인 또는 법인, (n)호에서는 최종 이용자는 공중통신망이나 공중이 이용할 수 있는 전자통신서비스를 제공하지 않는 이용자라고 정의되어 있다. 위 각 개념들은 필요에 따라 해당 지침의 각 조항에서 사용되고 있는데, 위 정의 조항들의 취지를 종합적으로 고려했을 때 위 최종 이용자라는 개념은 "소비자"와 공중에게 통신서비스를 제공하는 사업자를 제외한 "사업자"들을 포함하는 개념으로 이해할 수 있다. 즉, 우리 법상에서 "부가통신사업자"로서 규제의 대상이 되는 자들도 EC 프레임워크 지침에서는 최종 이용자의 한 범주로 포함되어 있는 것이다.

이와 관련하여 아직 우리의 통신법에는 이에 정의 조항이 포함되어 있지는 않으나 한미 FTA와 한 EU FTA를 통하여 최종 이용자 규정이 이미 법제화되어 있다는 점에 주목할 필요가 있다. 한미 FTA에는 14.24조, 한 EU FTA 7.37.조 (i)호 정의 조항에서 최종 이용자를 공중 통신서비스의 공급자 이외의 서비스 공급자를 포함한 공중통신서비스의 최종 소비자 또는 가입자 (a final consumer of or subscriber to a public telecommunications service, including a service supplier other than a supplier of public telecommunications services)로 정의하고 있다. 한마 FTA에 대한 평가는 별론으로 하더라도, 최종 이용자들의 정의가 법적 효력을 가지는 규범에 구체화된다는 점에 한정해서 보면, 이후 망 중립성 원칙의 논의에 따른 단대단 원칙을 규범화시키기 위한 논의에 대하여 좋은 근거가 될 수 있다는 점에서 긍정적인 것으로 평가된다. 향후 통신법의 논의가 궁극적으로는 통신사업자들에 대한 국가규제는 완화시키되, 최종이용자의 측면에서

88) EC 프레임워크 지침 원문은 유럽연합 홈페이지 내 유럽연합법 싸이트 (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0021:EN:NOT) 참조

의 인권적인 접근을 지켜야 한다는 사정을 고려할 때, 최종 이용자의 정의규정과 법제화는 필요한 부분이라 하겠다.

라. 최종 이용자의 법적 권리

미국은 FCC에서 오픈 인터넷 규칙을 제정하여 직접적으로 "망 사업자에 의한 차별, 차단을 금지"를 정하였으나 이는 최종 이용자의 권리로부터 도출하였다기보다는 공정한 경쟁을 통한 혁신추구라는 공리주의적 측면의 강조를 통하여 그 정당성을 강조하고 있다. 그러나 미국은 이 오픈인터넷 규칙을 제정하면서 이용자의 지위와 함께 더불어 끝단의 사업자들(edge provider)의 지위를 강조하면서 망 중립성 원칙이 지켜지지 않으면 지금까지 이루어진 혁신에 큰 장애가 발생할 것임을 설명하고 있다.

한편, 유럽의 경우는 인권적인 기초 하에 논의가 시작되고 있다. 앞에서 언급한 EC 프레임워크는 제8조에서 최종 이용자의 접속권, 어플리케이션 또는 서비스 차단금지, 투명성 원칙, 차별금지 원칙등을 신설하면서 중요한 권리들을 규정하였고, 망 중립성에 대한 유럽위원회 선언을 추가한 바 있다. 이후 EU는 단일시장을 위한 통신법 초안 (Proposal for a Regulation of the European and if the Council laying down measures concerning the European single market for electronic communications and to achieve a Connected Continent, and amending Directives 2002/20/EC, 2002/21/EC and 2002/22/EC and Regulations (EC) No 1211/2009 and (EU) No 531/2012, 이하 "통신법 초안")[89]에서 망 중립성 원칙과 관련된 최종 이용자의 권리를 23조부터 24조까지에서 제시하면서 망 중립성 원칙을 규범적으로 정립하려고 시도하고 있다. 특히 이 통신법 초안의 제안서에서 기본권으로써 표현과 정보의 자유, 사업의 자유, 차별금지, 소비자 보호 및 개인정보 보호에 미칠 효과들이 분석되었음을 설명하고 있어, 통신법 초안이 중요한 권리들에 기반을 두고 논의되었음을 설명하고 있다.[90] 통신법 초안에서는 망 중

89) 통신법 초안 원문은 유럽연합 홈페이지 내 유럽연합법 싸이트 (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2013:0627:FIN:EN:PDF) 참조

90) 물론 이 법에 대하여는 통신사가 망을 통제할 수 있는 서비스(specialised service)를 넓게 인정함으

립성 원칙은, 바로 최종 이용자의 권리와 직결되는 것이라는 점을 명확히 설명하고 있다. EU에서 논의 중인 통신법 초안은 우리법이 어떻게 망 중립성 규범을 도출하는 것이 바람직할 것인지에 대한 좋은 참고자료가 될 수 있을 것으로 보인다.

3. 망 중립성 원칙과 관련된 최종 이용자의 권리

아직 우리나라에서 최종 이용자의 권리에 대한 규범적 근거는 쉽게 확인하기 어려운 것이 사실이다. 그러므로 최종 이용자와 관련된 권리의 실질을 확인하기 위해 우선 국제적인 수준에서 논의되고 있는 최종 이용자의 권리를 먼저 살펴보도록 한다.

가. 인터넷 접속권(access to the Internet)

인터넷 접속권에 대하여는 세계인권선언과 시민적 및 정치적 권리에 관한 국제규약 제19조상 "표현의 자유조항"[91]에서 인터넷 접속권을 유추할 수 있는 여지도 있으나, 아직까지는 인권보다는 헌법상 권리나 다른 인권들을 실현가능하게 하는 것으로 보아야 한다는 논의가 주류인 것으로 보인다.[92] UN 특별보고관 프랭크 라뤼(Frank La Rue)는 2011년경 "표현의 자유에 대한 보고서(Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression)"에서 인터넷 접속권을 인권으로 직접 규정하지는 않았다. 이는 각 국가마다 정보기술 활용 상황이 다른 만큼 인터넷에 대

로써 실제로는 망 중립성에 반할 수 있는 소지가 있다는 반론도 있으므로 이 초안에 대한 평가는 현재로서는 단정적으로 할 수 없을 것으로 생각된다.

91) 표현의 자유 조항 : Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas **through any media** and regardless of frontiers. 강조는 필자.

92) The New York Times, 2012년 1월 4일자 Vint Cerf, "Internet access in not a human right", (원문은 http://www.nytimes.com/2012/01/05/opinion/internet-access-is-not-a-human-right.html?_r=0) 참조.

한 보편적 접속을 모든 사람이 일시에 권리로 향유 할 수는 없다는 현실적인 한계를 확인한 것이다. 그러나 이 보고서는 "정부는 모든 사람들이 최대한 가능하게, 접속가능하게, 그리고 비용을 지불할 수 있는 범위 내에서 인터넷 접속을 할 수 있도록 할 의무가 있다"라고 적시하여 인터넷 접속권에 대한 국가수준(national level)에서의 의무화를 권고했다.[93] 즉, 국제적 수준에서도 아직까지는 인터넷 접속권이 인권으로 확실히 자리매김을 한 것은 아니지만, 인터넷 접속권의 중요성은 인터넷 사용이 직접적으로 정보접근과 연결되는 중요한 역할을 한다는 점에서 중요성을 가지고 있다는 점에 대한 공감대는 이미 형성되어 있다.[94]

이러한 인터넷 접속권과 관련하여 몇몇 정치적으로 그리고 경제적으로 발전된 나라들에서는 인터넷 접속권을 기본권 또는 인권적 개념으로 규정하여 왔다. 에스토니아 국회는 2000년경 인터넷 접속을 기본적인 인권으로 선언하는 법안을 통과시켰고, 프랑스 헌법위원회가 2009년 인터넷 접속을 기본권이라고 선언하였으며, 코스타리카 헌법재판소 역시 2010년 비슷한 결정을 한 바 있다. 심지어 핀란드는 좀 더 구체적으로 2009년 1초당 적어도 1메가바이트의 속도로 인터넷 접속이 이루어져야 한다는 브로드 밴드 수준에서의 입법화를 규정한 법령까지 발표하였다.[95] 우리가 논의의 출발점으로 삼고 있는 단대단 원칙에서의 최종이용자들의 권리는, 근본적으로 망 사업자의 차별이나 차단 등의 간섭 없이 최종이용자가 자유롭게 인터넷에 접속할 수 있는 것을 의미하므로, 위와 같은 인터넷 보편적 접속(권)과 연결될 수밖에 없다.

---

93) Rrank La Rue, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression", Human Rights Council seventeen session, 2011. 5. 16. 22쪽 (원문은 http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf)

94) David Souter, "Human Rights and the Internet : a review of perception in human rightos rganisations", APC, 2012. 6. 23쪽

95) Rrank La Rue, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression", Human Rights Council seventeen session, 2011. 5. 16. 18쪽 (원문은 http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf)

나. 표현과 정보에 대한 자유(freedom of expression and information)

표현과 정보에 대한 자유는 세계인권선언, 시민적 및 정치적 권리에 관한 국제규약 제19조로부터 직접적으로 인정되는데, 이 규정은 당연히 인터넷에서의 표현과 정보에 대한 자유까지 확장된다고 이해되고 있다.[96] 인터넷 자체가 표현의 자유에 있어서 가장 중요한 플랫폼이므로 인터넷상의 커뮤니케이션을 차별, 차단하지 않는 것을 의미하는 망 중립성 원칙은 표현과 정보에 대한 자유의 핵심적인 요소로 이해될 수 있다. 미국 망 사업자가 2004년도 자사 가입자들의 수신 이메일 중에 이라크 전쟁에 반대한 운동가들의 연합체 URL이 포함된 이메일을 시스템에서 필터링했다는 의혹을 받았을 때에도 망 중립성 원칙의 훼손 문제이면서도 동시에 표현의 자유 침해에 해당한다는 점이 함께 지적된 바 있다.[97] 즉, 최종 이용자는 인터넷이라는 수단을 통하여, 누군가에게 정보나 사상, 구체화되지 않은 아이디어들을 전달하거나, 검색하거나 또는 이를 전달받는 형식의 커뮤니케이션을 동시다발적으로 하게 되는 것이 일반적인데, 이는 표현과 정보에 대한 자유가 예정하는 권리 범위에 해당한다.

다. 프라이버시권(Privacy) 개념의 확장과 정보적 자기결정권

망 중립성 침해행위가 가장 중대하게 침해하는 이용자의 권리는 바로 프라이버시권이라고 할 수 있을 것이다. 앞에서 검토한 것처럼 망 사업자는 망 중립성 원칙을 침해하는 과정에서 필연적으로 이용자들의 커뮤니케이션의 대상 데이터의 내용 등에 대하여 실시간으로 감시하고 그 내용을 확인할 수밖에 없다. 감시는 오늘날 프라이버시권에 영향을 주는 요소이면서, 인터넷의 다양한 활동을 위협하는 행위로 이해되고 있다. 정부나 기업들은 망을 통제, 감시하면서 이용자들의 행위에 직접적인 영향을 주게 된다. 유럽에서 최초로 망 중립성 법을 제정한 네덜란드의 경우에도, 네덜란드의 통신사 KPN이 "WhatsApp"이라는 인터넷

96) David Souter, "Human Rights and the Internet : a review of perception in human rightos rganisations", APC, 2012. 6. 16-24쪽.

97) Scott Marcus, Pieter Nooren, Jonathan Cave, Kenneth R. Carter, "Network Neutrality:Challenges and responses in the EU and in the U.S.", European Parliament, 2011. 5., 45쪽.

전화를 사용할 경우 추가 요금을 부과할 것이라는 계획을 발표하자 망 사업자가 인터넷 전화사용을 알아내기 위하여 이용자들의 통신을 감시하는 것은 바로 프라이버시 침해에 해당한다는 분노에 찬 여론이 일어났고, 이에 힘입어 망 중립성 규정이 의회를 통과할 수 있었다. 즉, 망 중립성 원칙을 침해행위는 대부분 실시간 감시를 통해 이루어지는 경우가 대부분이므로, 프라이버시의 침해와 직접적으로 연결될 가능성이 크다. 그런데 프라이버시란 일반적으로 사적 영역에 대한 비밀 또는 비공개의 자유를 의미하는 단어로 공적인 영역과 구별되는 개인적인 일들을 알리지 않을 권리를 말하는 것이다. 따라서 인터넷을 통해 전송하는 정보가 프라이버시권의 보호 범위에 포섭되는 것인가에 대해서는 논의를 정리해 볼 필요가 있다.[98]

1) 프라이버시의 본래적 의미

공과 사를 구분하는 것은 인간의 오랜 역사를 통해 너무나도 당연한 일이었으며, 삶의 사적인 영역은 주거하는 공간의 문을 닫고 잠금으로써 당연히 보호될 수 있었다.[99] 그래서 사생활에 대한 보호는 불법침입 등에 대한 금지에서 나오는 부수적 이익 정도로 이해되었던 것이다. 그러나 사진 및 인쇄술과 같은 정보를 기록하고 전파하는 기술이 발전함에 따라 인해 비밀로 하고 싶은 사적인 영역이 문 밖으로 확장되기도 하고, 종래에는 침해할 방법이 없어 사적인 공간 깊숙한 곳에 감추어 둘 필요가 없었던 것들에 대한 침해가 가능하게 되기도 하였다.[100] 이러한 상황에서 18세기 이후 시민의 자유에 대한 인식이 성장하면서 프라이버시는 비로소 권리로 자리잡기 시작하였으며, 국가가 적극적으로 보호해야

98) 프라이버시권의 발전과정에 관하여 상세한 이론적 분석은 전현욱, 개인정보 보호에 관한 형법정책, 고려대학교 박사학위논문, 2010, 19-37쪽 참조.

99) 이를 Space Privacy라고 한다. Jarry Kang, Information Privacy, 50 Stanford Law Review 1193, 1998, 1202쪽 이하 참조.

100) 이러한 와중에 1980년 자신의 집에서 있었던 사교파티를 가십화하여 상세하게 보도한 지역신문 때문에 격분한 워렌(Warren)이 브렌다이스(Brandeis)와 함께 "프라이버시에 대한 권리(Right to Privacy)"라는 논문을 하버드 로 리뷰(Harvard Law Review)에 기고한 이래 영미법에서 프라이버시가 구체적인 권리로 자리잡기 시작했던 것이다.

하는 사적 영역에 대한 방어권으로 자리잡게 된다. 따라서 프라이버시권은 본래부터 "타인에 의한 원치 않는 간섭이나 강요로부터의 보호이며 개인의 행동의 자유에 대한 보호를 의미하는 개념"[101]이었다고 할 수 있다.

2) 정보적 자기결정권

그런데 자본주의와 정보처리기술의 비약적인 발전은 우리의 일상생활을 빠르고 편리하게 변화시켰고, 이러한 변화는 개인의 프라이버시에도 영향을 미쳤다.[102] 정보기술이 적극적으로 상용화됨에 따라 너무나도 많은 개인에 대한 정보가 인터넷과 컴퓨터에 넘쳐나게 되었고, 정보의 지배가 곧 힘이 되는 정보 사회[103]가 등장하게 된 것이다. 오늘날 국가와 기업은 과거에 비해 정보처리비용을 비약적으로 절감해주는 정보처리장치를 이용하여 정책수행의 효율성, 이윤의 극대화라는 각각의 목적을 위해 항상 더 많은 개인에 대한 정보를 수집하여 저장, 이용하려고 한다. 그리하여 개인은 대기업과 국가로부터의 정보적 자유권을 확보하기 위하여 자신의 개인정보에 대한 수집 및 이용여부를 스스로 결정할 권리를 주장하게 되었고, 이러한 현상으로 인하여 정보적 자기결정권이라는 새로운 문제가 등장하게 되었다.[104]

그런데 정보처리기술의 수준은 지금도 그 발전을 계속하고 있고, 보다 최신의, 고도의 기술은 항상 자본과 권력을 가진 쪽에서 선점 또는 독점하게 되어 있다. 그리하여 정보이용자와 정보주체 사이에서도 힘의 불균형의 논리가 그대로 적용되어 약자는 타 정보에 대한 접근이 용이하지 않고, 나아가 강자에 의하여 자신의 정보가 침해될 수 있는 상황에 놓이게 된다. 이러한 상황에서 정보적 자기결정권은 더 이상 인격과 연관된 사적영역에 대한 보호를 위한 권리라고만 볼 수

101) Carol Gould, The Information Web, Ethical and Social Implications of Computer Networking, Boulder, 1989, 44쪽.

102) Lawrence Lessig, Code and other Laws of Cyberspace, 김정오 역, 코드 - 사이버공간의 법이론, 나남출판, 2002, 334쪽 참조.

103) 정보사회에 관한 형법이론적 이해는 전현욱, 해킹의 형법적 규율 방안, 고려대학교 석사학위논문, 2000, 5쪽 이하 참조.

104) 이 개념은 독일연방헌법재판소의 결정(BVerfGE 65, 1)를 통해 의미가 정립되었다.

없으며, 공적영역으로 그 논의의 중심이 완전히 확장되었다고 볼 수 있다. 그리하여 오늘날 정보적 자기결정권은 단순히 사적 내부 영역에서의 방어적 성격을 지닌 권리가 아니라 정보주체가 정보이용자에게 정보의 수집, 이용에 대한 범위와 처리에 대한 기준 준수 등을 적극적으로 요구할 수 있는 권리라고 볼 수 있다.[105]

그러나 정보주체의 정보적 자기결정권과 정보이용자의 정보이용권은 서로 충돌하는 개념으로 전자에 대한 보호를 강화하는 것은 후자에 대한 과도한 제한으로 이어진다. 정보이용권의 과도한 제한은 정보화시대의 성격에 역행하는 것이고, 정보주체가 모두 정보이용자가 되는 상황을 감안한다면, 정보적 자기결정권의 보호범위를 어느 정도로 설정해야 하는지는 쉽게 결정할 수 있는 문제가 아니다. 게다가 정보적 자기결정권의 보호를 위하여 정보이용자에 대한 형사처벌을 그 수단으로 사용하고자 한다면, 더더욱 신중한 검토가 필요할 것이다.[106] 그러므로 선별적 송·수신 방해행위가 통신비밀보호법상의 감청 구성요건에 해당하는 것으로 확정된다 해도 정당화 될 수 있는 가능성에 관해서 신중하게 고려해야 한다.

라. 기타의 권리

망 중립성은 열거한 권리 이외에도 보편적 접속과 관련하여 평등권(equality of rights), 교육권 (right to education) 등과 직간접적으로 관련된다.[107] 유럽에

105) 법원은 개인정보를 대상으로 한 조사, 수집, 보관, 처리, 이용 등의 행위는 모두 원칙적으로 개인정보자기결정권에 대한 제한에 해당한다고 판시하여 개인정보에 대한 자기결정권을 폭넓게 인정하려는 태도를 취하고 있다. 헌법재판소 2005.5.26. 선고, 99헌마513.

106) 일부 법무법인은 저작권자로부터 대리권을 받아 인터넷상에서 저작권을 침해한 것으로 확인된자로부터 합의금 명목으로 저작권 침해로 인한 손해액보다 훨씬 많은 합의금을 받아내기도 한다. 이는 저작권에 대한 정보적 자기결정권을 강력하게 보호하는 것이 저작물 이용자의 자유를 위축시키는 것으로 해석할 수 있다. 이러한 문제현상에 관해서는 전현욱, 지적재산권과 형법정책, 경원법학 제3권 제2호, 2010, 249쪽 참조.

107) Frank La Rue, “Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression”, Human Rights Council seventeen session, 2011. 5. 16. 18쪽.

서 최초로 망 중립성 법을 통과시킨 네덜란드 통신법의 경우에도 유럽인권조약을 그 근거로 제시하고 있다. 망 중립성 원칙을 규범화하는데 있어서는, 최종 이용자들의 권리들이 실현될 수 있는 방향으로 접근해야 하며 이 과정에서 헌법상 기본권이나 국제규범이 선언하고 있는 인권은 중요한 근거로 볼 수 있을 것이다.

제6절 소 결 - 망 중립성 원칙은 형사정책 관점에서 보아야 한다.

지금까지의 검토를 통해서 형사법적으로는 매우 생소한 개념인 망 중립성 원칙을 왜 형사정책적 관점에서 바라보아야 하는지를 살펴보았다. DPI 장비를 활용하여 패킷의 패턴을 분석하고 차별적으로 송·수신을 차단하는 행위는 인터넷 이용자의 통신의 비밀과 통신의 자유 두 법익을 동시에 침해하는 행위이다. 그러므로 망 중립성은 망 이용비용의 분담 문제가 아니다. 현대 정보사회에서 통신의 비밀과 통신의 자유는 시민의 기본적 자유권의 내용이며 공론의 장 형성에 없어서는 안 되는 필수적인 요소이다. 그래서 민주주의의 필수적인 전제가 되는 통신의 비밀과 통신의 자유에 대한 강력한 보호가 필요하다는 사회적 합의는 현재 통신비밀보호법상의 강력한 형사처벌 구성요건으로 남아있다.

그러므로 망 중립성에 관한 정책방안, 즉 합리적 트래픽 관리의 기준은 통신비밀보호법상 감청 구성요건에 해당하는 행위를 어떻게 정당화시킬 수 있을 것인가에 대한 고민을 통해 제시되어야 한다. 이하에서는 국외의 망 중립성 관련 논의의 전개 현황을 통해 다양한 이해관계를 가진 당사자들의 주장을 상세하게 살펴보고, 망 중립성을 둘러싼 분쟁과 그 해결과정, 그리고 망 중립성 정책을 법제화하는 과정을 상세하게 들여다봄으로써, 지금 우리에게 적합한 망 중립성 정책 방안, 즉 선택적으로 데이터의 송·수신을 방해하는 행위에 대한 정당화 가능성을 검토함에 있어 관하여 고려해야 할 요소들에 대하여 살펴보겠다.

(원문은 http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf)

제3장

주요국가의 망 중립성 정책 현황

전현욱 · Michael Geist · Chris Marsden

03

주요국가의 망 중립성 정책 현황

인터넷은 국경을 초월한 정보통신 수단으로 이에 관한 국가정책은 당연히 국제적인 관점에서 검토되어야 한다. 그러나 우리나라뿐만 아니라 세계적으로 망 중립성에 대한 정책은 아직 수립 과정 중에 있으며, 따라서 통신비밀보호 또는 프라이버시 보호와 망 관리에 관한 각국의 분쟁 현황과 규제기관의 정책동향은, 국가마다 그 접근의 방향에 있어서 서로 조금씩 다른 모습으로 나타나고 있다. 투명성, 차별 금지, 차단 금지, 합리적 트래픽 관리 허용 등 망 중립성에 관한 주요원칙은 대체로 동일하나 아래 표[108]에서 보는 바와 같이 각 국가의 규제 관점 및 가치기준에 따라 그 구체적인 내용이나 강도, 법제화 방법은 차이를 보이고 있다. 따라서 각각의 합리성을 비교분석하는 것은 우리나라의 정책방향 설정에 있어서 좋은 참고자료가 될 것으로 생각한다.

108) 정보통신정책연구원, 통신망의 합리적 트래픽 관리기준 마련을 위한 토론회 자료집, 8쪽의 표를 재구성하고 보완함.

표 3 주요국의 망중립성 규제 관점과 가치 기준

국가	규제 관점	가치 기준
미국	최종 이용자와 컨텐츠 제공자의 권리 측면에서 접근	개방성 중시
캐나다	자유로운 이용과 합리적인 망 관리의 조화를 추구	개방성과 시장기능 균형
EU	유럽 통신시장의 통합을 위해 국제규범 제정	시장기능 중시하면서 투명성으로 보완
영국	시장 자율 지지	

그러나 아직 세계적으로도 망 중립성을 직접적으로 형사정책적 관점에서 다루고 있는 논의나 연구 성과는 찾기가 쉽지 않으며, 다만 망 중립성 원칙 위반행위가 개인의 프라이버시를 심각하게 침해하며, DPI 장비를 통해 패킷의 패턴을 분석하는 것은 통신의 비밀과 자유를 심각하게 침해한다는 점에 대한 인식이 이제 점차 확산되고 있는 것으로 보인다. 그러므로 제3장에서는 추후 논의의 발전을 위한 자료제공의 의미를 담아, 가능한 범위 내에서 주요국가의 망 중립성 정책 현황과 다양한 이해당사자의 관점을 충분히 전달하고자 노력했다.

제1절 미국의 망중립성 정책 동향

미국은 인터넷의 기본 구조를 설계하여 실용화한 나라로 정보통신산업분야의 기술발전을 선도하고 있는 국가이다. 동시에 전통적으로 개인의 자유와 권리에 대한 인식이 강한 나라로 프라이버시에 대한 침해에 민감하게 대응하고 있다. 그러나 넓은 국토 면적으로 인해 통신망 구축비용이 상대적으로 많이 소요되기 때문에, 인터넷 서비스 제공자가의 신규 시장 진입이 쉽지 않고 따라서 소수의 인터넷 서비스 제공자가 지역별 독점구도를 형성하면서 발전하고 있는 상황이어서 독점적 통신사를 적극적으로 규율하여 망 중립성을 보장하려는 움직임을 보이고 있다. 그러나 미국의 경우 망 중립성 논의는 그 나름대로의 사정을 고려하면서 발전해 나아가고 있는 것으로 보인다. 하지만 이 문제와 관련하여 산업의 영향력이 가장 큰 미국이 선도적 역할을 수행하고 있음에도 불구하고, 오히려

산업의 영향력이 너무 큰 탓으로 차세대 인터넷 전화 등 이해관계가 첨예하게 대립하는 부분에 대한 논의는 오히려 부차적 문제로 희석되는 경향이 있다.

1. 미국의 망 중립성 정책 도입 추진 배경

2005년부터 미국 내에서 인터넷 프로토콜, 인터넷 전화 등 망 중립성에 대한 실질적인 규제 요구가 시작되었다. 2004년 노스캐롤라이나에 소재한 인터넷 서비스 제공자인 매디슨 리버 커뮤니케이션(Madison River Communications)이 자사의 네트워크를 이용하는 보나지(Vonage) 사의 인터넷 전화(VoIP)를 차단한 사건이 세상에 알려지면서 이에 대한 논의가 촉발되었다.[109] 2005년 미국 연방통신위원회(Federal Communications Commission, FCC)는 인터넷 전화 차단에 대해 조사를 실시하였고 매디슨 리버사에 즉각적인 차단 중지명령과 함께 15,000 달러의 과징금을 지불하라는 결정을 내렸다. 같은 해 8월, FCC는 인터넷의 개방성의 증진과 광대역망 확장을 목적한 망 중립성 원칙[110]을 발표하였다. 2005년 FCC의 망 중립성 4대 원칙은 다음과 같다.

2005년 FCC 망 중립성 4대 원칙

1) 컨텐츠 차별 금지 – 소비자는 자신이 선택한 적법한 인터넷 컨텐츠에 접근할 권리가 있다.
2) 어플리케이션 및 서비스 차별 금지 – 소비자는 법이 허용하는 범위 내에서 어플리케이션과 자신이 선택한 서비스를 이용할 권리가 있다.
3) 단말기 차별 금지 – 소비자는 네트워크에 해를 가하지 않는 법적으로 허용된 기기를 선택해 네트워크에 연결할 수 있는 권리가 있다.
4) 사업자간 경쟁 보장 – 소비자는 망사업자, 어플리케이션 제공자, 서비스 제공자, 컨텐츠 사업자 간의 경쟁에 따른 혜택을 받을 수 있다.

109) Madison River Communications, LLC and Affiliated Companies, Order, File No. EB-05-IH-0110, 20 FCC Rcd 4295 (2005).

110) 하지만 FCC의 망 중립성 원칙은 강제력이 없는 권고안이기 때문에 구속력은 없다. 자세한 내용은 Appropriate Framework for Broadband Access to the Internet over Wireline Facilities, Policy Statement (rel. Sept. 23, 2005) ("Internet Openness Policy Statement"). 참조.

이후 론 와이든(Ron Wyden) 상원의원의 인터넷사용의 자유 및 컨텐츠 차단 금지에 관한 법안[111]을 시작으로 망 중립성에 관한 다양한 법안이 의회에 상정되기도 하였다. 입법적 노력과는 별도로 FCC는 통신시장에 대한 규율 권한을 활용하여 자체적으로 망 중립성을 대규모 통신사의 합병조건에 삽입하는 등 보다 적극적인 조치를 취하였다. 그러나 2007년 미국 연방통상위원회(Federal Trade Commission)과 미 법무부를 포함해 관련부처는 망 중립성 규제가 경쟁을 위축하고 인터넷 발전에 부정적인 영향을 미칠 수도 있으므로 규제 마련은 제반 상황을 면밀히 검토하고 결정하자며 FCC가 제안한 망 중립성 규제 마련에 대해 신중한 입장을 취하였다.[112]

FCC는 2007년 망 중립성 규제에 대한 대중의 인식 확인, 인터넷 서비스 제공자의 영업 현황, 초고속 인터넷망 보급률 등 인터넷 사용 환경을 파악하기 위해 광범위한 조사를 진행하였고 이 조사를 토대로 2009년, 기존의 망 중립성 4원칙에 비차별성(nondiscrimination)과 투명성(transparency)를 더한 6가지 원칙을 내용으로 하는 "Notice of Proposed Rule Making(NPRM)"을 발표하였다.[113] FCC는 규제안에서 망 중립성 적용의 예외사항으로 합리적인 네트워크 관리를 설명하면서 적용 범위를 한정한 한편 무선 인터넷도 망 중립성을 적용할 것을 제안하였다.

111) 2006년 5월 18일, 제109차 의회에 상정되었다. H.R. 5417 (109th): Internet Freedom and Nondiscrimination Act of 2006

112) 미법무부의 망 중립성에 관한 입장보도, "Department of Justice Comments on Network Neutrality in Federal Communications Commission Proceeding", 2007년 9월 6일 (http://www.justice.gov/opa/pr/2007/September/07_at_682.html) 참조.

113) FCC, "NOTICE OF PROPOSED RULE MAKING- Before the Federal Communications Commission Washington, D.C. 20554", 2009, 2-3쪽 참조; 정석균, IT Network 정책방향에 대한 연구 : 망 중립성과 효율성을 중심으로, 디지털정책연구 제10권 제1호, 2012, 53면.

2. FCC 오픈 인터넷 규칙[114)]

이후 의견 수렴을 통해 2010년 12월 FCC는 "Open Internet Rules"를 발표한다.[115)] 핵심 내용을 요약하면 다음과 같다.

2010년 FCC Open Internet Rules의 주요 내용

1. 컨텐츠 중립성 – ISP 가 인터넷 상에서 합법적인 이용자 선택에 의한 컨텐츠 전송과 수신을 막는 행위를 금지함.
2. 어플리케이션 및 서비스 이용 – ISP 가 이용자가 선택한 합법적인 서비스 또는 어플리케이션의 구동을 막는 행위를 금지함.
3. 차단 금지(단말기기 중립성) – ISP 는 망에 해를 주지 않는 한 합법적인 기기를 이용하여 망에 접속하거나 사용하는 이용자를 막을 수 없음.
4. 경쟁 혜택 – 망 사업자, 어플리케이션 사업자, 서비스 사업자, 컨텐츠 사업자 간 경쟁의 혜택을 이용자로부터 박탈하는 행위를 금지함.
5. 불합리한 차별 금지 – ISP 는 합법적인 컨텐츠, 어플리케이션, 서비스를 차별해서는 안 됨.
6. 망관리의 투명성 –ISP 는 이용자, 컨텐츠, 어플리케이션, 서비스 사업자의 보호를 위해 합리적으로 요구되는 망관리 및 다른 기타 조치들과 관련된 있는 그대로의 정보를 공개해야 함.

연방통신위원회(FCC)의 오픈 인터넷 규칙의 목적은 소비자에게 선택의 자유와 함께 표현의 자유를 제공하고 이를 통해 혁신과 경쟁을 촉진하기 위한 개방된 플랫폼을 제공하는데 있다. 하지만 트래픽을 선택적으로 차단할 수 있는 DPI 등 새로운 기술이 발전하면서 인터넷 서비스 제공자가 애플리케이션과 통신의 자유로운 흐름에 개입하고 인터넷 서비스 시장이 경쟁이 심화되면서 공공의 이익이 아닌 상업적 이익을 우선하는 인터넷 서비스 제공자들이 인터넷의 개방성을 저해하고 있다. 이러한 문제점을 해결하기 위한 FCC의 오픈 인터넷 규칙은 투명성(transparency)과 차단금지(no blocking), 불합리한 차별금지(no unreasonable discrimination)로 구성된다.

투명성 원칙에 따라 인터넷 서비스 제공자는 반드시 망관리 현황, 실태 및

114) 이하 내용은 FCC가 의회에 제출한 망 중립성 규제안을 요약하였다. FCC, "NOTICE OF PROPOSED RULEMAKING- Before the Federal Communications Commission Washington, D.C. 20554", 2009, 참조.

115) FCC 망 중립성 원칙의 배경에 관해서는 김천수, 망 중립성에 대한 공법적 고찰, 한국외국어대학교 박사학위논문, 2012, 76쪽 이하 참조.

광대역 서비스의 상업계약 조건 등에 관한 정보를 공개하여야 한다. 차단금지 원칙은 유무선 무선 통신망에 모두 적용되며 망을 이동하는 애플리케이션, 서비스, 컨텐츠의 차단을 금지하고 있다. 마지막으로 불합리한 차별금지 원칙은 인터넷 서비스 제공자의 컨텐츠, 애플리케이션, 액세스 서비스 차별을 금하고 있다. FCC의 오픈 인터넷 규칙의 내용은 2011년 제정된 우리나라 방송통신위원회의 망 중립성 및 인터넷 트래픽 관리에 관한 가이드라인에 많은 영향을 주었다. 우리나라의 망 중립성 가이드라인에 관해서는 제4장에서 상술한다.

가. 투명성

FCC의 투명성 원칙[116]에 따라 인터넷 서비스 제공자는 네트워크 관리 현황, 트래픽 성능, 서비스 가입조건 등에 관한 정보를 투명하게 공개하여야 한다. FCC는 이를 통해 사용자의 선택의 권리가 보호되고 무엇보다도 인터넷 서비스 제공자에 의한 트래픽 제한을 줄일 수 있을 것으로 기대한다. 또한 시장경쟁을 촉진해 네트워크 기반시설에 대한 투자가 증가가 네트워크의 확대로 이어져 많은 사람들이 인터넷을 이용할 수 있게 되는 등 다양한 긍정적인 혜택을 볼 수 있게 된다. 하지만 투명한 공개정보만으로는 인터넷의 개방성을 보장하는 데는 한계가 있기 때문에 FCC는 부족한 점을 보완하기 위하여 차단금지와 차별금지 원칙을 도입하였다.

나. 차단금지

차단금지 원칙[117]은 인터넷 서비스 제공자의 적법한 컨텐츠, 서비스 및 애플

116) 47 CFR 8.3 – Transparency. A person engaged in the provision of broadband Internet access service shall publicly disclose accurate information regarding the network management practices, performance, and commercial terms of its broadband Internet access services sufficient for consumers to make informed choices regarding use of such services and for content, application, service, and device providers to develop, market, and maintain Internet offerings.

117) 47 CFR 8.5 - No Blocking. (a) A person engaged in the provision of fixed broadband Internet access service, insofar as such person is so engaged, shall not block lawful content,

리케이션 차단 금지를 규정하고 있다. 이 원칙은 서비스 제공자와 경쟁하는 음성전화나 애플리케이션의 차단 금지를 명시함으로써 네트워크의 최종사용자뿐만 아니라 인터넷 관련 사업자에게도 자유로운 액세스 권리를 부여하고 있다.

다. 불합리한 차별금지

인터넷 서비스 제공자가 상업적인 이익을 이유로 트래픽을 차별할 수 있다는 점을 우려해 FCC는 불합리한 차별금지 원칙[118]을 도입하였다. FCC는 합리적인 네트워크 관리와 불합리한 차별은 엄연히 다름을 설명하기 위해 합리적인 네트워크 관리의 판단 기준을 제시하였다. FCC는 합리적 차별의 판단 기준으로 정보의 제공의 투명성, 최종 사용자의 통제력(end-user control) 즉, 서비스 선택권, 애플리케이션의 유형을 구분한 차별 및 우선처리 등을 들었다.

3. FCC의 망 중립성 원칙을 둘러싼 법적 분쟁

가. Comcast vs. FCC 사건

2007년, 미국의 거대 ISP 기업 가운데 하나인 컴캐스트(Comcast)사가 사용자 간 파일 공유 시스템인 비트토렌트(BitTorrent)의 트래픽 속도를 선택적으로 늦추었다며 시민운동단체인 Free Press와 Public Knowledge가 FCC에 공식적으로

---

applications, services, or non-harmful devices, subject to reasonable network management. (b) A person engaged in the provision of mobile broadband Internet access service, insofar as such person is so engaged, shall not block consumers from accessing lawful Web sites, subject to reasonable network management; nor shall such person block applications that compete with the provider's voice or video telephony services, subject to reasonable network management.

118) 47 CFR 8.7 - No Unreasonable Discrimination. A person engaged in the provision of fixed broadband Internet access service, insofar as such person is so engaged, shall not unreasonably discriminate in transmitting lawful network traffic over a consumer's broadband Internet access service. Reasonable network management shall not constitute unreasonable discrimination.

불만을 제기하면서 사건이 세상에 알려졌다. FCC는 이러한 속도 제한은 망 중립성 위반이라며 컴캐스트사에 시정 명령을 내렸지만 FCC는 관련 규제 권한이 없다며 즉시 항소하였다. 사건의 쟁점이 된 것은 문제의 본질인 망 중립성이 아니라 FCC의 관할권에 관한 것이었다. 미국 콜럼비아 연방항소법원은 망 중립성 원칙을 위반한 컴캐스트사에 대한 FCC의 제재는 권한을 넘어선 행위라고 판결하였다. 법관 3인의 재판부 전원합의로 나온 이 판결로 망 중립성 정책에 대한 논쟁이 다시 점화되었다.[119]

나. Verizon vs. FCC

거대 통신사 Verizon은 FCC의 오픈 인터넷 규칙이 연방통신법이 규정하고 있는 FCC의 권한을 넘은 것이라며 소송을 제기하였으나, 백악관에서 오픈 인터넷 규칙을 심사하고 있다는 이유로 소송은 기각되었다. 이후 2011년 9월 백악관은 오픈 인터넷 규칙을 승인하고 연방 규칙(Code of Federal Regulations)의 통신부문에 이를 삽입하였다.(Title 47, Part 8) 그러자 Verizon이 다시 소송을 제기했으며 현재 결정이 임박해 있다고 한다.[120]

119) 이 사건 외에도 컴캐스트는 업무용 프로그램인 로터스 노츠(Lotus Notes)의 사용을 제한하거나 속도를 낮추었다는 이유로도 FCC에 제소되었다.

120) WIRED, 2013년 4월 13일자, "We're About to Lose Net Neutrality – And the Internet as We Know It"(http://www.wired.com/opinion/2013/11/so-the-internets-about-to-lose-its-net-neutrality) 참조.

제2절 캐나다의 망 중립성 규제에 관한 논의 전개 과정

Michael Geist[121)]

1. 서 론

망 중립성은 최근 몇 년간 캐나다뿐만 아니라 전세계에서 상당한 관심을 불러일으키고 있다.[122)] 망 중립성의 의미에 대해서는 명확한 정의가 내려져 있지 않지만 망 중립성의 핵심은 인터넷서비스제공자(ISP, 이하 ISP라 함)가 컨텐츠의 출처, 소유 또는 목적지에 따라 컨텐츠와 애플리케이션을 차별하거나 서비스 품질을 떨어뜨지 않고 모두 동등하게 처리하겠다는 약속이다. 콜롬비아 대학교 팀 우(Tim Wu) 교수가 처음으로 망 중립성이라는 단어를 만들었는데[123)], 그는 망 중립성을 개방형 네트워크가 "모든 컨텐츠, 사이트, 플랫폼을 동등하게 처리해야 할 디자인 원칙(design principle)"으로 정의하고 있다.[124)] 다시 말해 중립적인 접근 방식을 채택하려면 ISP가 차별, 선호 또는 컨텐츠에 관계없이 모든 데이터를 동등하게 취급해야 한다는 가장 기본적인 원칙을 엄격히 따라야 할 것이다.

망 중립성 침해의 위법성과 위험성과 관련해서는 이미 오래전부터 문제가 제기되어 왔다. 전문가들은 ISP가 경제적 자기 이익에 굴복해 경쟁 사이트나 서비

121) 제2절은 이 연구과제의 공동연구진인 Michael A. Geist 교수가 집필하였다. Geist 교수는 캐나다 인터넷과 전자상거래법 연구소 소장으로 프라이버시와 지적재산권에 관하여 활발한 연구를 수행하였으며, 약 2008년 이후부터는 망 중립성과 이에 대한 법정책에 관하여 적극적인 연구를 수행하고 있다. 캐나다의 프라이버시 커미셔너의 자문위원이며, 블로그 및 언론에 칼럼을 발표하는 등 다양한 분야에서 활발하게 활동하고 있다.

122) "Battle over 'net neutrality' arrives in Canada", CBC (2006년 11월 2일); "NDP calls for net neutrality" 참조. CBC (2008년 4월 21일) online: CBC (http://www.cbc.ca/); David Bazan et al, Audio-CD: Rock The Net: Musicians For Network Neutrality (Thirsty Ears: 2008); Canadian Liberty Association, "2008 Election Campaign Kit" at 7, online: CLA (http://www.cla.ca/); and "Liberals speak out in support of net neutrality", Liberal Party Newsroom(2009년 6월 19일) online: Liberal Party of Canada (http://www.liberal.ca/).

123) "Net Neutrality Star Tim Wu Joins Federal Trade Commission as Senior Policy Advisor", Forbes (2011년 10월 2일) 참조: Forbes http://www.forbes.com/).

124) Tim Wu et al, "Network Neutrality FAQ", online: Tim Wu (http://timwu.org).

스에서 오는 데이터를 차단하거나 속도를 늦추는 방법으로 "패킷 선호(packet preferencing)"을 하게 될 것이라고 우려 했다.[125] ISP는 자사의 네트워크를 이동하는 컨텐츠의 내용에 상관없이 이를 전달하는 매개자(intermediary)의 역할(예를 들면 끝과 끝을 연결하는)을 할뿐이라고 주장한다. 하지만 ISP가 인터넷 전화 서비스, 음악 다운로드 서비스 및 기타 부가가치 컨텐츠를 경쟁적으로 제공하고 있기 때문에 홈 네트워크에 특혜를 부여하고 있다는 점은 부인하기 힘든 사실이다.

망 중립성과 관련하여 몇 가지 문제가 제기 되었는데 특히, "이중 인터넷(two-tier Internet)"에 대해 우려가 제기되고 있다. 이중 인터넷이란 ISP가 속도가 빠른 네트워크를 구축해 이른바 "빠른 라인(fast line)"과 일반 라인으로 나눈다. 빠른 라인은 일반 라인보다 속도가 훨씬 빠르지만 추가 비용이 청구되며, 반대로 추가 비용이 없는 일반 라인은 트래픽 속도가 느리다는 단점이 있다. ISP는 이러한 이중 인터넷 구조로 트래픽을 차별하는 것이다. 이러한 이중 인터넷은 경쟁 약화의 가장 큰 원인이 될 수 있다. 예를 들면, 대형 스튜디오의 텔레비전 프로그램과 영화는 이들 스튜디오가 빠른 라인(또는 ISP와 같은 소유주)을 이용하기 때문에 소비자에게 더 빨리 제공될 수 있지만 반면에 이보다 규모가 훨씬 작은 소규모 스튜디오의 영화, 프로그램 또는 사용자 생성 컨텐츠는 느린 라인을 이용해 더딘 속도로 최종 사용자에게 전달되게 될 것이다. 경쟁은 디지털 경제의 확산과 밀접한 연관이 있다. 전자상거래 기업과 투자자들은 기업의 크기나 규모에 상관없이 모든 네트워크를 동일하게 취급하는 것으로 알려져 있는 망 중립성에 크게 의존하고 있다. 이러한 망 중립성을 통해 재원이 많은 기업이 아니라 최고의 상품과 서비스를 제공하는 기업이 시장을 점할 수 있는 것이다. 망 중립성과 관련해 또 다른 문제는 온라인 이용자의 프라이버시, 언론의 자유와 같은 법률로 보장하는 기본권과 관련이 있다. 인터넷제공자가 선택적이

125) David P Reed, Jerome H Saltzer & David D Clark, "Active Networking and End-To-End Arguments"; Mark A Lemley & Lawrence Lessig, "The End of End-to-End: Preserving the Architecture of the Internet in the Broadband Era"; and David Clark & Marjory Blumenthal, "Rethinking the Design of the Internet: The End to End Arguments vs. the Brave New World", online: The Center for Internet and Society (http://cyberlaw.stanford.edu/).

고 인위적으로 일부 컨텐츠나 애플리케이션의 접근을 막거나 속도를 늦추도록 허용해야 한다는 주장은 경쟁을 약화시킬 뿐만 아니라 캐나다 권리자유헌장(Charter of Rights and Freedoms)에서 보장하는 프라이버시와 언론의 자유를 침해하는 것이다. 또한 프라이버시에 대한 우려는 이른바 "트래픽 셰이핑(traffic shaping-통신량 조절)" 등으로 인한 투명성 결여로 인해 더욱 심화될 것이다.

캐나다에서는 이동통신 사업자인 Telus가 노동쟁의 기간 동안 일부 노조를 지지하는 웹사이트에 대한 접근을 차단(차단하는 과정에서 기타 600여개 이상의 사이트에 대한 접근도 차단)한 것을 비롯해 통신사업자인 Rogers가 BitTorrent[126] 등 일부 애플리케이션의 속도를 제한하는 등 망 중립성을 침해하는 일련의 사건이 발생하면서 기업과 사용자 모두가 계속해서 우려의 목소리를 내고 있다. 이 사건들에 대한 구체적인 내용은 후술한다.

온라인 컨텐츠에 대한 망 중립성 측면에서 캐나다 국내법은 몇 가지 흥미로운 문제를 제기하고 있다. 캐나다 권리자유헌장은 직접적으로 민간 기업에 적용되지는 않지만 캐나다 국민의 "생각, 믿음, 의견 및 표현의 자유"를 보장한다. 캐나다 대법원은 권리자유헌장에서 명시하고 있는 표현의 자유에 관한 Ford v. Attorney General(Quebec) 사건에서 표현의 자유는 말하는 사람을 넘어 듣는 사람의 자유도 의미한다는 기념비적인 판결을 내렸다[127]. 인터넷제공자는 권리자유헌장의 적용대상이 아니지만 캐나다 기업이 이러한 원칙을 준수할 것으로 예상하는 것이 타당할 것이다.

캐나다 전기통신법(Telecommunication Act, 이하 통신법이라 함)은 지속적으로 문제가 제기되고 있는 규제절차에 관한 두 개 조항은 망 중립성과 밀접한 관련이 있다.[128] 먼저 통신법 제27조 제2항은 통신 서비스 제공에 있어 부당한 차별을 금지하고 있다. 접근이 차단된 웹사이트가 정보통신 서비스에 해당된다 할지라도 동 조항은 주로 경쟁 서비스 부문에 적용된다. 다음으로 제36조는 "위원회(캐나다 라디오 텔레비전 전기통신 위원회(Canadian Radio-television Telecommunications

126) Michael Geist's testimony in House of Commons, Standing Committee on Industry, Science and Technology, Evidence, No 047 (2007년 2월 26일) at 1635 참조.

127) Ford v. Attorney General (Quebec), [1988] 2 SCR 712.

128) Telecommunications Act, SC 1993, c 38.

Commission)가 승인한 경우를 제외하고 캐나다 통신사는 컨텐츠를 제한하거나 일반 사용자를 위해 통신사가 제공하는 정보통신의 의미 또는 목적에 영향을 미쳐서는 안 된다"고 명시하고 있다."[129] 여기서 말하는 "제한" 및 "의미에 미치는 영향"의 범위를 자세히 알려면 동조항의 의미가 명확하고 구체적이어야 한다.

망 중립성에 대한 계속되는 불만과 망 중립성과 관련해 적용할 수 있는 국내법의 불명확성으로 인해 캐나다 ISP, 컨텐츠 크리에이터, 이용자들을 위한 트래픽 관리 실무의 적법성에 대한 명확한 지침이 없었다. 지침의 부재로 인해 캐나다는 세계 최고 수준의 망 중립성 정책 개발을 촉진하는 규제절차를 마련하게 되었다.[130] 본 연구는 캐나다의 망 중립성 이슈 및 정책에 관한 것으로 먼저 정책의 발전을 살펴보고자 한다. 제2절에서는 디지털 권리 단체가 주목하고 국가 차원에서의 규제 수립의 단초가 된 초기 망 중립성에 대한 적신호가 무엇인지 알아보고자 한다. 제3절에서는 2006년부터 2009년까지 전개된 망 중립성 정책수립 요구 증가를 중점적으로 다루어 보고자 한다. 제4절에서는 망 중립성을 직접적으로 언급하고 있는 인터넷 트래픽 관리정책에 대한 규제 공청회를 살펴보고자 한다. 마지막으로 제5절과 제6절에서는 망 중립성 관련 정책 및 법집행의 문제점을 분석해보고자 한다.

---

129) 역설적이게도, 2001년 일부 사이트 접근 차단은 캐나다의 망 중립성에 있어 중요한 선례가 된 Telus는 자신들은 시스템을 이용하는 콘텐츠를 제한하거나 이에 영향을 미칠 수 없는 단순히 중간자이기 때문에 인터넷 서비스 제공자(ISP)에게는 책임이 제한된다는 주장의 근거로 제36조를 들었다. ISP는 정부에 제출한 저작권정책 의견서에 "ISP 정보의 전송을 시작하지 않을 뿐만 아니라 전송의 수신자를 선택하지도 않고 전송되는 정보를 선별, 제한, 수정 또는 변경하지 않는다"고 덧붙였다. [Telus Communications Inc, "Submission to the Departments Industry Canada and Canadian Heritage: Response to Consultation on Digital Copyright Issues" (2001년 9월 14일), online: Industry Canada (http://strategis.ic.gc.ca/eic/site/crp-prda.nsf/eng/home)] 사실 인터넷 사용자들을 위한 혜택 때문에 망 중립성은 ISP가 고객을 확보하고 새로운 인프라에 대한 투자를 확보하고 경쟁과 혁신을 촉진하는데 있어 중요한 역할을 하였다. 연구에 따르면 광대역 서비스 제공자의 서비스 확대 촉진을 위한 인센티브는 망 중립성 제도가 있을 때 훨씬 더 크다고 한다. 이는 망 중립성 제도 하에서는 서비스 확대를 위한 인센티브가 제한된다는 ISP의 주장과는 대치되는 것이다.

130) Mark Goldberg, "Canada Leads World With Net Neutrality Regulatory Framework", CircleID (2009년 10월 21일) online: CircleID (http://www.circleid.com/).

2. 2004~2006년: 망 중립성 적신호

2004년, 캐나다에서는 처음으로 망 중립성에 적신호가 켜지는 사건이 발생하였다. 2004년, 캐나다 라디오 텔레비전 전기통신 위원회(Canadian Radio-television Telecommunications Commission- CRTC, 이하 방송통신위원회라 함)가 인터넷 전화(voice-over-IP, VOIP) 서비스와 관련해 실시한 공개 협의에서 캐나다 주요 통신사의 모기업은 제3자에 의한 서비스 제공에 대해 호의적인 입장이 아님을 역력히 드러냈다. 퀘백주내 최대 통신사인 Videotron을 소유한 Quebecor는 위원회에 Vonage와 같은 인터넷 기반 전화서비스가 결코 시설기반 경쟁의 발전에 있어 어떠한 도움도 되지 못할 것이라고 주장했다.[131]

일 년 뒤, 캐나다 선두 통신사업자 중 하나인 Telus는 당시 노조와 노사분쟁 중이었으며 통신사 노조를 지지하는 사이트 "Voices for Change"에 대한 접속을 차단했는데 이러한 특정 사이트에 대한 접속차단은 전례가 없는 일이었다. Telus는 접근 차단 이유로 해당 사이트가 영업상 기밀정보 및 일부 직원의 프라이버시 및 보안과 관련된 사진을 게재하고 있었기 때문이라고 차단 이유를 설명했다.[132] 그럼에도 불구하고 해당 사이트는 Telus 네트워크가 아닌 다른 네트워크를 이용해서는 접근할 수 있었기 때문에 접근차단은 사실상 아무런 효과가 없었다. 또한 Telus 네트워크에서도 프록시 서비스(proxy service)를 이용하면 해당 사이트에 접근할 수 있었다. 이후 Telus는 해당사이트에 Telus 피고용인를 위협할 목적으로 콘텐츠를 게재하지 못하도록 하는 내용의 법원 명령을 받아 냈지만 일방적인 접근 차단은 오히려 수많은 법적 문제를 일으키는 계기가 되었다. Telus는 이용약관에 따라 회사는 콘텐츠를 차단할 수 있는 권리가 있다고 주장했다. 이러한 주장이 당시 약 1백만 명에 달하는 가입자에게 적용된다 할지라도

131) Canadian Radio-Television and Telecommunications Commission (CRTC), Telecom Public Notice CRTC 2004-2: Regulatory framework for voice communication services using Internet Protocol, vol 3 (Gatineau: CRTC, 2004) at paras 4470-71 참조.

132) "Telus cuts subscriber access to pro-union website", CBC (24 July 2005) online: CBC (http://www.cbc.ca/); and Ian Austen, "A Canadian Telecom's Labor Dispute Leads to Blocked Web Sites and Questions of Censorship", The New York Times (2005년 8월 1일) online: The New York Times (http://www.nytimes.com) 참조.

문제는 이러한 차단이 인터넷의 근간에서 이루어졌고 Telus가 도매 서비스 제공자(wholesale provider)이며 네트워크 통신사인 Telus의 네트워크를 이용하는 다른 ISP(및 이용자)의 접근을 차단했다는 점에 있다.

Telus의 조치는 망 중립성 침해와 관련해서만 문제가 되는 것이 아니다. 캐나다 최대 통신 사업자 Rogers Communication(이하 로저스라 함)은 조용히 "트래픽 셰이핑" 기술을 이용해 BitTorrent(비트토렌트) 등과 같은 P2P 서비스에 대한 접근 및 iTunes 등 팟캐스트 다운로드를 제한하였다. 캐나다에서는 BitTorrent가 합법이며 수많은 오픈소스 소프트웨어 개발자와 독립 영화감독, 아티스트가 이와 같은 P2P 서비스를 이용하고 있음에도 이러한 트래픽 셰이핑이 이루어지고 있었다. 로저스는 이러한 애플리케이션이 이용할 수 있는 광대역을 제한함으로써 캐나다 아티스트들이 자신의 작품을 널리 알릴 수 있는 기회를 빼앗았을 뿐만 아니라 캐나다 내 오픈소스 소프트웨어의 개발을 저해했다.[133]

이러한 트래픽 셰이핑에 대응하기 위해 많은 파일 공유 애플리케이션은 데이터 패킷의 콘텐츠 분석을 어렵게 하기 위해 콘텐츠를 암호화하기 시작했다. 그 결과 끊임없는 기술적인 "추격게임(cat and mouse game)"이 시작되었고, ISP의 속도저하를 피하기 위한 더욱 높은 수준의 암호설정으로 이어졌다.[134] 하지만 다른 한편으로는 암호설정으로 인해 ISP가 다른 암호화 애플리케이션(이메일, 원격 데스크톱 애플리케이션 등)을 암호 설정이 되어 있는 파일 공유 콘텐츠로 착각해 이러한 애플리케이션까지도 속도를 늦추게 할 가능성이 높아졌다. 로저스의 트래픽 셰이핑은 또한 이용자 측면에서도 심각한 문제가 될 수 있다. 예를

133) P2P 파일 공유는 또 다른 부차적인 피해를 가한다. Glance 네트워크의 CEO는 "일부 웹 컨퍼런싱 제공다는 열악한 트래픽 관리 정책으로 세계 일부 지역에서는 서비스의 속도가 매우 늦다"고 지적했다. 또한 "ISP가 트래픽 관리를 거부하는 경우가 많아 서비스 복구를 위한 문제점 파악에 있어 상당한 어려움을 겪는다." [Rich Baker, "How Network Non-Neutrality Affects Real Businesses" (2008년 3월 24일), online: Xconomy (http://www.xconomy.com/)].

134) "Canada" under "Bad ISPs" in Vuze Wiki (http://wiki.vuze.com/). In the U.S., Comcast engaged in similar traffic shaping [Peter Svensson, "Comcast blocks some Internet traffic", NBC News (2007년 10월 19일) online: NBC News (http://www.nbcnews.com)] 참조. [Dan Frommer, "BitTorrent, Comcast (CMCSA) Shake Hands, Downloaders Still Screwed", Business Insider (2008년 3월 27일) online: Business Insider <http://www.businessinsider.com/>] 참조.

들면, 기업은 자신들이 지불한 비용만큼 서비스를 완전히 이용할 수 있는 소비자의 서비스 이용능력은 저해하고 있는 반면 빠른 데이터 전송속도와 최대용량 등의 표현을 사용해 서비스를 광고하는 것은 받아들이기 쉽지 않다.[135]

망 중립성 논란에서 빼놓을 수 없는 캐나다 최대 인터넷 서비스 제공자인 Bell Canada(이하 Bell이라 함)은 과도한 광대역 사용 문제를 해결하기 위해 네트워크를 관리하고 있다고 광고해 트랙픽 셰이핑 문제를 새롭게 제기했다. Bell사가 직접적으로 네트워크 관리를 공개했음에도 불구하고 비난은 잠잠해지지 않았다. 좀더 자세히 살펴보면, Bell의 무제한 데이터 요금제는 "멀티미디어 스트리밍, 인터넷 전화 또는 네트워크 용량을 과도하게 사용하는 기타 애플리케이션" 금지 등 소비자에게 불리한 조건을 포함하고 있다.[136] Bell은 BitTorrent 등 P2P 애플리케이션에 대해 트래픽 셰이핑을 실행하고 있음을 인정했다.[137]

Bell의 인터넷 서비스 제공과 관련해 가장 논란이 되는 부분은 바로 기간통신사업자(wholesale partner)에게 알리지 않고 이루어진 기간 서비스(wholesale service)의 속도제한이다.[138] 트래픽 속도를 제한하기 위해 Bell은 "심층패킷분석(deep packet inspection, 이하 DPI라 함)"을 네트워크에 설치하였다. DPI를 이용해 ISP는 네트워크를 이동하는 콘텐츠의 내용을 확인할 수 있어 콘텐츠에 따라 트래픽을 관리할 수 있는데 이러한 트래픽 속도 제한은 경쟁과 관련해 다음

---

135) 일부 가입자들은 Rogers의 트래픽 셰이핑을 "광대역 망 관리"로 망 중립성을 침해하고 있는 것으로 보지 않는다. [Mark Evans, "Rogers: It's Bandwidth Management; Not Throttling"(2007년 4월 13일), online: Mark Evans Tech (http://www.markevanstech.com)] 참조. 이러한 생각은 트래픽 쉐어링과 망관리의 차이점을 구별하지 않기 때문인 것으로 보인다. 트래픽 쉐어링은 특정한 애플리케이션과 콘텐츠에 대한 접근을 어렵게 한다. 이는 기술적 제한이 "합리적"인가에 관한 문제이다. 트래픽 쉐어링이 많은 기타 암호화 데이터에 미치는 영향을 고려해 보았을 때, 소비자들이 월간 정액제를 지불하고 있고 이러한 제한이 일부 애플리케이션에 불필요하게 적용되고 있다는 사실은 기술 제한이 망 중립성 침해의 근거가 되지 않음을 보여주고 있다.

136) Michael Geist, "Canadians deserve better ISP transparency", The Toronto Star (2007년 10월 8일) online: The Toronto Star (http://www.thestar.com/) ; Bell crimps P2P file-sharing during peak hours, CBC (2008년 3월 25일) online: CBC (http://www.cbc.ca) 참조.

137) Ryan Paul, "BitTorrent blocking goes north: Canadian ISP admits to throttling P2P", Ars Technica (2007년 11월 5일) online: Ars Technica (http://arstechnica.com/) 참조.

138) Karl Bode, "Bell Canada Throttles Wholesalers, Doesn't Bother To Tell Them", DSL Reports (2008년 3월 24일) online: DSL Reports (http://www.dslreports.com/).

의 3가지 문제점을 야기하였다.

먼저, DPI는 ISP의 경쟁력 특히 온타리오와 퀘백주에 있어 지대한 영향을 미치게 될 것이다. 사실, 방송통신위원회는 Bell과 같은 대형 인터넷 서비스 제공자에게 정해진 가격에 재판매사업자(retail)에게 임대하도록 함으로써 캐나다의 제한된 ISP 경쟁을 해결하려고 노력하였다. 대규모로 이루어지는 선택적 속도제한은 개별 서비스제공자가 자신들이 제공하는 서비스를 차별화 할 수 있는 능력을 제한하게 되고 따라서 시장의 경쟁력까지 약화되게 된다. 둘째, 경쟁에 대한 우려는 기업에서 사용하는 가상 사설 네트워크(virtual private network, VPN) 및 방송사에서 이용하는 비디오 스트리밍과 같은 ISP에서 제공하는 서비스에 영향을 미치게 될 것이다. DPI와 속도제한을 통해 Bell은 기업들이 당연하게 여기는 서비스에 프리미엄 요금제를 실시하려 할 것이고 그렇게 되면 비용이 증가하게 되고 재판매 사업자가 사라지게 될 것이다. 셋째, 속도제한으로 인해 문화가 바뀌게 될 것이다. 주요 ISP가 모든 고객에게 더 나은 서비스를 제공하려면 속도를 제한할 수밖에 없다고 주장하지만 케이블과 위성 TV 기업이 주문형 비디오 시스템(video on demand)을 소비자에게 판매하게 됨에 따라 비디오 시장에 막대한 영향을 미치게 될 것이다.[139]

2008년 Bittorrent 프로토콜을 기반으로 한 Vuze가 실시한 연구가 발표되면서 캐나다의 또 다른 서비스 제공자 Cogeco(이하 코지코)에게 세간의 관심이 집중되었다. ISP의 네트워크 관리 기술을 추적하기 위해 Vuze는 이용자들이 네트워크 개입을 측정할 수 있는 플러그인 방식을 개발했다. 이러한 개입(예를 들면, 메시지 재설정)은 일상적인 네트워크 활동 중에서도 발생할 수 있으며 P2P 파일 공유를 방해하기 위해 잘못된 메시지를 생성할 수도 있다. 방대한 자료를 바탕으로 Vuze는 속도제한을 하는 주요 ISP의 순위를 매겼다. 메시지를 가장 많이 재설정한 회사는 미국 통신사인 Comcast(컴캐스트)였고 다음으로 퀘백과 온타리오에 인터넷 서비스를 제공하는 캐나다 통신사 코지코가 뒤를 이었다. 더욱이 캐나다 통신사 중 이와 관련해 좋은 점수를 받은 제공자는 단 한 곳도 없었다.[140]

---

139) Bell이 트래픽 관리 대중의 좋지 않은 여론으로 인해 트래픽 셰이핑이 역효과를 낼 수 있다고 인정한 것은 주목할 만하다. [Bell Canada, "Management's Discussion and Analysis: Risks That Could Affect Our Business and Results", online: Bell Canada (http://www.bce.ca/)] 참조.

3. 2006~2009년: 망 중립성 규제에 대한 요구 증가

캐나다에서는 웹사이트 차단, 패킷 또는 경쟁 인터넷 통신사의 서비스에 대한 차별, ISP의 스팸 차단 효율성에 대한 의구심 및 법집행기관의 감독 가능성 측면에서 ISP의 가입자의 프라이버시 및 개인정보가 담긴 데이터 보호에 대한 우려가 제기되는 동시에 국가차원에서 새로운 ISP 규제체계(accountability framework)의 시행을 요구하는 목소리가 더욱 커졌다. 망 중립성과 관련하여 제한된 광대역망의 사용 경쟁 심화 및 통합 확대에 따라 서비스 제공자들이 경쟁 서비스 제공자 또는 기업에 비해 자사(또는 연계 컨텐츠)에 대해 경제적 혜택을 주는 상황에서[141], 네트워크 서비스 제공에 있어 컨텐츠의 중립성은 규제감독 및 불이행 시 이에 대한 엄중한 처벌을 명시하고 있는 캐나다 국내법에 따라 네트워크 서비스 제공에 있어 비차별성은 확고히 지켜져야 할 절대적인 기본 원칙이라는 주장이 제기되었다.

더욱 엄격한 규제시행에 대한 요구가 거세짐에 따라 캐나다 정보통신정책에 대한 2006년 성과분석 보고서(2006 Telecommunications. Policy Review Panel Report[142])는 망 중립성 기준 보호에 관한 조항 또는 "오픈 액세스(open access) 조항"을

---

140) 본 연구는 인터넷에서 볼 수 있음: "First Results from Vuze Network Monitoring Tool" (2008년 4월 18일), online: TorrentFreak (http://torrentfreak.com/images/vuze-plug-in-results.pdf). See also "Cogeco ranks poorly in internet interference report", CBC (2008년 4월 22일) online: CBC (http://www.cbc.ca/). 일부 연구자들은 연구방법 및 재설정 데이터의 관련성에 대해서 의문을 제기하였다 [Iljitsch van Beijnum, "Vuze says some ISPs abuse TCP resets; data not that clearcut", Ars Technica (2008년 4월 23일) online: Ars Technica (http://arstechnica.com/)] 참조

141) 2009년 Bell은 가입자에게 영화와 텔레비전 프로그램에 대한 온란인 접근을 제공하는 Bell TV 온라인 서비스에 집중하겠다는 계획을 발표하였다. [Christine Persaud, "Bell Silently Closes Online Video Store", Market News (2009년 9월 6일) online: Market News (http://www.marketnews.ca/)]. 가입자들이 무제한으로 Bell TV 온라인에서 제공하는 컨텐츠에 무제한으로 접근할 수 있지만 Bittorrent 등을 통한 경쟁 컨텐츠에 대한 접근을 제한함에 따라 Bell의 접근 제한과 관련해 우려가 제기되었다.

142) 정보통신정책에 대한 성과분석 보고 패널은 2011년 4월 11일 설립되었다. 캐나다 연방산업부는 캐나다의 통신정책 및 규제제도 검토를 위해 Gerri Sinclair, Hank Intven, André Tremblay를 패널로 선정했다. 또한 패널에 캐나다내 국제 경쟁 통신산업에 대한 권고안을 마련할 것을 요청했다. 패널이 제시한 권고안은 시장지향적인 것이지만 보고서는 망 중립성, 유비쿼터스 광대역 접근, 프라이버시, 스팸, 소비자 보호 등 소비자와 관련해 중요한 사안에 대한 내용도 포함하고 있다.

신설할 것을 요구했다. 보고서의 권고안은 다음과 같다.

"인터넷에 접근할 수 있는 모든 통신 네트워크를 통해 공개된 인터넷 애플리케이션이나 소비자가 직접 선택한 컨텐츠에 접근할 수 있는 소비자의 권리를 확고히 할 수 있도록 전기통신법(Telecommunications Act)은 개정되어야 한다. 따라서 수정안은 다음을 포함해야 한다.

(a) 방송통신위원회에 이러한 소비자의 접근권을 보장하고 집행할 수 있는 권한 부여

(b) 인터넷 접근 제공과 관련해 합리적인 기술 제약 및 효율성 고려, 및

(c) 형법, 저작권법 및 방송통신법 등 인터넷 접근에 관한 법적 제약"[143]

분석 결과 보고서를 작성한 패널은 망 중립성과 관련해 입법까지는 필요없다고 주장한 Telus와는 의견을 달리했다. 패널은 "오픈 액세스는 애플리케이션과 컨텐츠에 대한 접근 차단 및 상당하고 고의적인 서비스질 저하와 같은 사례를 검토할 수 있는 권한을 규제당국에 부여하는 정당성의 근거가 되기 때문에 매우 중요하다"는 결론을 내렸다.[144]

또한 보고서는 이른바 통신법에 따라 프라이버시를 보호하고 방송통신위원회가 프라이버시 보호에 있어 보충적인 역할을 해야 한다는 견해를 비롯해[145] 및 2010년까지 캐나다내 보편적인 광대역 접근을 목표로 한 새로운 국가 광대역 전략 수립에 대한 권고안을 포함하고 있다.[146]

---

143) Telecommunications Policy Review Panel, Final Report 2006, (Ottawa: Industry Canada, 2006) 6-18.

144) Ibid.

145) Ibid at 6-13.

146) Ibid at 7-17 참조. 정보접근법(Access to Information Act)에 따라 수집한 문서에 따르면, 2006년 봄 캐나다 연방사업부가 보고서의 권고안의 완전한 시행에 대한 업계 지지를 확인하기 위해 보고서에 대해 관련기업과 비공식 협의를 진행했다고 한다. 산업부장관에게 제출된 제안서를 보면 산업부가 "관련 기업에게 권고안의 상위 5개와 하위 5개를 검토할 것을 요청"했다고 정부 관계자들이 진술했으며 "대부분의 회사가 패널의 권고안을 개별적으로 시행한다면 이에 반대하기 때문에 권고안을 종합적으로 시행되어야 한다는 결론을 내렸다." [Michael Geist, "Videotron Rekindles Fear of a Two-Tier Internet" (2006년 11월 6일), online: Michael Geist's Blog (http://www.michaelgeist.ca/)].

2006년까지 방송통신위원회는 망 중립성과 관련한 문제를 기피하는 것으로 보였다. 사실, 위원회는 통신산업에 대한 규제를 적극적으로 완화하는 등 망 중립성과는 반대 방향으로 움직였다.[147] 위원회의 이러한 방향설정은 Telus의 특정 사이트 접근 차단과 같은 망 중립성 위반과 관련해 캐나다 국내법에 있어 상당한 혼란을 야기했다. ISP에 대한 패킷 차별 또는 트래픽 셰이핑 등에 대한 정보를 공개할 의무가 없었다는 점에서 특히나 이러한 모호성이 문제가 되었다.

2006년 캐나다 공영방송인 캐나다 방송공사(Canadian Broadcasting Corporation)는 소비자의 엔터테인먼트 현황에 대해 방송통신위원회에 보고서를 제출하였다. 비록 보고서에는 망 중립성이라는 단어를 직접적으로 사용하고 있지는 않지만 망 중립성과 관련해 우려를 제기하고 있다. 방송공사의 보고서 내용은 다음과 같다.

"광대역 액세스 공급자가 인터넷 동영상 연결에 사용할 수 있는 광대역을 관리함에 있어 혜택이 있을 수 있기 때문에 인터넷 동영상 관련 사업 사례 분석은 매우 복잡하다. 캐나다 케이블 회사는 케이블 회사의 운영상의 특혜에 따라 서비스별로 전송역량을 차등 할당하는 "광대역 셰이핑(bandwidth shaping)"을 하고 있다. 이러한 광대역 셰이핑을 통해 전송역량을 효율적으로 사용할 수 있다. 또한 광대역 셰이핑은 케이블 가입자에 대한 일반 텔레비전 프로그램 전송, VOD 또는 케이블 회사 소유의 인터넷 동영상 서비스 제공 등 서비스 내용이 무엇이든 제3자 제공자의 인터넷 동영상이 케이블 회사의 사업에 위협이 되지 않도록 할 수 있다. 이렇게 복잡한 상황으로 인해 인터넷 동영상이 상업적으로 동영상 컨텐츠를 제공하는 주요한 방법이 될 수 있는지는 명확히 확인할 수 없다."[148]

방송공사의 보고 내용은 망 중립성에 실질적으로 부합하는 것으로 캐나다의 공영 방송사가 "관망"식 규제접근에 반대하고 있음을 보여준다. 반면, 대형 ISP는 망 중립성 관련 입법에 반대하고 있다. 예를 들면, Bell 캐나다는 망 중립성

147) "Review panel takes step in right direction", National Post (2006년 3월 23일) online: National Post (http://www.nationalpost.com/) 참조.

148) "CBC Reporting on Today's Entertainment Trends", Slyck News (2006년 9월 9일) online: Slyck News (http://www.slyck.com/) 참조.

은 "규제가 아닌 시장원리에 따라 결정되어야 한다"고 주장하고 있다.[149]

기타 시민사회단체와 전문가들은 망 중립성을 지지하고 있다. 예를 들면, 통신정책포럼(Alternative Telecommunications Policy Forum)은 "네트워크 운영자, 즉 광대역 인터넷 서비스 제공자는 자신들의 재원 또는 소유권에 기초해 광대역 인터넷 서비스에 있어 컨텐츠, 애플리케이션, 또는 서비스를 차별해서는 안 된다"는 내용의 지침서 초안을 마련하였다.[150] 하지만 일반 대중은 망 중립성 관련 사안에 대해 무관심하며 망 중립성에 대한 논의는 "통신사 압력단체"가 이끌고 있다.[151]

망 중립성 입법에 반대하는 사람들은 시장의 경쟁에 의해 정부 개입의 필요성이 사라지게 될 것이며 현실적으로 캐나다의 광대역 서비스 시장은 아무리 좋게 말해도 소수가 과점하고 있다고 주장한다. 캐나다 국민의 선택은 제한되어 있다. 도시에 거주하는 소비자는 차별 없는 케이블과 전화 인터넷 패키지 중에 선택할 수 있는 반면 농촌지역에 거주하는 소비자의 경우 광대역 서비스와 관련해 전혀 선택권이 없는 경우가 대부분이다. 또한 광대역 네트워크에 접근할 수 있는 소비자는 언제나 가격 인상과 서비스 제한이라는 선택에 직면한다.

반면 연방정부는 망 중립성 관련 사안을 계속해서 직시하고 있다는 공식입장을 발표했지만 ISP의 시장 주도적 분쟁에 동조하는 것처럼 보인다. 정보접근법에 따라 입수한 일련의 정부문서[152]를 보면 2007년 초 정부는 게이트키퍼(gatekeeper) 역할을 자청하지만 실상은 컨텐츠 사용량에 따라 요금을 부과하고자 하는 주요 통신사의 의도를 명확히 알고 있었다.

---

149) "Battle over 'net neutrality' arrives in Canada", CBC (2006년 11월 2일) online: CBC (http://www.cbc.ca/) 참조.

150) Andrew Clement et al, Connecting Canadians: Investigations in Community Informatics (Edmonton: AU Press, 2012) at 460.

151) Bryan Zandberg, "Canada Sleeps Through War to 'Save the Internet'", The Tyee (2007년 1월 17일) online: The Tyee (http://thetyee.ca/) 참조.

152) "Does the Minister intend to allow telecommunications companies to determine the content that its customers can and cannot access by imposing special rates, undermining net neutrality?" Question Period Card in Telecommunications Policy Branch, Network Neutrality – Questions and Answers, (Ottawa: Industry Canada, 2006) 참조.

"Bell, Telus 등 캐나다 통신사는 인터넷 컨텐츠 전송에 있어 점점 더 많은 역할을 하고자 한다. 컨텐츠 전송 매개체인 통신사는 통신사가 자신들의 역할에 대해 요금을 부과할 수 있는 자유가 있는 컨텐츠의 게이트키퍼가 되어야 한다고 생각한다."

하지만 이러한 정부 문서를 통해 캐나다 정부가 망 중립성과 관련해 ISP의 입장을 받아들이려는 경향을 보이고 있음을 알 수 있다.

"많은 시사평론가들은 망 중립성에 대한 논의가 이를 찬성하는 진영과 반대하는 진영의 실제 주장보다 더욱 확대되어 있고 복잡하다고 지적한다. 먼저, 인터넷은 데이터 전송에 있어 결코 중립적이거나 평등할 수 없다. 지금까지 인터넷의 진화를 살펴보면 새로운 애플리케이션과 이용자의 증가하는 요구에 따라 인터넷 설계와 운영이 이루어지고 있고 비록 일부 이용자들만이 과도하게 데이터를 사용하고 있지만, 모든 가입자들을 위해 일정한 서비스 수준을 보장하려면 '트래픽 셰이핑'을 비롯해 차별적인 컨텐츠 배치, 네트워크 남용을 방지하기 위한 필터링과 차단을 포함해 상당한 수정이 수반되어야 한다."[153]

다시 말해, 민간 기업간의 '계약상의 합의' 측면에서건 또는 산업의 독자생존을 위한 '기술적인 조치' 측면에서건 "트래픽 셰이핑"을 만들어 냄으로써 정부는 망 중립성과 관련해 불간섭주의적 접근방식을 선택했다. 이러한 정부 정책으로 인해 "최대한 실현 가능한 정도까지 인터넷 인프라의 진화, 투자, 혁신이 시장원리에 따라 형성되게 되었다." 정부에 따르면 망 중립성 입법에 대한 논의는 "시기상조"였다.[154]

하지만 놀랍게도 캐나다는 국제 망 중립성 정책 수립에 있어 활발한 역할을 하고 있다. 2006-2007년, 경제협력개발기구(OECD)는 "인터넷 트래픽 우선순위화"라는 제목의 보고서를 작성하였다.[155] OECD 회원국으로 활발한 활동을 하고

153) 2007년 2월 19일 Maxime Bernier 산업부장관은 산업, 과학, 기술 상임위원회에서 했던 발표에서도 이와 비슷한 발언을 하였다.

154) 정부는 "통신사 개혁"에 대한 지지를 보여주는 여론조사에 근거해 정부입장을 정당화하는 것 같다. [House of Commons Debates, 39th Parl, 1st Sess, No141 (2007년 2월 7일) at 1455].

155) OECD, "Working Party on Telecommunication and Information Services Policies – Internet Traffic Prioritisation: An Overview (DSTI/ICCP/TISP(2006)4/FINAL)" (2007년 4월 6일), online: OECD (http://www.oecd.org/internet/ieconomy/38405781.pdf).

있는 캐나다가 초안 작성에 참여하였다. OECD 보고서는 ISP의 반독점 행위, 정보접근 저해 가능성, 컨텐츠 모니터링으로 인한 프라이버시 침해 가능성을 지적하고 있다. 또한 본 보고서는 비록 경쟁으로 반경쟁적인 행위에 따른 이점을 상쇄하는 국가로 캐나다를 직접적으로 언급하지는 않았지만 활발한 경쟁이 이러한 우려를 잠재우는데 도움이 될 것이라고 기술하고 있다.[156]

망 중립성에 대해 논하려면 그 논쟁의 시작점은 보다 투명한 공개 규칙일 것이다. 예를 들면, Wu와 같은 전문가들은 광대역 사용제한 및 기타 중요한 서비스 이용 제한에 대한 공개를 권고했다.[157] 하지만 이러한 정보공개는 보다 포괄적인 규제를 위한 첫걸음에 불과하다. 2007년 3월, 산업, 과학, 기술 상임위원회(Standing Committee on Industry, Science, and Technology)는 통신사 규제완화에 대한 매우 짧은 보고서(한 단락 분량)를 상정하였다. 보고서에 따르면 위원회는 산업부장관에게 결정 CRTC 2006-15 수정 명령을 철회하고 통신서비스산업의 현대화를 위한 정책, 법령 및 규제 개혁을 포괄하는 종합안을 의회에 상정할 것을 권고하였다.[158]

이는 상임위원회가 산업부장관의 2006년 정보통신정책에 대한 성과분석 패널의 권고안의 선택적 시행에 반대하고 있고 종합적인 규제안을 요구하고 있음을 보여주고 있다. 통신산업에 대한 규제완화를 결정한 보수정부는 여전히 이러한 권고에 "반대"하고 있다.[159] 캐나다의 망 중립성 지지자들 중 상당수가 규제완화에 찬성했다는 점에 주목해야 할 것이다. 하지만 이들은 산업부장관의 캐나다 통신산업 현대화 및 망 중립성이 VoIP, IPTV, 기타 신생 애플리케이션 업계의

156) Ibid. p.28-29

157) Tim Wu, "Wireless Net Neutrality: Cellular Carterfone and Consumer Choice in Mobile Broadband", New America Foundation (2007년 2월 15일), online: New America Foundation (http://newamerica.net/)참조.

158) House of Commons, Standing Committee on Industry, Science and Technology, Sixth Report: Deregulation of telecommunications (March 2007) 참조.

159) "Tories overrule CRTC, further deregulate phone market", Canada.com (4 April 2007) online: Canada.com (http://o.canada.com/) 참조. 권고안에도 불구하고 통신산업 규제 완화를 가속화한 산업부 장관을 비난한 녹색당의 언도보도 ["Green Party alarmed by recklessness of Bernier's rush to deregulation", Green Party (2007년 4월 5일) online: Green Party of Canada (http://www.greenparty.ca/)] 참조.

공정한 경쟁에 해가 될 것이라는 주장에 대해서는 이의를 제기하고 있다.

반면 망 중립성을 지지하는 진영에서는 2007년 의견다양성(Diversity of Voices) 절차에 앞서 방송통신위원회에 의견서를 제출했다.[160] 캐나다 최대 미디어 엔터테인먼트 기업 중 하나인 Corus는 "캐나다의 연출가와 프로듀서들이 평등원칙에 따라 계속해서 네트워크 비트 스트림(networked bit stream)에 접근할 수 있도록 해야 한다"는 내용의 의견서를 제출했다. Corus는 망 중립성에 관한 업계 테스크포스 설립을 권고했다. 캐나다미디어협회(Canadian Media Guild) 역시 방송통신위원회에 제출한 의견서에서 망 중립성을 강력하게 지지했다. 미디어협회는 "인터넷 서비스 제공자들이 상업적인 이유로 고객이 특정 사이트에 접근하는 것을 통제하는 행위를 금지하도록 하는 규칙을 제정해 '망 중립성'을 보장"할 것을 방송통신위원회에 촉구했다.[161] 캐나다 전국 최대 규모의 노동조합인 전국 공무원 및 일반근로자 노동조합(National Union of Public and General Employees, 이하 NUPGE이라 함) 역시 망 중립성 보장을 위해 필요한 조치를 취할 것을 정부에 촉구했다.[162]

2007년 8월 내각이 개편되면서(문화부장관과 산업부장관 교체를 포함) 캐나다의 디지털 경제 경쟁력 강화를 위해 통신규제완화를 지역적 사안에서 보다 포괄적인 계획으로의 변경해야 한다는 요구가 재차 제기되었다.[163] 한편, 국민여론도 망 중립성 원칙을 지지하는 방향으로 선회한 듯했다. 레제 마케팅(Leger Marketing)에서 실시한 여론조사 결과 국민 대부분은 망 중립성 사안에 대해 잘 알지 못하지만 ISP가 "모든 컨텐츠, 사이트, 플랫폼을 동등하게 취급해야 한다"

160) CRTC, Broadcasting Public Notice CRTC 2008-4: Diversity of voices, (Ottawa: CRTC, 2008), online: CRTC (http://www.crtc.gc.ca/) 참조

161) Michael Geist, "Corus Calls For Net Neutrality Task Force" (20 July 2007), online: Michael Geist's Blog (http://www.michaelgeist.ca/); and Mark Goldberg, "Net neutrality and the new media proceeding" (2007년 8월 7일) online: Personal Website (http://www.mhgoldberg.com/) 참조

162) "NUPGE seeks action on Internet access and net neutrality", National Union (2007년 8월 3일) online: National Union of Public and General Employees (http://nupge.ca/) 참조

163) Michael Geist, "A blueprint for reforming the digital economy", The Toronto Star (2007년 8월 20일) online: The Toronto Star (http://www.thestar.com/) 참조

는 점에 대해서는 강하게 지지하고 있는 것으로 나타났다. ISP가 "웹사이트내 특정 컨텐츠 접근에 대해 추가 요금을 부과할 수 있도록 해야 한다"는 질문에 대해서는 응답자의 2/3가 반대했다. 또한 응답자의 76%는 연방정부가 "일반에게 공개된 인터넷 애플리케이션과 컨텐츠에 접근할 수 있는 인터넷 소비자의 권리 보장을 위해 관련법을 통과시켜야 한다고 생각한다"고 답했다.[164] 사실, 여론조사 결과는 캐나다 통신시장의 투명성 결여를 다시금 지적하고 있는데 ISP가 트래픽 셰이핑 실태에 대한 자료를 공개하고 있지 않기 때문에 대부분의 소비자가 망 중립성에 대해 알고 있지 못한 것을 이들의 탓으로 돌릴 수도 없다. 하지만 망 중립성 원칙에 대한 강력한 지지는 입법의 필요성을 명확히 보여주었다. 2008년 초, NUPGE는 망 중립성을 재차 요구하였고 이와 관련해 공공협의를 진행할 것을 정부에 촉구했다.[165]

정치적으로는 녹색당이 2007년 선거공약으로 망 중립성을 채택했다. 녹색당은 "인터넷의 최초설계 원칙인 망 중립성을 지키기 위해 최선을 다할 것이다. 망 중립성이라 함은 가장 널리 사용되는 공공정보 네트워크는 모든 컨텐츠, 사이트, 플랫폼을 동등하게 처리해야 한다는 것으로 따라서 네트워크는 모든 형태의 정보를 동등하게 취급하고 모든 종류의 애플리케이션을 지원할 수 있어야 한다"고 주장했다. 또한 녹색당 소속 하원의원은 캐나다 내 인터넷 통신사업자 지위를 인정하는 법안을 입법화할 예정이다. 동법안은 서비스 제공자들의 컨텐츠 차별을 금지하고 서비스 제공자들의 네트워크를 통해 전달 된 컨텐츠에 대해서는 ISP의 책임을 면제하고 있다.[166]

2008년 2월, 문화부 상임위원회는 캐나다 방송공사와 공영방송에 대한 보고서를 발표하였는데 망 중립성 사안을 여러면에 걸쳐 심도 있게 다루었다. 위원회 보

164) the results of the survey in "Canadians rebuff restrictions on their Internet access", CNW Group (2007년 10월 1일) online: CNW Group (http://www.newswire.ca) 참조.

165) "Consultations and legislation needed to protect net neutrality", National Union (2008년 2월 20일); and "NUPGE asks CRTC to investigate Internet 'traffic shaping'", National Union (2008년 3월 28일) online: National Union of Public and General Employees (http://nupge.ca/) 참조.

166) Green Party of Canada, Vision Green (2007년 10월 15일) at 154, online: Green Party of Canada (http://www.greenparty.ca/sites/greenparty.ca/files/VisionGreenOct15.pdf).

고서는 "네트워크 비(非)중립은 대규모 통합을 통해 시장변화에 대응하지 못하는 방송공사/라디오 캐나다에 막대한 영향을 미칠 수 있다. 컨텐츠 제공자가 상이한 서비스에 대해 요금을 지불하는 다중 네트워크(multi-tiered network)로 인터넷이 진화한다면 컨텐츠와 서비스질의 저하 및 온라인 전송에 대한 추가 요금 지불 요구 가능성으로 인해 기업의 경쟁력은 심각한 타격을 받게 될 것이며 이는 또한 법에서 명시하고 있는 목적을 실현하기 위한 능력을 저해하게 될 것이다"라고 평가했다.[167]

이러한 우려를 고려해 상임위원회[168] 위원의 과반수가 "디지털 시대에 국가 공영방송의 역할을 수행하는데 있어 캐나다 방송공사/라디오 캐나다에 대한 차별 없는 접근이 반드시 보장되어야 한다"는데 동의했다. 따라서 위원회는 방송통신위원회에 새로운 미디어 프로젝트 구상안의 일부로 망 중립성 문제를 다룰 것을 권고했다.

몇 달 뒤, 신민주당(New Democratic Party, NDP)는 2006년 정보통신정책에 대한 성과분석 보고 패널의 권고안을 따르고 망 중립성에 관한 법안을 입법할 것을 정부에 촉구했다.[169] 2008년 4월, 노동조합(NUPGE) 또한 스테판 디옹(Stephane Dion) 당시 야당대표에게 캐나다의 인터넷 중립성을 보호하기 위한 "정부의 조치마련 촉구"를 지지해 줄 것을 요청했다.[170] 2008년 5월, 의회에서 망 중립성지지 집회가 열리자 이에 대한 대응으로 찰리 앵거스(Charlie Angus) 새민주당 하원의원은 망 중립성 사안과 관련해 의원 입법 법안을 상정할 계획이라고 발표했다.[171] 발표 다음날 상정된 법안은 캐나다 통신법에 투명성, 중립적

167) House of Commons, Standing Committee on Canadian Heritage, CBC/Radio-Canada: Defining Distinctiveness in the Changing Media Landscape, ch 2 (2008년 2월).

168) 위원회의 보수진영은 방송공사가 아니라 방송통신위원회를 언급하고 있음을 근거로 보고서에 반대하는 내용의 소수의견을 발표하였다.

169) "NDP calls for net neutrality", CBC (2008년 4월 21일) online: CBC (http://www.cbc.ca/).

170) "NUPGE asks federal Liberals to join net neutrality campaign", National Union (2008년 4월 28일) online: National Union of Public and General Employees (http://nupge.ca/) 참조. 보도된 바에 따르면 한 진보진영의 하원의원은 정부의 규제완화 접근 방식은 "캐나다 인터넷 사용자의 권리를 충분히 고려하고 있지 않다"고 말한 것으로 전해지고 있다. [Michael Geist, "Liberal Response to Net Neutrality" (2008년 5월 8일), online: Michael Geist's Blog (http://www.michaelgeist.ca/)].

인 네트워크 관리, 정보공개 관리 등을 포함하고 있었다.

"네트워크 운영자들은 자신들이 소유한 광대역 네트워크를 이용한다는 이유로 또는 최종 목적지에 따라 특정 컨텐츠, 애플리케이션, 서비스에 특혜를 주거나 속도를 제한하거나 우선 취급하는 등의 네트워크 관리를 해서는 안 된다."[172]

동법안은 컴퓨터 보안 제공, 속도에 민감한 통신 우선취급, 차등 요금제 또는 데이터 상한제, 스팸 필터링, 서비스 약관 위반 처리 및 관련법 위반 방지를 포함해 위에서 언급한 일반 원칙에 몇 가지 예외 사항을 명시하고 있다. 동법안은 또한 관련정보 공개 방법 및 투명성 제고를 주요 골자로 한다. 법안은 "네트워크 운영자는 이용자가 운영자의 네트워크에 기기를 연결하지 못하게 하거나 이를 방해해서는 안 되며, 단 이러한 기기 연결이 실질적으로 네트워크에 손상을 가하거나 불합리하게 다른 가입자의 네트워크 사용 품질을 떨어뜨리는 경우는 제외 한다"고 명시하고 있다.[173] 이에 더해 법안은 "네트워크 운영자에게 특정 시간대 인터넷 속도, 유형, 이용자의 광대역 서비스 제한을 포함해 이용자의 인터넷 접근에 대한 정보를 이용자에게 제공하도록 하고 있다."[174] 2008년 연방선거가 다가옴에 따라 캐나다 도서협회(Canadian Library Association), SaveourNet.ca 등 다양한 시민사회단체와 비영리단체는 망 중립성을 선거공약으로 채택할 것을 촉구하는 연합에 합류하였다.[175]

---

171) "Internet protesters to descend on Ottawa", CBC (2008년 5월 26일) online: CBC (http://www.cbc.ca/); and "NDP to introduce 'net neutrality' private member's bill", CBC (2008년 5월 27일) online: Ibid 참조.

172) Bill C-552, An Act to amend the Telecommunications Act (Internet Neutrality), 2nd Sess, 39th Parl, 2008, cl 36.1(1).

173) Ibid cl 36.1(3).

174) Ibid cl 36.1(4). 2008년 6월, David McGuinty 신민주당 의원은 통신사 명확성 및 공정성 법안을 일반의원 발의 법안으로 상정했다. 법안에 따라 위원회는 제공자의 기기잠금을 금지하고 네트워크 속도에 관한 정확한 정보 제공, 이동전화, 광대역 망의 네트워크 관리의 투명성 제고 방법 등을 연구하도록 했다. 위원회는 재원, 소유 또는 목적지에 근거해 광대역 망에 대한 패킷 전송의 우선 취급, 특혜, 속도 감속 등에 관한 망 중립성 보고서를 작성해야 한다. [Bill C-555, An Act to provide clarity and fairness in the provision of telecommunication services in Canada, 2nd Sess, 39th Parl, 2008] 참조.

175) Canadian Liberty Association, "2008 Election Campaign Kit" at 7, online: CLA (http://www.cla.ca/news/CLA%20Election%20Kit%202008.pdf). For a brief overview of the

망 중립성에 관한 규제의 돌파구는 2008년 마련되었는데 당시 캐나다 인터넷 제공사업자연합(Canadian Association of Internet Providers- CAIP, 이하 인터넷 사업자연합이라 함)은 Bell Canada의 네트워크 임대 사업자에 대한 서비스 제한 중지 및 중단을 요구하는 Part VII application(캐나다 운송법(Transport Act), 제4장 위원회에 제출하는 입법청원서(Application of certain enactments to the Board)를 방송통신위원회에 제출했다.[176] 청구를 통해 Bell의 영업행위 즉, 네트워크 속도를 최대 90%까지 늦추는 데이터 이용 속도 제한 행위에 대해 더 많이 알 수 있었다. 인터넷사업자연합은 데이터 속도 제한으로 인해 독립인터넷서비스제공자(independent ISP)가 자신들의 네트워크를 관리할 수 없을 뿐만 아니라 이들이 사용하지 않는 광대역망에 대해서도 사용료를 지불하도록 만든다고 주장했다. 인터넷사업자연합은 Bell은 위법행위를 하고 있으며 이는 통신법 제36조(Telecommunication Act), 그 중에서도 개인의 사생활보호를 위한 제7조(a), (i)에 명시되어 있는 통신정책의 목적에 반할 뿐만 아니라 통신사 네트워크를 이용해 전달되는 컨텐츠에 대한 통신사 개입 금지에 반한다고 주장하면서 데이터 속도 제한 영업행위와 관련해 프라이버시 침해를 우려했다.[177]

Bell의 DPI 시스템에 관한 프라이버시 논쟁은 다음과 같다.

"독립 ISP의 최종 이용자가 발신지이거나 목적지인 인터넷 데이터 트래픽의 속도를 제한하기 위해 Bell은 먼저 각각의 데이터 패킷을 열어보고 다음으로 패킷 데이터와 헤더 정보를 검사한 후 문제가 되는 컨텐츠에 일정한 규칙을 적용한다. Bell의 데이터 속도 제한은 Bell의 이러한 영업행위가 도매 서비스 제공자가 사용자(뿐만 아니라 Bell의 최종 네트워크 사용자)의 통신 프라이버시를 침해

---

digital policies of various political parties in the 2008 election, see Michael Geist, "Which party is ahead on the digital scoreboard?", The Toronto Star (14 October 2008) online: The Toronto Star (http://www.thestar.com/).

176) Bell's throttling practices 참조.

177) Canadian Association of Internet Providers, "Re: Part VII Application by the Canadian Association of Internet Providers Requesting Certain Orders Directing Bell Canada to Cease and Desist from "Throttling" its Wholesale ADSL Access Services" (2008년 4월 3일) at para 116, online: Canadian Advanced Technology Alliance (http://www.cata.ca/files/PDF/caip/CAIP-PartVII__Traffic-Shaping_Final_v2.pdf).

할 수 있음을 보여주고 있다."[178]

결국, 인터넷사업자연합은 보다 명확하고 강한 어조로 광범위한 망 중립성 문제를 제기했다.

"Bell이 행하고 있는 기간 통신사업자의 ADSL 액세스 서비스의 차단 또는 속도 제한은 독립 ISP의 GAS 및 HAS에 대한 복잡한 알고리즘 사용과 관련이 있다. 이를 통해 Bell은 선택적으로 이러한 독립 ISP 최종 사용자의 데이터 처리량을 최대 90%까지 속도를 느리게 하고 있다. 이렇게 느린 속도에서는 오디오나 동영상 컨텐츠(예를 들면, CBC의 'Next Great Prime Minister's program) 등 인터넷에서 사용할 수 있는 일반적인 컨텐츠가 알아볼 수 없을 정도로 속도가 느려진다. 사실, Bell은 어떤 경우에는 해당 컨텐츠에 접근을 차단하거나 아니면 접속하고 싶지 않도록 만들어 서비스의 질을 저하시키고 있다. 따라서 Bell은 일부 컨텐츠를 다른 컨텐츠와 분리하고 낮은 우선순위를 부여한 다음 Bell이 전적으로 결정한 방법에 따라 최종 수신인에게 전송해도 되겠다고 결정할 때까지 격리하는 방법으로 개입하고 있다.

또한 Bell은 컨텐츠 발신자나 수신자가 생각한 시간 내에 또는 방법으로 이러한 컨텐츠가 전송되지 못하도록 막아 이들 컨텐츠의 "의미(meaning)"와 원하는 "목적(purpose)"에 영향을 미치고 있다."[179]

---

178) Ibid at paras 78-79;84.

179) Ibid at paras 92-94.Tom Barrett, "'Throttling' Net Traffic", The Tyee (2008년 4월 9일) online: The Tyee (http://thetyee.ca/) 참조. 후에, Primus Communications과 무선 Nomad가 위원회에 CAIP를 지지하는 제안서를 제출하였다. [Primus Telecommunications Inc., "Re: Application requesting certain orders directing Bell Canada to cease and desist from "throttling" its wholesale ADSL Access Services" (2008년 4월 15일), online 참조: CRTC (http://www.crtc.gc.ca/public/partvii/2008/8622/c51_200805153/891007.pdf)] ISP 서비스에 대한 벌금 징수와 관련해 ISP는 방송통신법 적용 대상에서 제외할 것을 주장하기 위해 "소극적"인 데이터 전송자의 역할을 근거로 내세웠다. Michael Geist, "Canadian ISP Alliance Forms For New Media Fight" (2008년 7월 15일), online: Michael Geist's Blog 참조. (http://www.michaelgeist.ca/). Rogersdml "파이프" 표현과 따라서 이전에 컨텐츠에 기초한 "트래픽 관리"를 인정했음에도 컨텐츠 다운로드에 대해 책임이 없다는 발언은 이중 잣대의 예가 되고 있다. (2007년 4월 13일), online: Mark Evans Tech (http://www.markevanstech.com); and Joanne Chianello, "Canadian content available

방송통신위원회에 Bell의 DPI와 관련해 조치를 취할 것을 요청한 Vaxination Informatique가 제출한 의견서도 인터넷사업자연합의 청구를 지지하고 있다.[180]

인터넷사업자연합의 의견서에 대해 Bell은 자사의 영업행위는 정당한 것이며 이러한 사안을 긴급하게 다루어야 할 필요가 없다고 주장하고 있다.[181] Bell은 심층패킷분석과 관련한 프라이버시 침해에 대해서는 침묵하고 있으며 회사는 해당 데이터를 보존하거나 사용하지 않는다는 공식적인 입장만을 발표하고 있다. Bell은 네트워크 사용에 관한 일부 데이터를 공개했는데 이러한 데이터는 오히려 P2P 파일공유가 네트워크 과부하의 원인이 된다는 자신의 주장에 대해 설득력을 잃게 하는 듯하다. Bell은 피크 타임에 상위 5%의 사용자들이 전체 부하의 33%를 일으킴으로써 인터넷 속도가 느려지는 "혼잡"이 발생한다고 주장했다. 소수 사용자의 과도한 트래픽 사용은 수치상으로만 보면 높은 것이 사실이지만 다른 국가들과 비교하면 오히려 낮다고 할 수 있는데 일부 국가의 경우 상위 5%의 사용자들이 전체 광대역망의 절반 이상을 사용한다.[182] 속도 제한에 대한 Bell의 의견서에 대해 인터넷사업자연합은 다음과 같이 주장했다.

"경쟁사 GAS의 트래픽 속도를 제한한 Bell의 행위는 사실상 회사가 주장하는 "네트워크 정체"와는 관련성이 거의 없어 보이며 이를 뒷받침할 근거가 부족하지만 반대로 이러한 행위가 재판매 시장(retail telecommunications market)에서 경쟁을 약화시키고자하는 의도에서 시작되었음을 보여주는 명확한 근거가 있다.

---

online may be regulated", Ottawa Citizen (2009년 2월 16일) online: Ottawa Citizen (http://www.ottawacitizen.com)].

180) Vaxination Infomatique's submission is available online: CRTC (http://www.crtc.gc.ca/public/partvii/2008/8622/c51_200805153/886374.PDF) 참조.
예를 들면, Bell의 대응은 Canada.com (2008년 4월 11일) online: Canada.com (http://o.canada.com/) 참조. 비슷한 시기, L'Union des Consommateurs과 퀘백의 소비자단체는 Bell Canada의 트래픽 속도 관리에 대해 집단소송을 제기하였다. 모든 지역 가입자를 대신해 인증을 요구한 소송에서 원고는 Bell의영업행위는 고의적으로 서비스 속도를 제한했고 프라이버시를 침해했다고 주장했다. ["Demande de recours collectif contre Bell", CNW Group (2008년 5월 29일) online: CNW Group (http://www.newswire.ca)] 참조.

181) Bell Canada's April 2008 submissions are available online: CRTC (http://www.crtc.gc.ca/public/partvii/2008/8622/c51_200805153/890988.zip).

182) Michael Geist, "Does Bell Really Have a P2P Bandwidth Problem?" (2008년 4월 17일), online: Michael Geist's Blog (http://www.michaelgeist.ca/) 참조.

Bell이 데이터 속도를 제한했던 시기와 만약 속도를 제한하지 않았으며 다른 결과가 날 수 있었던 일련의 사건이 발생했던 시기 간에 너무나 많은 '우연'이 있다."[183]

새로운 의견서는 DPI 기술의 영향과 VPN과 VOIP 서비스(P2P 네트워크 포함)의 속도제한에 대한 새로운 주장을 포함하고 있다. 또한 의견서에는 서스캐처원 주내 최대통신사인 SaskTel의 의견도 포함하고 있다. SaskTel은 Bell과는 달리 "어떠한 형태의 트래픽 셰이핑, 속도제한, 또는 사용제한도 사용자 또는 애플리케이션"에 시행하고 있지 않음을 보여주는 근거를 제시하였다.[184]

인터넷사업자연합은 데이터 속도 제한이 왜 통신법 제36조의 일반 통신사 조항을 위반하는지를 재차 설명했으며 그 내용은 다음과 같다.

"통신법 제36조는 통신사는 "컨텐츠를 제한하거나 통신사가 대중에게 제공하는 통신의 의미 또는 목적에 영향을 미쳐서는 안 된다"고 명확히 규정하고 있다. Bell의 속도 제한은 통신의 의미와 목적에 분명히 영향을 미치고 있다. 사실 인터넷사업자연합이 청원서에 기술한 바와 같이 Bell은 경쟁사의 최종 사용자가 이용할 수 있는 데이터 처리량 또는 데이터 전송 속도를 최대 90%까지 느리게 하고 있다. 이렇게 느린 속도에서는 오디오나 동영상 컨텐츠(예를 들면, CBC의 'Next Great Prime Minister's program) 등 인터넷에서 사용할 수 있는 일반적인 컨텐츠가 알아볼 수 없을 정도로 속도가 느려진다.

이렇게 속도를 매우 느리게 함으로써 Bell은 이러한 컨텐츠를 다른 컨텐츠와 분리하고 낮은 우선순위를 부여한 다음 Bell이 전적으로 결정한 방법에 따라 최종 수신인에게 전송해도 되겠다고 결정할 때까지 격리하는 방법으로 컨텐츠를 통제하고 있다. 이와 마찬가지로 Bell은 컨텐츠 발신자나 수신자가 생각한 시간 내에 또는 방법으로 이러한 컨텐츠가 전송되지 못하도록 막아 이들 컨텐츠의 '의미(meaning)'와 '목적(purpose)'에 영향을 미치고 있다."[185]

---

183) Canadian Association of Internet Providers, "Re: Part VII Application by the Canadian Association of Internet Providers Requesting Certain Orders Directing Bell Canada to Cease and Desist from "Throttling" its Wholesale ADSL Access Services" (24 April 2008) at para 9, online: CRTC (http://www.crtc.gc.ca/public/partvii/2008/8622/c51_200805153/895702.pdf) 참조.

184) Ibid at para 62.

2008년 5월 캐나다 개인정보보호국(Privacy Commissioner of Canada)은 DPI와 관련한 프라이버시 침해 논란에 대하여 직접적으로 언급하였는데 당시 캐나다 인터넷정책 공익클리닉(Canadian Internet Policy and Public Interest Clinic-CIPPIC, 이하 공익클리닉이라 함)은 Bell의 DPI에 대해 개인정보보호와 전자문서에 관한 법((Personal Information Protection and Electronic Documents Act, PIPEDA)에서 보호하고 있는 프라이버시를 침해하고 있다며 회사를 고발하였다.[186] 공익클리닉은 DPI를 통한 개인정보 수집과 관련해 이용자 동의를 얻지 않은 것을 포함해 프라이버시가 실질적으로 침해되고 있음을 확인했다. 공익클리닉은 또한 Bell이 "사용자의 통신 내용을 검사하지 않고도 네트워크를 관리"할 수 있음을 보여주는 증거가 있다면서 Bell의 정보수집 제한이라는 프라이버시 원칙을 위반했다고 주장했다.[187] 고소장에는 "트래픽 관리 목적으로 DPI를 이용하고 있음을 대중에게 명확하고 확실한 방법"으로 공개하지 않았음을 고려해 볼 때 Bell이 개방성 원칙을 위반하고 있다는 주장도 포함되어 있다.[188]

결정을 수차례 연기[189]한 후 2008년 11월 방송통신위원회는 인터넷사업자연합이 Bell을 상대로 소를 제기한 사건에 대해 판단했다. 위원회는 사업자연합의 주장을 기각하였고 "Bell은 속도제한과 관련해 모든 고객(소매 및 도매)을 동등하게 취급했다고 판시하면서 Bell의 손을 들어 주었다. 이러한 위원회의 판단은 본 사건의 핵심 즉, 차별적 네트워크 관리가 아니라 특정한 맥락에서 도매 셰이핑이라는 사건의 본질에 대해 문제점을 보여주고 있다. 위원회는 P2P가 트래픽 혼잡을 유발하기 때문에 Bell의 혼잡 해결을 위한 네트워크 관리 기술 이용 조치는 합당하다고 판단했다. 또한 위원회는 Bell의 행위가 경쟁을 약화시킬 것이라는 우려를 일축하면서 단순히 트래픽 속도를 느리게 한 것만으로는 통신법을

185) Ibid at paras 74-79.

186) Canadian Internet Policy and Public Interest Clinic, "Re: Bell Canada/Bell Sympatico Use of Deep Packet Inspection: PIPEDA Complaint" (2008년 5월 9일), online: CIPPIC (https://www.cippic.ca/sites/default/files/Bell-DPIPIPEDAcomplaint_09May08.pdf).

187) Ibid at para 38.

188) Ibid at para 45.

189) "CRTC delays ruling on Bell's throttling", CBC (2008년 10월 17일) online: CBC (http://www.cbc.ca/) 참조.

위반하는 컨텐츠 관리로 볼 수 없다는 결론을 내렸다.[190]

그러나 위원회의 이러한 결정이 망 중립성 지지진영의 완전한 패배를 의미하는 것은 아니었다. 2009년 7월, 위원회는 망 중립성 및 네트워크 관리 문제를 해결하겠다고 약속했다.[191] 위원회는 공청회 내용 중 일부를 바탕으로 특정 트래픽 관리 조치를 승인하는 기준을 마련할 것이라고 밝혔다.[192] 당시 컨텐츠 차단 금지 및 네트워크 관리의 투명성 제고[193] 등 몇몇 사안에 대해서는 합의가 이루어지고 있는 것처럼 보였다. 위원회 결정 이후 방송통신위원회가 트래픽 속도 제한에 대한 회사의 입장을 '확인'해주었다고 Bell은 주장[194]했지만 부위원장은 이번 결정이 속도제한을 '승인'하는 것이 아님을 명확히 했다.[195]

인터넷 트래픽 관리와 심리진행 결정에 따라 수많은 의견서가 제출되었고 이와 관련해 논평이 게재되었다. 개인정보보호국은 위원회의 결정에 주목하였고 "경제 및 사회정책적 측면에서 이제 정부가 망 중립성을 검토해야 할 시기가 되

190) CRTC, Telecom Decision CRTC 2008-108: The Canadian Association of Internet Providers' application regarding Bell Canada's traffic shaping of its wholesale Gateway Access Service, (Ottawa: CRTC, 2008), online: CRTC (http://www.crtc.gc.ca/) 참조. 예를 들면 방송통신위원회의 미디어 통합에 관한 결정은 "CRTC allows Bell to continue internet throttling", CBC (2008년 11월 20일) online: CBC (http://www.cbc.ca/) 참조; Chris Sorensen, "Bell can squeeze downloads, CRTC rules", The Toronto Star (20 November 2008) online: The Toronto Star (http://www.thestar.com/); and Nate Anderson, "Canadian regulators allow P2P throttling", Ars Technica (2008년 11월 20일) online: Ars Technica (http://arstechnica.com/).

191) CRTC, Telecom Public Notice CRTC 2008-19 – Notice of consultation and hearing: Review of the Internet traffic management practices of Internet service providers, (Ottawa: CRTC, 2008), online: CRTC (http://www.crtc.gc.ca/) 참조. 2009년 3월, 방송통신위원회는 망 중립성에 관한 온라인 협의를 실시했다. 사용자 경험, 혁신, 방송통신위원회의 역할, 망관리, ISP 투명성을 주제로 협의가 진행되었다.

192) Ibid at para 9(5) 참조.

193) The CRTC required Bell to provide its wholesale customers with advanced notice of its traffic management plans. See CRTC, Telecom Decision CRTC 2008-108, (Ottawa: CRTC, 2008) at para 74, online: CRTC (http://www.crtc.gc.ca/) 참조.

194) "Bell welcomes CRTC decision allowing wholesale Internet network management", Bell Canada (2008년 11월 20일) online: Bell Canada (http://www.bce.ca/) 참조.

195) Peter Nowak, "We're not endorsing internet throttling: CRTC", CBC (2008년 11월 20일) online: CBC (http://www.cbc.ca/) 참조.

었다. 우리는 망 중립성 논의에 참여하기를 희망한다"고 발표했다.[196] 개인정보보호국은 DPI 기술을 이용한 네트워크 관리 및 프라이버시 침해에 대한 위원회의 네트워크 관리 심리 의견서를 제출함으로써 이러한 논의에 참여할 수 있었다.[197] 의견서는 스팸, 저작권침해 자료 등 일부 컨텐츠, 혐오 컨텐츠 및 망성능 조사를 위한 트래픽 하중 모니터링 등 대한 인터넷 트래픽 검사를 포함해 DPI 사용에 관한 우려에 대해 언급하고 있다. 개인정보보호국은 프라이버시를 네트워크 분석에 고려해야 할 필요성에 대해서도 의견을 개진하였다.

"우리는 통신법과 통신정책에서 명시하고 있는 프라이버시 보호를 촉진하기 위해서는 포괄적으로는 인터넷 트래픽 관리 그리고 상세하게는 DPI와 관련한 결정 및 규제는 DPI 기술의 본질적인 프라이버시 침해 가능성 및 ISP의 DPI 기술 이용 방법을 고려할 것을 제안한다."[198]

"인터넷 트래픽 관리를 위한 DPI 기술이 불투명하게 활용되고 있으며 개인/소비자의 기대와 잠재적으로 일치하지 않는다는 우려가 제기되고 있으며 '불합리한 네트워크 관리'에 사용되고 있음을 보여주는 법적 근거가 있다."[199]

망 중립성에 대한 협의 및 공청회 공지 후 전기통신 위원회에 몇 가지 중요한 의견서가 제출되었다.[200] 캐나다 청각장애인협회는 "청각장애인 또는 장애가 있는 사람들에 대한 의도치 않은 결과가 지역에 부정적인 영향을 미치지 않도록 트래픽 관리 제안에 있어 장애인의 의견 고려"를 주장하였다.[201]

기상통신망을 소유하고 있는 Pelmorex Media는 망 중립성을 강력하게 지지하는 내용의 의견서를 제출했다. 하지만 좀 더 정확히 말해 본 의견서는 무선 망

196) Daphne Guerrero, "CRTC begins dialogue on traffic shaping" (2008년 11월 21일), online: Office of the Privacy Commissioner of Canada (http://blog.priv.gc.ca/) 참조.

197) Privacy Commissioner of Canada, "Re: Telecom Public Notice CRTC 2008-19" (2009년 2월 18일), online: CRTC (http://www.crtc.gc.ca/public/partvii/2008/8646/c12_200815400/1027577.PDF) 참조.

198) Ibid at para 21 참조.

199) Ibid at para 31 참조.

200) Supra note 78.

201) Canadian Association of the Deaf, "Re: Public Notice 2008-19" (2009년 1월 16일) at para 8, online: CRTC (http://www.crtc.gc.ca/public/partvii/2008/8646/c12_200815400/1008694.DOC)

중립성의 중요성을 강조하고 있다.

"위원회는 모든 무선과 유선 네트워크 운영자를 포괄할 수 있도록 망 중립성과 트래픽 관리에 대해 보다 광의의 정의를 규정해야 한다고 생각한다. 우리는 위원회가 유무선 네트워크 운영자들이 평등하게 트래픽을 관리하고 트래픽을 똑같이 또는 비교 가능한 방법으로 관리하도록 하기 위해 필요한 조치를 취해야 할 필요가 있다고 본다. ISP나 네트워크 운영자가 생산 또는 제공하는 컨텐츠를 우선처리하는 방식의 네트워크 관리를 허용해서는 안 될 것이다."[202]

Pelmorex의 의견서는 무선 네트워크 관리[203]뿐만 아니라 캐나다 통신사의 무선 망 중립성 침해로 추정되는 사례 목록도 함께 포함시켰다는 점에서 주목할 만 하다. 통신사의 회사명을 직접 언급하지는 않았지만 침해로 추정되는 사례로는 이동통신 사이트의 광고 차단, 웹 페이지에 내장되어 있는 트랙 코드 제거(따라서 광고 트래픽 전송을 제한), 접근을 차별하는 "자사의 폐쇄망(walled garden)" 구축, 휴대폰에서는 통신사의 홈페이지를 통해서만 인터넷 접근 허용, 스마트폰에서 애플리케이션을 사용하기 전에 사전 승인 요구, 광고를 포함한 문자 메시지 전송에 대해 추가 이용요금 부과 등이 있다.[204]

캐나다 영화텔레비전제작협회(Canadian Film and Television Production Association-CFTPA, 이하 제작협회라 함)는 증가하고 있는 P2P 애플리케이션 사용을 적법한 사업 모델로 설명하면서 트래픽 속도 제한이 이러한 사업 모델에 가할 수 있는 잠재적인 위협을 언급했다.

"P2P 애플리케이션은 반박의 여지없이 승인받지 않은 컨텐츠를 배포하는데 사용되고 있지만(이메일, 뉴스그룹, 웹) 동시에 독립 제작자가 오디오-동영상 프로그램을 전송하는 수단이 되며 광대역을 적극 활용할 수 있는 새로운 사업 모델의 근간이 되고 있다. 따라서 제작협회는 차별적인 트래픽 속도 제한이 컨텐

202) Pelmorex Media Inc., "Re: Telecom Public Notice CRTC 2008-19," (2009년 2월 23일) at para 36, online: CRTC (http://www.crtc.gc.ca/public/partvii/2008/8646/c12_200815400/1029399.pdf) 참조.

203) Score Media also noted that its mobile site traffic nearly equaled its fixed Internet site [Score Media Inc., "Re: Telecom Public Notice CRTC 2008-19," (2009년 2월 23일) at para 3, online: CRTC (http://www.crtc.gc.ca/public/partvii/2008/8646/c12_200815400/1029790.pdf)].

204) Supra note 89 Appendix.

츠 배포가 승인받은 제3자 또는 제작자에 의해 이루어지든 또는 "저작권을 침해"하는 컨텐츠 역시 인터넷을 통해 배포될 수 있다는 점을 고려해 보았을 때 독립 제작자 및 기타 컨텐츠 제공자의 컨텐츠 개발 능력을 촉진할 수 있는 새로운 애플리케이션 개발을 저해할 수 있다는 점을 우려한다."[205]

제작협회는 방송통신위원회는 "서비스 조건으로(condition of service) ISP의 애플리케이션과 프로토콜을 차별하는 트래픽 관리 금지"를 제안하였다[206]. 한편, 캐나다 다큐멘터리 영화단체(Documentary Organization of Canada)는 다음과 같이 주장했다.

"트래픽 관리라는 명분하에 이루어지는 ISP의 데이터 속도제한에 대해 우리는 심각한 우려를 표명하고 동시에 망 중립성 원칙을 지지한다. P2P 애플리케이션을 대상으로 트래픽 세이핑 기술을 이용해 ISP는 실질적으로 게이트키퍼의 역할을 하고 있다."[207]

CBC도 망 중립성을 지지하면서 다음과 같이 발표했다.

"CBC/Radio Canada는 통신 컨텐츠를 왜곡하거나 필요한 때에 접근하지 못하도록 하기 위해 인터넷에서 이루어지는 통신을 변경하거나 특정 웹사이트에 대한 접근을 차단한다면 트래픽 관리는 분명 통신법 제36조의 위반이다."[208]

캐나다예술회의(Canadian Conference of the Arts, CCA)는 다음과 같이 발표했다.

"인터넷 사용자가 컨텐츠에 접근하기 위해 이용하는 네트워크를 제공하는 기업

---

205) Canadian Film and Television Production Association, "Re: Telecom Public Notice CRTC 2008-19" (2009년 2월 23일) at para 58, online: CRTC (http://www.crtc.gc.ca/public/partvii/2008/8646/c12_200815400/1030120.PDF) 참조.

206) Ibid at para 81 [emphasis in original]. In a later submission by the CFTPA that argued Bell's throttling practices unduly disadvantaged peer-to-peer content, peer-to-peer applications, and end-users accessing legal peerto-peer content [available online: DSL Reports (http://www.dslreports.com/r0/download/1441998~60cdd142c47391b7bfd55f76129c2a3d/Part%20VII%20Applicat ion%20-%20CFTPA.pdf)] 참조.

207) Documentary Organization of Canada, "Re: Telecom Notice of Public Consultation and Hearing CRTC 2008-19" (2009년 11월 23일) at 2, online: CRTC (http://www.crtc.gc.ca/public/partvii/2008/8646/c12_200815400/1030141.PDF) 참조.

208) CBC, "Re: Review of the Internet traffic management practices of Internet service providers, Telecom Public Notice CRTC 2008-19" (2009년 11월 23일) at para 23, online: CRTC(http://www.crtc.gc.ca/public/partvii/2008/8646/c12_200815400/1030285.PDF) 참조.

이 영업이익을 위해 사용자의 컨텐츠 접근을 제한하기로 결정하거나 실제로 제한을 하고 있거나 트래픽 혼잡을 해결하기 위해서 '순수하게' 트래픽을 관리하거나 또는 다른 이유로 트래픽을 관리한다면 그 누구도 캐나다의 인터넷 사용자가 무제한으로 컨텐츠에 접근할 수 있다고 주장할 수 없을 것이다."[209]

캐나다 영화, 텔레비전, 라디오 예술가 연합(Alliance of Canadian Cinema, Television and Radio Artists, ACTRA)[210]와 캐나다미디어협회 역시 이와 비슷한 입장을 취하였다.[211] 여러 협회 및 단체에서 제출한 제안서는 예정된 망 중립성에 관한 공청회가 사업, 혁신, 소비자 등 광범위한 영향을 미칠 수 있으며 망 중립성과 캐나다 문화부문이 밀접하게 연관되어 있음을 알 수 있다.

방송통신위원회의 망 중립성에 관한 협의 공지 후 구글, eBay, Amazon, PayPal 등 인터넷 기업으로 구성된 영향력 있는 오픈 온라인 연합(Open Internet Coalition)도 제안서를 제출했다. 연합은 방송통신위원회에게 "구별적인 (nuanced) 규제 접근방식"을 취할 것을 촉구했는데 그 내용은 다음과 같다.

"컨텐츠와 애플리케이션-중립 트래픽 관리(일부 허용)와 광대역 네트워크 투자를 저해하고 소비자의 선택을 축소하며 사용자의 표현의 자유에 개입하고 혁신을 억제하는 불법적인 애플리케이션 특정 트래픽 관리를 구별해야 한다."[212]

Network B.C를 통해 브리티시콜럼비아 주정부도 제안서를 제출했다.

"망 중립성은 인터넷의 근간이다. 또한 망 중립성은 확장가능하고 견실한 네트워크 인프라에 대한 투자에 상당히 의존하고 있다. 하지만 "적극적인 트래픽 셰이핑"은 네트워크 인프라 투자 촉진에 거의 아무런 영향을 미치지 못할 뿐만

209) Canadian Conference of the Arts, "Re: Review of the Internet traffic management practices of Internet service providers, Telecom Public Notices CRTC 2008-19, -19-1, -19-2" (2009년 2월 23일) at para 8, online: CRTC (http://www.crtc.gc.ca/public/partvii/2008/8646/c12_200815400/1030237.DOC) 참조.

210) Alliance of Canadian Cinema, Television and Radio Artists, "Re: Telecom Public Notice CRTC 2008-19" (2009년 2월 23일), online: CRTC (http://www.crtc.gc.ca/public/partvii/2008/8646/c12_200815400/1031363.PDF) 참조.

211) Canadian Media Guild, "RE : Telecom Public Notice CRTC 2008-19" (2009년 2월 23일), online: CRTC (http://www.crtc.gc.ca/public/partvii/2008/8646/c12_200815400/1031064.PDF) 참조.

212) 오픈인터넷연합, "RE : Telecom Public Notice CRTC 2008-19" (2009년 2월 23일) p.2-3, online: CRTC (http://www.crtc.gc.ca/public/partvii/2008/8646/c12_200815400/1029708.pdf)

아니라 미래의 용량 요구에 부합하기 위해 기존 및 레거시 네트워크를 압박해도 된다는 보안에 대한 잘못된 인식으로 이어질 수 있다. 또한 적극적인 트래픽 셰이핑의 사용은 잠재적으로 네트워크 업그레이드를 지연시켜 미래에는 더욱 광범위한 네트워크 투자가 이루어져야 할지도 모른다."[213]

"특히 ISP가 유일한 게이트웨이 서비스 제공자의 역할을 하는 상황에서는 트래픽 관리를 위한 적극적인 트래픽 셰이핑 사용은 통신법 제7조(a), (b), (g), (f), (h)에서 규정하고 있는 정책 목적에 반한다."[214]

2009년 5월, 인터넷 트래픽 관리 공청회를 두 달 앞두고 캐나다 인터넷제공자 사업자연합(Canadian Association of Internet Providers, CAIP)은 2008년 11월 있었던 방송통신위원회의 Bell의 트래픽 속도 제한에 대한 결정을 철회할 것을 촉

---

213) Network BC, "RE : Telecom Public Notice CRTC 2009-19" (2009년 2월 17일) at para 4, online: CRTC (http://www.crtc.gc.ca/public/partvii/2008/8646/c12_200815400/1030213.zip).

214) 캐나다 통신법

제7조 캐나다 통신정책(Canadian Telecommunications Policy)

7. It is hereby affirmed that telecommunications performs an essential role in the maintenance of Canada's identity and sovereignty and that the Canadian telecommunications policy has as its objectives

(a) to facilitate the orderly development throughout Canada of a telecommunications system that serves to safeguard, enrich and strengthen the social and economic fabric of Canada and its regions;

(b) to render reliable and affordable telecommunications services of high quality accessible to Canadians in both urban and rural areas in all regions of Canada;

(c) to enhance the efficiency and competitiveness, at the national and international levels, of Canadian telecommunications;

(d) to promote the ownership and control of Canadian carriers by Canadians;

(e) to promote the use of Canadian transmission facilities for telecommunications within Canada and between Canada and points outside Canada;

(f) to foster increased reliance on market forces for the provision of telecommunications services and to ensure that regulation, where required, is efficient and effective;

(g) to stimulate research and development in Canada in the field of telecommunications and to encourage innovation in the provision of telecommunications services;

(h) to respond to the economic and social requirements of users of telecommunications services; and

(i) to contribute to the protection of the privacy of persons.

구하는 탄원서를 방송통신위원회에 제출하였다.[215] 탄원서에서 사업자연합은 결정에 포함되어 있는 사실 및 법률 오류를 주장하고 특히, 소송의 쟁점이 된 사안에 대한 위원회의 이해 부족을 지적했다. 또한, 사업자연합은 망 중립성과 관련해 7월에 있을 공청회를 열기도 전에 방송통신위원회가 이미 결정을 한 것이 아니냐며 많은 사람들이 제기하고 있는 우려를 부각시켰다.

"사실, 위원회는 PN 2008-19[216] 소송에서 제기된 일부 사실과 법률문제를 속단했고 그렇게 함으로써 PN 2008-19 사건에 대한 절차가 진행되기도 전에 이미 위원회의 결정 범위를 축소했다. 2008-108 결정(Decision 2008-108)[217]이 유효한 한 통신법 제27조 제2항과 제36조에 의거한 CAP 기반 트래픽 속도제한의 적법성에 대한 PN 2008-19의 결과를 위원회가 속단했다는 인식은 사라지지 않고 계속될 것이다."[218]

탄원서는 특히 위원회가 통신법 제27조 제2항과 제36조를 해석하는 방법에 대한 법률 오류뿐만 아니라 P2P와 DPI 기술사용에 관한 오류의 예를 설명하고 있다. 사업자연합이 탄원서를 제출함에 따라 세간의 관심이 앞으로 있을 망 중립성에 대한 공청회에 쏠린 가운데 공청회가 있기 몇 주 전에 위원회를 방어적인 입장에 놓이기 했다는 점을 고려해 보면 가히 놀라운 일이었다.

한편, 찰리 앵거스(CHarlie Angus) 신민주당 하원의원은 또 다른 망 중립성 법안을 의회에 상정했는데[219] 이는 과거법안[220]과 비교해 보다 엄격한 내용을 포함하고 있다. 자유당 역시 위원회가 망 중립성 공청회를 준비함에 따라 이 사

---

215) Canadian Association of Internet Providers, "Application to Review and Vary Telecom Decision CRTC 2008-108" (2009년 5월 21일), online: Canadian Advanced Technology Alliance (http://www.cata.ca/files/CAIP/R_V_on_Throttling_%2820May09FINAL%29-1.pdf).

216) 역주: 인터넷 서비스 제공자의 인터넷 트래픽 관리에 관한 결정으로 자세한 내용은 http://www.crtc.gc.ca/partvii/eng/2008/8646/c12_200815400.htm 참조.

217) 역주: 벨 캐나다의 기간통신의 게이트 액세스 서비스에 대한 트래픽 셰이핑에 대한 캐나다 인터넷 제공자사업자연합의 신청에 관한 것으로 자세한 내용은 방송통신위원회 홈페이지 http://www.crtc.gc.ca/eng/archive/2008/dt2008-108.htm 참조.

218) Ibid at para 12.

219) 법안 C-398, An Act to amend the Telecommunications Act (Internet neutrality), 2nd Sess, 40th Parl, 2009.

220) Supra note 52.

안과 관련해 당의 입장을 취하였다. 2009년 6월 마크 가르노(Marc Garneau) 자유당 하원의원은 질의응답 시간에 다음과 같은 질문을 하였다.

"존경하는 의장님, 21세기 자유 민주시대, 혁신과 지식경제 시대에 어떤 도구도 인터넷보다 중요한 것은 없습니다. 인터넷은 오늘날 자유로운 생각과 아이디어를 전달하고 공유할 수 있는 근간입니다. 자유당은 망 중립성 원칙과 개방, 경쟁적인 인터넷 환경을 지지합니다. 과연 보수당이 망 중립성 원칙을 지지할지 의문입니다."[221]

다음으로 토니 클레먼트(Tony Clement) 산업부 장관이 앞으로 있을 디지털 경제 전략 회의에 대해 설명했지만 망 중립성에 대해서는 어떠한 입장도 취하지 않았다. 뒤이은 자유당의 언론보도를 통해 자유당이 트래픽 관리를 반경쟁행위로 보고 있으며 프라이버시 침해에 대해 우려하고 있음을 알 수 있다.[222] 이러한 언론보도는 방송통신위원회가 주최하는 망 중립성에 대한 공청회를 몇 주 앞둔 상황에서 중요한 새로운 국면에 접어들었음을 보여주고 있다. 신민주당과 자유당이 개방형 인터넷 보호를 지지하자 국가 차원의 디지털 전략의 개발에 대한 중요성이 증가하고 있는 상황에서 보수당에 대한 입장표명의 압력이 거세졌다.

2009년 7월, 방송통신위원회의 망 중립성 공청회가 열렸고 그 결과 캐나다의 망 중립성에 있어 가장 중요하다고 할 수 있는 법적근거가 마련되었다. 공청회와 그에 따른 인터넷 트래픽 관리 실무(Internet Traffic Management Practices, ITMPs) 지침은 다음에서 후술한다.

---

221) *House of Commons Debates,* 40th Parl, 2nd Sess, Vol 144 No 078 (2009년 6월 8일) at 1445.

222) "Liberals speak out in support of net neutrality", Liberal Party Newsroom (2009년 6월 19일) online: Liberal Party of Canada (http://www.liberal.ca/).

4. 2009: 캐나다 라디오 텔레비전 방송통신위원회의 인터넷 트래픽 관리 실무 지침

방송통신위원회의 트래픽 관리에 관한 공청회에서 국내 텔레콤과 케이블 회사 그리고 소비자, 크리에이터, 기술 그룹이 격돌하였다. 텔레콤과 케이블회사의 주장의 요지는 가입자의 인터넷 활동과 일부 애플리케이션의 과도한 트래픽 발생 제한(예를 들면 트래픽 속도 제한)을 목적으로 한 DPI 기술사용을 포함한 네트워크 관리는 모든 가입자에게 최적의 접근을 제공하기 위해서는 반드시 필요하다는 것이다.[223] 다른 한편으로 소비자연합, 독립 ISP, 방송사, 크리에이터 그룹, 기술회사는 프라이버시, 경쟁 및 소비자 권리에 대한 문제를 제기했다. 미디어 공청회 동안 캐나다의 대표 통신사 Rogers는 "월드 가든(walled garden)은 없으며 우선 취급하는 컨텐츠도 없다. 네트워크는 단순히 파이프에 지나지 않다. 우리는 현재 더 크고 더 넓은 파이프로 이동하고 있다"[224]고 주장하였다. 트래픽 관리 공청회의 핵심은 이러한 주장의 타당성을 입증할 수 있느냐 하는 것이다.

가. 기술적인 문제

공청회 시작부터 방송통신위원회 위원들은 통신사의 주장 즉, 트래픽 혼잡이

---

223) 흥미로운 점은, 네트워크 관리가 반드시 필요하다고 현재 주장하는 동일한 통신사와 케이블 회사가 두 달 전 캐나다의 컨텐츠 지원이라는 제목 하에 열렸던 방송통신위원회의 새로운 미디어 공청회에서 네트워크 관리의 가능성에 대해 정면으로 부딪치자 서로 다른 입장을 취했다. 예를 들면, Shaw는 현재 빠르고, 믿을 수 있으며 적정한 가격의 접근을 보장하기 위해서는 트래픽 관리가 필요하다고 주장하고 있다. 하지만 Shaw의 대표에게 새로운 미디어 공청에서 트래픽 확인의 가능성에 대해 질문을 하자 그는 위원회에, "우리가 확인할 수 있는 것은 네트워크를 오가는 데이터의 용량이다. 하지만 우리는 어떤 종류의 데이터가 오고가는지는 알 수 없다. 이메일이 될 수도 있고 포르노가 될 수도 있다. 우리는 가정으로 가는 데이터의 종류를 확인할 수 있는 시간이 없다. 따라서 그 내용은 알 수 없다."[CRTC, Canadian broadcasting in new media hearings, vol 9 (Gatineau: CRTC, 2009) at para 10263, online: CRTC <http://www.crtc.gc.ca/ >] 참조. 또한 뉴미디어 공청회에서 MTS Allstream의 전문가 증인은 "때때로 심층패킷분석을 한다. 예를 들면, 정보기관의 요청에 따라 비밀리에 이루어지는데 소비자에게는 이러한 사실을 직접 얘기하지는 않는다"고 진술했다. [상게서 vol 10 at para 11249 참조]

224) 상게서, vol 9 at paras 9822-23.

문제이며 DPI 기술사용 금지가 소비자의 인터넷 접근 비용의 증가로 이어질 수 있다는 주장을 받아들인 것으로 보였다. 사실, 공청회는 혼잡 시간대에 "우선화(prioritizing)"기술을 사용할 필요성이 있지만 언제 이러한 기술을 사용할지는 예측할 수 없으며[225] "네트워크를 관리하지 않는 것이 중립 네트워크는 아니다"[226]라고 주장하는 Sandvine사 등 DPI 서비스 제공자의 발표로 시작되었다. Sandvine은 네트워크에서 악의적인 트래픽 제거, 속도에 민감한 데이터 전송을 위한 서비스 품질 보장, 가입자에게 추가비용이 발생할 수 있음의 고지하고 주문형 서비스의 일환으로 파일 다운로드를 위한 광대역 확대[227]하는 등 적법한 목적을 위해 우선화 기술을 사용할 수 있다고 주장했다. 또한 DPI 서비스 제공자는 "[접근 타입, 네트워크의 이동성, 인터넷 애플리케이션, 트래픽 혼잡관리 솔루션간 또는 솔루션내 네트워크 구조의 다양성을 고려하면 허용 가능한 트래픽 관리에 대한 새로운 규칙은, 특히 이러한 관점에서 시대적 변화에 부합하지 못하게 될 것이며 지속적인 인터넷의 건전성을 저해하게 될 것"[228]이라고 주장했다. 샌드바인(Sandvine)은 광대역 네트워크를 과도하게 사용하는 일부 사용자를 대상으로 하는 정책에 대해서는 신중한 입장을 취하면서도 시간대별, 비(非) 광대역 인센티브 애플리케이션을 우선화하는 정책에 대해서는 지지하는 입장을 밝혔다.[229] 또한 "우선화 기술이 반드시 프라이버시를 침해하는 것이 아니며 이는 기술을 어떻게 사용하느냐에 달려 있다"고 주장했다.[230]

---

225) 트래픽 혼잡을 예측할 수 있느냐는 사안은 ISP가 논란을 덜 불러일으키는 피크 시간대 트래픽 관리를 주장하지 않으면서 피크 시간대에 트래픽 문제를 해결 할 수 있도록 네트워크를 설계할 수 있는지와 관련이 있다. The conversation in CRTC, Transcript of Proceeding: Review of the Internet traffic management practices of Internet service providers, vol 1 (Gatineau: CRTC, 2009) at paras 247-56, online: CRTC (http://www.crtc.gc.ca/) 참조.

226) 상게서, p.50 참조. Sandvine은 후에 인터넷이 처음으로 생겨났을 때 모든 사용자들은 동등한 지위에 있었다는 주장으로 자시들의 주장을 명확히 했다. 하지만 시간이 지나면서 사용자들은 자신의 이익만을 생각하게 되었고 일부 사용자는 다른 사용자보다 더 많은 광대역망을 사용한다. 따라서 인터넷을 관리하지 않으면 일부 사용자가는 다른 사람들의 이익을 침해하면서 자신들의 이익만을 추구하게 될 것이다. [Ibid at paras 321-23]

227) Ibid at para 51.

228) Ibid at para 54., Sandvine은 각각의 트래픽 관리는 특정 시간대에 개별적으로 판단되어야 한다고 주장하면서 규제가 필요 없음을 시사했다.

229) Ibid at paras 62-65.

나. 망 중립성 지지단체

소비자단체는 DPI 및 기타 인터넷 트래픽 관리가 합법한지를 입증할 입증 책임이 누구에게 있는지에 집중했다. 소비자단체는 지금까지 수집한 자료에 따르면 DPI와 기타 인터넷 트래픽 관리 기술의 사용은 통신법 제36조를 위반하고 있는 것으로 보이며, ① 네트워크 트래픽과 관련해 심각한 문제 및 이를 해결해야할 긴급성, ② 이러한 기술이 사용자의 권리 침해 최소화, ③ 문제에 비추어 해결방안이 적합한지를 입증할 입증책임이 통신사에 있다고 주장했다. 따라서 위의 세 단계 테스트에 근거해 제36조의 "합법적" 위반 청구가 받아들여진다면 소비자는 반드시 자신들의 컨텐츠 권리에 미치는 영향을 고지 받아야 할 것이다. 이러한 정보는 ISP의 홈페이지에 게재되어야 할 것이며 Bell은 회사의 트래픽 속도 제한 방침에 대한 시행방법에 대해서는 공개를 거부했다. 또한 시민단체는 이러한 방침은 모든 경쟁사, 사용자, 애플리케이션 및 트래픽을 동등하게 취급하고 소비자보호를 강화하며 속도에 민감한 데이터 서비스를 용이하게 하고 사용자의 프라이버시와 보안을 보호할 수 있어야 한다고 주장했다.

소비자단체는 DPI 기술은 원하지 않거나 악의적인 컨텐츠로부터 소비자를 보호할 목적으로만 제한적으로 사용되어야 한다고 주장했다. 이들은 만약 DPI 기술이 제공자의 상업적 이익을 위해서 사용된다면 이는 전적으로 받아들일 수 없다는 점을 강조했다. 또한 ISP는 DPI 기술을 이용해 방문한 웹사이트 및 방문 시간을 보여주는 패킷을 조사하고 있다고 덧붙였다. 소비자의 프라이버시 침해와 관련해 ISP는 소비자의 동의를 얻지도 않았을 뿐만 아니라 이러한 정보를 수집하고 있다는 사실을 공개하지도 않았다.[231] 또한 네트워크 관리 목적으로만 DPI기술을 사용할 때조차도 프라이버시가 침해될 수 있다는 소비자 단체의 주장은 주목할 만하다. 그러나 방송통신위원회의 위원장은 DPI 기술 이용 자체만으로도 프라이버시를 침해한다는 주장을 받아들일 준비가 되어 있지 않다고 답했다.[232]

---

230) Ibid at paras 75-77.

231) Ibid at paras 730-811. 소비자단체는 통신법 제36조, 예를 들면 변경 또는 검사 없이 컨텐츠를 전달할 권리는 가장 높은 수준의 보호를 위한 "기본권"이라고 생각한다. [Ibid at para 87]

자신들의 주된 목표는 차별 없는 인터넷의 빠른 접근, 개방성이라고 설명하는 오픈 인터넷 연합(Open Internet Coalition, OCI)는 다음의 네 가지를 주장했다. 첫 번째 주장은 혁신으로 인터넷연합은 인터넷의 개방성은 혁신의 원동력이며 개방형 인터넷에 대한 활발한 접근은 공공정책에 있어 중요하다는 것이다. 두 번째는 첫 번째 주장과 밀접한 관련이 있는데 인터넷연합은 애플리케이션 특정 트래픽 관리는 사용자들이 인터넷에 대한 매력을 잃게 만든다고 했다. 세 번째로 이들은 특정한 트래픽 관리는 받아들일 수 있다고 주장했다. 시간이 지나면서 인터넷을 통한 멀티미디어 포맷의 온라인 사용이 확대되면서 트래픽 혼잡이 심각한 문제가 되고 있다는 것이다. 인터넷연합은 과거에는 용량을 늘려 이러한 문제를 해결할 수 있었다는 점을 강조했다. 마지막으로 일정한 트래픽 관리가 허용되려면 통신법 제27조 제2항과 제36조의 해석에 따른 간단한 '시험'을 통과해야 한다고 덧붙였다. 또한 연합은 유용한 트래픽 관리와 차별의 의미를 구분해야 하며 통신사가 네트워크 관리를 통해 혼잡을 줄이면서도 인터넷의 개방성을 지켜나갈 수 있음을 보여주는 증거가 있다고 주장했다.

한편, 인터넷연합은 애플리케이션간 차별은 통신법 제27조의 차별의 구성요건에 해당된다고 주장하면서 동법 제27조와 제36조를 근거로 한 세 가지 "시험"에 대해서 설명했다. 다시 말해, 문제가 되고 있는 트래픽 관리가 ① 속도에 민감하고 실질적인 목적에 부합하는지, ② 좁은 의미에서 목적에 부합하는지 ③ 이러한 목적을 실현하기 위한 최선의 방법인지를 확인하는 것이다. 시험의 제 1단계와 관련해서 인터넷연합은 네트워크의 기능 약화는 긴급하고 실질적인 목적이 될 수 있지만 현재까지 입수한 증거는 네트워크의 기능을 약화시킬 정도의 트래픽 혼잡이 발생하고 있다는 주장이 근거가 없음을 보여주고 있다고 주장하고 있다. 또한 BitTorrent와 같은 P2P 애플리케이션이 인터넷을 "악용"하고 있다는 주장에 대해서도 의구심을 표명했다. 시험의 제2단계에 대해서는 트래픽 속도 제한이 결코 좁은 의미에서 이러한 목적에 부합하지 않는다고 주장했다. 제3단계와 관련해서는 트래픽 혼잡을 효과적으로 해결하면서도 애플리케이션간에 차별을 하지 않는 기술, 예를 들면 네트워크 용량 확대는 찬성한다고 했다.[233]

232) Ibid at paras 823-24.

크리에이터와 프로듀서 그룹도 BitTorrent 기반의 유통의 잠재적 경제효과를 강조하면서 망 중립성을 지지했다. 예를 들면, 독립영화와 텔레비전연맹(Independent Film and Television Alliance, IFTA)과 캐나다 영화텔레비전제작협회(Canadian Film and Television Production Association)는 프레젠테이션을 통해 ① 독립영화제작자는 캐나다와 미국에 있어 중요한 컨텐츠 창작자이며 ② 인터넷은 독립적으로 제작된 작품의 자금지원, 제작 및 유통에 있어 필요한 도구(때로는 유일한 도구)이며, ③ ISP와 제작사의 수직적통합과 같은 업계합병은 합작한 작품의 우선 취급(및 더욱 빠른 속도)의 방법으로 독립적으로 제작된 작품을 위협하며, ④ 네트워크 혼잡에 대한 보다 명확한 개념 정의가 필요하고, ⑤ 광대역 서비스에 대한 수요에 부합하기 위한 최선의 방법은 용량확대이며, ⑥ 트래픽관리 실태를 반드시 소비자에게 투명하게 공개하여야 하며, ⑦ 방송통신위원회는 ISP가 통신법 제27조 제2항의 면책대상이 되는지를 재고해야 한다고 주장했다. 라스트 마일(last-mile)[234] 용량 확대 또는 컨텐츠 전달 네트워크 배정 등과 같이 트래픽 속도를 제한하지 않으면서 혼잡 문제를 해결할 수 있는 다른 방안에 대해서도 설명했다.[235]

캐나다 장애인의회(The Council of Canadians with Disabilities)와 ARCH 장애인법 센터(ARCH Disability Law Centre-ARCH, 이하 센터라 함)는 명확한 지침과 통신법 제27조와 제36조의 주석서를 마련할 것을 방송통신위원회에 촉구했다. 이들 단체는 트래픽 관리는 직·간접적으로 차별을 해서는 안 되며 장애인이 자신의 프라이버시를 포기하도록 해서는 안 된다고 주장했다. 센터는 또한 통신법 제36조의 논란에 대해 3단계 접근법을 발표했다. 3단계 접근법은 트래픽 관리가 ① 제36조에 의거해 위반이 되는지 검토, ② 법에 위배되는지 및 불공정한 차별에 해당되는지 검토, ③ 중립/긍정적인 개입 기준에 근거한 정당화 가능성 검토로 구성된다. 마지막으로 인터넷상의 수많은 지원 프로그램을 고려해 이들 단체는 트래픽 관리가 필요한 특별 예외 조항(예를 들면 장애인을 위해 필요한 서비

233) 인터넷연합 프레젠테이션, Ibid vol 2 at paras 991-1055.

234) 역주: 소비자 가정으로 직접 연결된 전화나 케이블의 일부 시스템으로 쉽게 말해 기간통신사 선로 중 소비자 가정에 이어지는 마지막 부분을 말함. 보통 백본망은 하이스피드라 함.

235) Ibid vol 3 at paras 2040-2117.

스)에 대한 백서작성을 주장했다. 따라서 트래픽 관리 정보공개는 장애인에게 있어 매우 중요하다.[236]

캐나다 인터넷정책 공익클리닉(Canadian Internet Policy and Public Interest Clinic- CIPPIC, 이하 공익클리닉이라 함)은 민주미디어캠페인(Campaign for Democratic Media, CDM)을 대신해 특히 통신법 제27조 제2항과 제36조의 위반에 관한 규범지침 마련과 ISP의 영역 구분을 권고했다. 민주미디어캠페인은 이 사안을 프라이버시와 관련해 "공공 인터넷" 공간에 대한 실질적이고 이론적인 침해로 간주하였다. 트래픽 혼잡과 관련해 사용자와 공급자 측면의 문제를 모두 고려해야 한다고 주장했다. ISP는 최선의 역량을 제공하고 있지 않을 뿐만 아니라 P2P 파일공유가 트래픽 혼잡의 원인은 아니라고 했다. 공익클리닉은 시장의 기능은 수요와 공급을 충족시키는 것이지 수요를 억압하는 것이 아니다"라고 주장했다. 또한 공익클리닉과 민주미디어캠페인은 ISP의 트래픽 속도 제한의 적법성은 부인하고 개방형 인터넷의 가치를 강력히 지지했다. ISP가 경쟁하는 주요한 방법은 광대역 망을 확대하는 것이며 따라서 ISP는 인위적으로 망이 부족한 상황을 만들어 경제적 이익을 취해서는 안 된다고 주장했다. ISP를 포함해 누구도 인터넷을 적법하게 소유할 수 없다는 점을 상기시켰다. 민주미디어캠페인은 또한 "공공 인터넷"과 "전용 서비스"간의 명확한 정의의 구분과 무제한적인 트래픽 증가로 인해 트래픽 혼잡이 발생하고 이는 서비스의 악화로 이어질 수 있다는 추정 등 방송통신위원회가 고수하는 추정과 정의에 대해 의문을 제기했다. 대신 민주미디어캠페인은 인터넷 트래픽 증가에 부합하는 공급확대가 이루어지지 않는다면 혼잡이 발생할 수 있다고 주장했다. 민주미디어캠페인은 또한 일정한 인터넷 트래픽 관리가 문제해결에 적합한 방법일 수 있다는 방송통신위원회의 가정에 의문을 제기했다. 민주미디어캠페인은 트래픽 관리는 "트래픽 개입(traffic interference)" 행위라고 주장했다. 민주미디어캠페인에 따르면 P2P 특정 트래픽 관리는 애플리케이션과 사용자에 대한 차별적인 행위이며 겉으로 보이는 것처럼 컨텐츠와 메시지를 제한함으로써 통신법 제36조를 위반하고 있다고 주장했다.[237]

---

236) Ibid at paras 2282-2348.

소비자단체와는 반대로 다수의 통신사와 독립 ISP는 방송통신위원회의 조치를 지지하는 의견을 냈다. 캐나다 매니토바 주 내 최대의 통신사인 MTS Allstream은 이러한 조치에 따라 규제를 하거나 트래픽을 제한할 필요성이 사라지기 때문에 시장경쟁이 활성화 될 수 있다고 주장했다. 이에 덧붙여 인터넷 트래픽 관리는 재판매차원에서만 적용되어야 하며 시장지배적 통신사(dominant carrier)의 기간통신 사업자에게는 결코 이를 적용해서는 안 된다고 주장했다(MTS Allstream에 따르면 일단 네트워크를 기간통신 사업자에게 판매하면 트래픽은 지배적 통신사의 네트워크 범위 외에 있게 되며 해당 네트워크에서 혼잡을 발생시키지 않는다는 것이다). 또한 MTS Allstream은 방송통신위원회가 각각의 인터넷 트래픽 관리 행태의 평가 및 타당성에 대해 실용적으로 사례별 접근방식을 취해야 한다고 주장했다. 트래픽 관리의 합리성 평가를 위한 하나의 기준은 과연 모든 컨텐츠 제공자에게 적용해야 할지에 관한 것이어야 한다. ISP는 네트워크 계획과 엔지니어링, 일반적용규칙 준수, 컨텐츠 취급에 있어 네트워크로 연결하는 위치 및 방법에 상관없이 연결할 수 있는 조치의 적용 및 컨텐츠 애플리케이션 프로토콜(CAP, 예를 들면 차단, 신속처리, 속대 제한, DPI 기술 등)을 통해 자신들이 소유한 네트워크를 관리한다. MTS Allstream은 CAP은 어떤 경우에 있어서는 필요할 수 있으며(예를 들면, 예상치 않은 갑작스러운 트래픽 증가 등), DPI 기술은 광범위한 네트워크 관리 전략 중 하나의 툴에 불과하다고 주장했다.[238]

퀘백에 위치한 소비자보호단체인 Union des Consommateurs는 실질적으로 트래픽 혼잡이 발생하고 있음을 입증할 증거가 충분치 않음을 시사했다. Union des Consommateurs는 방송통신위원회에 소유권의 집중, 합리적인 비용의 서비스 품질, 경쟁을 포함해 다양한 사안에 대해 고려할 것을 촉구했다. 단체는 특정 애플리케이션에 대한 허용 가능한 속도 제한과 관련해 네트워크에서 실제로 혼잡이 발생하고 있고, 긴급을 요구하는 애플리케이션이 만족스럽지 못한 서비스를 받은 경험, 속도를 제한하는 애플리케이션이 엄청난 혼잡의 원인이 되었음을 입증할 수 있는 명확한 증거가 있어야 한다고 주장했다. 하지만 지금까지 제

237) Ibid vol 4 at paras 3306-3424.

238) Ibid vol 3 at paras 2586-2679.

출된 데이터로는 P2P 애플리케이션이 혼잡의 주요한 원인이며 네트워크 용량을 확대해 P2P 트래픽의 '완만한 성장'을 수용할 수 있는지는 명확히 확인할 수 없다고 한다.

네트워크 관리가 필요하다면, 소비자단체는 "애플리케이션 특정 속도 제한"보다는 다른 선택방법이 있다고 주장한다(예를 들면, 피크 시간대 개인 사용자의 이용량 제한). 단체는 DPI 기술, 페이로드(payload) 처리, "애플리케이션 레이어 헤더(application layer header)" 사용은 프라이버시 침해에 대한 우려를 낳을 수 있을 뿐만 아니라 레이어 설계 원칙(layer design principle)을 위반함으로써 건전성을 약화시키고 데이터 암호화를 더욱 촉진할 우려가 있다고 주장했다. 대신 소비자단체는 단층패킷분석(Shallow Packet Inspection-SPI) 기술사용을 제안하였는데 그 이유는 SPI는 패킷의 페이로드를 검사하지 않아 프라이버시에 관한 우려를 경감시킬 수 있기 때문이다. SPI 기술은 각각의 흐름에 대한 통계를 수집하고 수집된 자료를 바탕으로 트래픽 흐름을 애플리케이션 종류별로 분류할 수 있다. 단체에 따르면 실험연구를 통해서 이러한 분류 방식이 매우 정확하다고 한다. 단체는 분류방식이 네트워크 관리를 위한 매우 구체적인 방법이라고 밝혔다. [239]

인터넷사업자연합은 혼잡이 캐나다 ISP 부문의 경쟁력 부족을 여실히 보여주고 있다고 주장했다. 따라서 연합은 네트워크 보안을 제외하고(네트워크 공격 차단) 주요 통신사가 자사의 도매 트래픽에 대한 트래픽 관리 역시 금지하도록 것을 방송통신위원회에 촉구했다. 경쟁을 더욱 강화하기 위해서는 통신재판매사업자를 위한 트래픽 관리의 사용은 최종 사용자가 결정해야 하고 따라서 반드시 사용자의 동의를 받아야 한다. '독립 ISP'를 대신해 인터넷사용자연합은 공격적으로 그리고 사용자의 동의 없이 이루어지는 인터넷 트래픽 관리는 "통신의 목적 또는 의미"에 개입함으로써 통신법 제27조 제2항과 제36조를 위반한다고 주장했다. 연합은 네트워크 용량구축과 망 세분화가 프라이버시 침해를 최소화할 수 있는 네트워크 관리방법이 될 수 있다고 재차 주장했다. [240]

---

239) Ibid vol 6 at paras 4718-70.

240) Ibid vol 4 at paras 2956-3031.

이후 질문에서, 인터넷사업자연합은 정보공개의 필요성을 강조했지만 개인정보는 향후 상업적인 이유로 사용한다 해도 트래픽 관리를 위해서는 사용되어서는 안 된다고 주장했다. 인터넷사업자연합은 현재의 프라이버시 제도를 벗어날 필요는 없다고 주장했다(예를 들면, 개인정보보호와 전자문서에 관한 법 및 통신비밀에 관한 방송통신위원회의 결정). 또한 연합은 트래픽 혼잡은 결코 인터넷 트래픽 관리에 관한 정책의 입안이 아닌 소비자의 선택과 경쟁에 관한 것이어야 한다고 강조했다. 연합은 또한 영국의 경우, 브리티시 텔레콤의 수직적 통합으로 인한 문제 해결을 위해 도매 서비스에 개별적으로 요금을 부과하고 있음을 보여주는 MTS Allstream가 제출한 증거에 대해서도 언급했다. 이러한 개별요금부과 정책은 경쟁심화로 이어지고 따라서 망 중립성 문제도 완화하게 될 것이다. 연합은 또한 기간통신 시장이 너무 작기 때문에 재판매 사업자가 혼잡의 원인이 되지 않음을 강조했다. Bell이 최초로 통신 재판매 시장에 트래픽 관리를 적용하고 다음으로 기간통신 시장에도 적용했다는 사실은 기간통신 시장과 통신 재판매 시장을 분류할 수 있으며 Bell이 재판매 사업자에 대해서는 별다른 우려를 하지 않았음을 보여주고 있다. 연합은 이에 더해 통신 재판매차원에서 최종 소비자가 동의한다면 어떠한 형태든 인터넷 트래픽 관리는 허용되어야 함을 명확히 했다.[241]

다. 망 중립성 반대 논거

소비자, 크리에이터 그룹, 일부 독립 및 지역 통신사는 망 중립성을 지지하고 있지만 기존의 통신사와 케이블 운영자는 새로운 규제조치에 대해 반대했다. Telus는 트래픽 혼잡이 심각한 문제가 된다면 트래픽을 관리할 권리가 있다고 주장했다. Telus는 또한 네트워크 용량 구축은 용량부족에 대한 해결 방안 중 하나에 불과하다고 보았다. 다른 해결방안으로는 트래픽 관리 및 사용기반 요금제 등이 있다. Telus는 또한 사전접근방식으로 “공통적으로 적용되는(one size fits all)” 규제는 통신사에 있어 위험을 증가시키는 원인이 될 수 있다고 주장했

241) Ibid at paras 3050-3275.

다. 대신 Telus는 방송통신위원회가 일반원칙을 마련할 것을 제안했다. 또한 불합리한 차별이 발생하면 예를 들면 사후 접근방식으로 문제를 해결해야 한다고 주장했다. 마지막으로 Telus는 불합당한 차별에 더해 방송통신위원회는 정당한 형태의 차별 허용을 필요성에 대해서도 고려해야 한다고 주장했다. [242]

이후 질의 시간에 Telus는 인터넷 서비스는 공공재에 해당되지만 ISP간 경쟁으로 인해 ISP 자체가 공공재는 아니라고 주장했다. Telus는 비록 트래픽 관리가 사용자의 프라이버시 권리를 침해하다면 사용자는 이에 대해 관심을 갖게 될 것이라는 점은 인정했지만 인터넷 사용자의 대다수가 ISP가 결정한 트래픽 관리에 대해 관심이 없다고 주장했다. 하지만 Telus는 소비자의 측면에서 더 나은 서비스를 위해 혼잡 관리를 계속할 수 있으며 기존의 연방 프라이버시 법률만으로도 잠재적인 우려를 해결하는데 충분하다는 입장을 고수했다.[243]

프레젠테이션을 통해 Rogers는 캐나다는 세계 제1의 케이블 모뎀 서비스 보급률을 자랑하고 있으며 선진8개국 중 가장 높은 수준의 광대역가입자망을 구축하고 있음을 언급했다. Roger에 따르면 정부 규제를 최소화했기 때문에 이렇게 놀라운 성공을 거둘 수 있었다고 한다. 즉, 정부 규제가 아니라 시장의 힘에 따라 이러한 성과를 거둘 수 있었다는 것이다. 개방형 인터넷, 통신사 차원의 반(反)경쟁 또는 프라이버시를 침해하지 않는 조치에 대한 약속을 공식화하기 위해 Rogers는 방송통신위원회에 인터넷 트래픽 관리 지침을 마련하지 않을 것을 촉구했다. 대신 Rogers는 사례별로 개별 인터넷 트래픽 관리 실태를 조사하는 연방통신위원회(FCC)의 접근방식을 채택하는 것이 더욱 효과적이라고 주장했다. 이러한 방식을 통해 위원회는 캐나다 ISP가 적합한 네트워크 관리를 위해 필요한 유연성을 보장할 수 있을 것이라고 했다. Rogers는 트래픽 관리는 단순한 트래픽 셰이핑 이상이라고 지적하면서 이는 소비자와 네트워크를 스팸으로부터 보호하고 서비스 공격과 바이러스 공격을 차단하고 아동 포르노 사이트 접근을 차단할 수 있다고 주장했다.

Rogers는 다른 사용자들의 공정한 네트워크 이용을 위해 업스트림 P2P 트래

242) Ibid vol 5 at paras 4065-4114.

243) Ibid at paras 4140-4366.

픽의 속도를 정형화(rate shaping- 전송량 제한)을 시행하고 있음을 인정했다. 이러한 전송량 제한은 단순히 자사의 서비스를 우선취급하는 것이 아니며 트래픽을 관리하지 않으면 경쟁사인 VOIP 제공자 역시 혼잡에 따른 피해의 가능성을 강조했다. 혼잡 해결을 위한 네트워크 역량 확대와 관련해 Rogers는 혼잡 문제를 해결하기 위해서는 추가로 상당한 업스트림 용량이 필요하며 이는 모든 소비자에 대한 요금 인상으로 이어질 수 있다고 했다. 도매 소비자의 경우 그들이 이용하는 서비스의 본질에 대해 이해하고 소비자의 요청에 대해 적합하게 대응하게 하려면 상당한 정보공개가 이루어져야 한다고 주장했다. 소비자단체가 제기하는 프라이버시 침해는 상당부분 이론적인 것이며 실무에 기초한 것이 아니라고 주장했다. Rogers는 현재 모바일 무선 데이터 트래픽의 속도를 정형화하고 있지는 않지만 무선 서비스 사용이 증가함에 따라 향후 일정한 형태의 트래픽 관리가 필요할 수 있다고 했다.

통신법 제36조와 관련해 Rogers는 P2P 파일 공유 컨텐츠의 속도를 제한하지 않고 있으며 또한 문제가 되는 파일의 의미 또는 목적을 변경하지 않는다고 주장했다.[244] 또한, 제27조 제2항과 관련해서는 동조항의 목적은 애플리케이션 제공자 보호에 있지 애플리케이션 그 자체의 보호에 있지 않다고 주장했다.

퀘백 주 내 최대 서비스 제공자인 Videotron 역시 방송통신위원회가 규제를 해서는 안 된다고 주장하면서 당시 잠재적인 문제 해결을 위한 '경제적 조치'만을 사용하고 있지만 향후 기술적 조치(예를 들면 트래픽 관리)의 사용 배제에 대해서는 거부 의사를 표명했다. Videotron은 "실질적인 문제"가 확인 되었을 때에만 규제를 적용해야 한다고 주장했다. 다만 시장지배적 통신사는 트래픽 관리를 회사의 통신 재판매사업자가 아닌 가입자에게만 적용해야 한다고 주장했다. 또한 엄청난 용량 확대비용을 초래할 수 있고 통신사는 통신 재판매사업자가 아니라 이러한 비용을 모두 부담해야 하는 네트워크 운영자임을 고려할 때 네트워크 관리가 필요하다고 주장했다.[245]

Shaw는 막대한 비용을 투자하였지만 P2P 트래픽으로 인해 여전히 네트워크

244) Ibid vol 6 at paras 4892-4939.

245) Ibid at paras 5332-81.

혼잡을 경험하고 있다고 했다. 따라서 Shaw는 투자와 함께 적합하고 필요한 네트워크 관리 전략이 함께 시행해야 할 필요성을 주장했다. 통신법은 현재 모든 ISP의 불합리한 특혜 또는 통신에 대한 개입을 금지하고 있다고 하면서 이미 현재의 규제만으로도 충분히 효율적으로 소비자를 보호할 수 있다고 주장했다.

Shaw는 DPI 기술이 P2P 애플리케이션의 과도한 광대역 망 사용 문제를 해결할 수 있는 "가장 효과적이며 효율적인 방법"이기 때문에 업스트림 P2P 트래픽을 제한하기 위해 이러한 기술을 사용하고 있다고 했다. 트래픽 관리기기를 연중무휴로 운영하고 있으며 기기는 혼잡 시간대에만 자동으로 트래픽을 조절한다고 했다. Shaw는 개별 ISP는 DPI 기술사용, 광대역 망 제한, 과도한 광대역 망 사용에 대한 추가 요금 징수, 시간대별 요금제, 캐싱(,catching), 용량 확대, 통신법 제27조 제2항과 제36조를 위반하지 않는 기타 방법을 포함하는 통신사만의 네트워크 관리 전략을 선택할 수 있다고 주장했다.

기조연설에서 Bell Canada는 공청회의 요지는 혁신에 관한 것이라고 주장했다. 통신사의 트래픽 관리는 (ⅰ) 제한적이고 긴급을 요하지 않는 트래픽에 제한되며, (ⅱ) 특정한 시간대에 제한되며, (ⅲ) 컨텐츠에 대한 접근을 차단하지 않는다고 했다. 프라이버시 문제와 관련해 Bell은 DPI는 단순히 트래픽 관리 목적으로만 사용되며 사용자의 통신 콘텐츠를 검사하지 않는다고 했다. 또한 망중립성 지지진영이 방송통신위원회에 제출한 주장과는 달리 재판매 사업자와 기간통신사업자의 GAS 사용자가 동일한 네트워크를 공유하는데 그 결과, 도매 트래픽은 소매 트래픽에, 소매 트래픽은 도매 트래픽에 영향을 미친다고 했다. 또한, Bell은 자사의 도매 소비자는 이들의 전체 시장 점유율을 지적하면서 회사의 소매 네트워크에 미치는 영향을 중요치 않게 생각한다고 주장했다.

Bell은 방송통신위원회에 다음의 세 가지 지침을 고려해 줄 것을 제안했다. (1) 부정적인 영향 제한- ISP는 인터넷 트래픽 관리가 소비자, 서비스, 프로토콜 또는 애플리케이션에 미칠 수 있는 부정적인 영향을 제한하기 위해 "합리적인" 노력을 다한다. 여기서 "합리적"이라 함은 각각의 네트워크는 네트워크 별로 다른 문제에 직면하고 있기 때문에 유연성이 필요함을 의미한다. (2) 투명성 - ISP는 트래픽 관리의 영향을 받을 수 있는 재판매 사업자와 기간통신사업자에게 "트래픽 관리의 본질을 네트워크의 보안과 상업적으로 민감한 정보를 위태롭게

하지 않는 방법으로 공개한다." (3) 프라이버시 - ISP는 프라이시 보호법에 의거하여 인터넷 트래픽을 관리한다. 통신법 제36조와 관련하여 Bell은 이 조항은 트래픽 관리에는 적용할 수 없다고 주장했다.[246]

Bell은 현 프라이버시 보호법(에를 들면, 개인정보보호와 전자문서에 관한 법)은 고객의 동의하에 마케팅 목적으로 수집한 데이터의 사용을 허용해야 한다고 주장했다.[247] 또한 "가장 침해가 적은 시험"이라 함은 현재 "가장 침해가 적은 방법"에 대한 합의가 없음에도 불구하고 단 하나의 단정적인 "가장 침해가 적은 방법"을 뜻한다고 주장했다. Bell이 주장하는 바와 같이 단정적인 기준은 피하고 대신에 합리적인 기준을 적용하는 것이 좋을 것이다. 이러한 이유로 Bell은 사전적이 아닌 사후적인 접근방식을 지지한다. Bell에 따르면, 프로토콜을 가리지 않는(protocol-agnostic) 즉, 비차별적 접근방식은 긴급을 요하는 트래픽을 포함해 사용자의 모든 트래픽의 속도 감소로 이어질 수 있다고 한다. 일부에서는 비차별적 시스템이 확실한 방법이라고 주장하지만 Bell은 오히려 이러한 시스템은 불합리하고 프라이버시를 침해하게 된다고 반박한다.[248]

프레젠테이션을 통해 Cogeco 케이블은 네트워크 관리의 일환으로 트래픽 셰이핑을 이용하고 있으며 이는 광대역 망을 지나치게 많이 사용하는 P2P 트래픽 애플리케이션을 대상으로 한다고 밝혔다. Cogeco는 트래픽 관리의 이유로 "공정하고 지속 가능한" 인터넷 서비스 제공을 들었다. 다음으로 Cogeco는 컨텐츠에 개입하지 않으며, 통신을 방해하거나 차단하지 않고(특정한 P2P 프로토콜의 특징을 파악하기 위한 최소한의 헤드 검사를 통한 P2P 전송 및 각각의 패킷의 페이로드 속도 둔화) 개인 식별인자를 검사하지 않는 트래픽 셰이핑 기술의 주요한 특징 을 간략하게 설명하였다. Cogeco는 또한 인터넷 트래픽 관리 규제 및 개인의 프라이버시를 보호하기 위한 추가 규칙이 필요 없다고 주장했다.[249]

Primus Telecommunications Canada는 모든 ISP는 자신들의 네트워크를 관리하고 적합하다고 판단하는 인터넷 트래픽 관리를 시행할 수 있어야 하며, 모든

246) Ibid vol 7 at paras 5972-6032.

247) Ibid at paras 6319-33.

248) Ibid at paras 6348-74.

249) Ibid vol 5 at paras 4401-71.

트래픽 관리는 사용자의 동의하에 이루어지고 있고 이와 관련해 어떠한 연역적인 잘못도 없을 뿐만 아니라 오직 혼잡이 발생한 때에만 네트워크 관리와 계획을 위해 DPI 기술을 이용하고 있다고 주장했다. Primus는 또한 모든 ISP는 소매와 도매 서비스 차원에서 이루어지는 인터넷 관리 실무에 대한 정보를 공개해야 하지만 보안과 관련한 사안은 공개해서는 안 된다고 덧붙였다.[250]

위성 인터넷 제공자인 Barrett Xplore는 농어촌 지역을 대상으로 하는 소규모 ISP 측면에서 트래픽관리를 논의하였다. Barrett는 각각의 ISP는 운영 상황, 혼잡 상황 및 비즈니스 모델에 맞는 트래픽 관리 툴을 사용할 수 있도록 허용해야 한다고 주장했다. 특히 모든 고객에게 최상의 서비스를 제공할 수 있도록 혼잡 시간대에 트래픽을 관리할 수 있는 적합한 툴의 사용의 필요성을 강조했다.

애플리케이션 특정 트래픽 관리와 관련해서는 광대역 망을 과도하게 사용하는 애플리케이션에 대한 차별은 통신법 제27조 제2항에 의거한 불공정하고 불합리한 차별이 아니라고 주장했다. 트래픽 관리 기술은 개별 사용자나 개별 애플리케이션을 대상으로 하지 않으며 피크 시간대에 광대역 망을 과도하게 사용하는 애플리케이션을 대상으로 하기 때문에 모든 애플리케이션에 차별 없이 적용된다고 주장했다. 또한 가입을 할 당시 소비자에게 서비스 제한에 대해서 알렸다면 이러한 트래픽 관리 툴은 합리적이며 필요하다고 덧붙였다. Barrett는 이러한 트래픽 관리 툴이 없다면 위성 무선 네트워크를 통해 캐나다 내 농어촌 지역까지 서비스를 확대할 사업적 이유가 없으며 고객들이 적합한 가격에 서비스를 제공받을 수 없다고 주장했다.

라. 결 정

2009년 10월 방송통신위원회는 망 중립성 침해에 대한 결정을 발표하였다.[251] 비록 위원회의 ITMP 결정이 망 중립성 지지자들이 희망했던 만큼의 결과는 아

250) Ibid vol 4 at paras 3779-3855.

251) CRTC, Telecom Regulatory Policy CRTC 2009-657: Review of the Internet traffic management practices of Internet service providers, (Ottawa: CRTC, 2009), online: CRTC (http://www.crtc.gc.ca/).

니었지만[252], 일부 중요한 부분에 있어서는 많은 진전을 보여주었다. 하지만 결정에 따라 ISP는 더 이상 마음대로 트래픽을 관리할 수 없게 되었다. 하지만 다른 한편으로는 이번 결정은 트래픽 속도 제한과 같은 트래픽 관리가 계속될 수 있음을 뜻한다. 소매 서비스에 대한 결정의 주요 내용은 다음과 같다.

(1) 트래픽 관리에 관한 새로운 제도를 도입한다. 소비자는 트래픽 관리에 대해 불만을 접수 할 수 있거나 또는 위원회가 자체적으로 조치를 취할 수 있다. 트래픽 관리가 이루어지고 있다고 믿을만한 불만이 접수되면, ISP는 다음을 이행하여야 한다.

사용하는 인터넷 트래픽 관리(Internet Traffic Management Practice, ITMP) 및 관리의 필요성과 목적 및 효율성을 설명하고 ITMP가 차별 또는 특혜에 해당하는 지를 설명한다.

조금이라도 차별 또는 특혜가 있는 경우,

- ITMP 문제가 되는 사안을 해결하기 위해, 그 목적에 부합하고 효율적이며, 문제해결 이외에는 다른 이유가 없음을 입증하고,
- ITMP로 인한 차별 또는 특혜를 합리적으로 가장 최소한으로 하고,
- 부차적인 ISP, 최종 사용자, 또는 다른 사용자에 대한 어떠한 피해도 합리적으로 최소화하고 있음을 입증하고,

252) 예를 들면, 위원회는 이용량 기반 요금제와 광대역망 제한을 허용했다. 하지만 이 두 가지 방법의 사용 확대는 인터넷의 선택, 이용가능성 및 가격을 저해한다는 이유로 미디어뿐만 아니라 정치적으로도 비난을 받았다. 2011년 초, 방송통신위원회는 이용량 기반 요금제에 대한 결정을 발표하였다. [CRTC, Telecom Decision CRTC 2011-44: Usage-based billing for Gateway Access Services and third-party Internet access services, (Ottawa: CRTC, 2011), online: CRTC (http://www.crtc.gc.ca/)]. 하지만 이에 관한 결정의 내용은 위원회가 이러한 문제를 어떻게 해결해야할지 알지 못하고 있음을 스스로 보여주었다. 저자의 본 결정에 대한 자세한 분석은 "Unpacking The Policy Issues Behind Bandwidth Caps & Usage Based Billing" (1 February 2011); Michael Geist, "What to do About Retail Usage Based Billing: A Modest Proposal" (7 April 2011); Michael Geist, "Why Net Neutrality and Usage Based Billing Are Two Sides of the Same Coin" (2011년 7월 11일); and Michael Geist, "Competition, Not Congestion Driving Internet Data Cap Debate" (18 July 2011), online: Michael Geist's Blog (http://www.michaelgeist.ca/)] 참조.

- ITMP의 기술적인 측면에 있어 네트워크 투자 또는 경제적 접근만으로는 ITMP와 동일한 목적을 효율적으로 해결할 수 없는 합당한 이유를 설명하여야 한다.

(2) 다음의 두 가지 사항을 고려하여야 한다. 첫째, 통신법 제27조 제2항의 의거해 특정한 애플리케이션에 대해 특혜를 주거나 또는 반대로 차별하는 트래픽 관리가 조사 대상이 되는지 둘째, 경제적인 트래픽 관리(예를 들면, 데이터 상한제)의 여부이다.

(3) 위원회는 트래픽 속도 제한에 관여한다. 위원회는 속도에 민감한 트래픽(예를 들면, 실시간 오디오 또는 동영상)과 관련해 트래픽 속도 제한이 현저한 속도 둔화를 야기할 경우 이러한 제한이 "컨텐츠 제한에 해당되고 문제가 되는 통신의 의미 및 목적에 영향을 미치는지"를 판단한다. 위원회는 이러한 활동에 대하여 사전에 승인을 받도록 한다. 시간에 민감하지 않은 트래픽에 대해서도 위원회는 트래픽 관리가 어느 정도까지 컨텐츠 차단 또는 제한에 해당되는지를 판단하고 이 경우 사전 승인을 받도록 한다.

(4) 위원회는 새로운 공개 요건을 의무화한다. ISP의 트래픽 관리를 관리 이유, 영향을 받는 대상, 관리 시기, 트래픽 관리의 대상이 되는 인터넷 트래픽, 사용자의 인터넷 사용에 미치는 영향(속도 등 특정한 영향)을 포함해 트래픽 관리에 대해 소비자에게 정보를 공개하도록 한다.

(5) 위원회는 또한 심층패킷분석으로 수집한 정보의 사용과 관련해 새로운 프라이버시 요건을 마련한다. 따라서 ISP에게 "트래픽 관리 목적으로 수집한 개인정보를 다른 목적으로 사용하거나 공개하지 못하도록 한다."[253]

또한 통신 재판매와 관련해, 위원회의 결정은 도매 서비스에 대해서는 설명하고 있다. 현재 운영 중인 ISP가 독립 ISP를 자사의 소매 고객과 동등하게 취급하면 동일한 불만접수 방식을 적용한다. 이러한 접근 방식이 제한적일 경우 사전 승인을 받아야 한다.[254]

253) Supra note 128 at paras 20-99.

254) Ibid at paras 68-95.

위의 요약에서 설명한 바와 같이, 위원회 결정은 공청회 기간 동안 소비자 단체가 권고한 방법과 유사한 검사 방법을 도입하고 있다. 또한 위원회는 애플리케이션 특정 조치에 대한 문제점을 인식하고 있고 새로운 공개 요건, 프라이버시 보호 조치 및 특정한 상황에서 트래픽 속도 제한의 통신법 위반에 대한 합의를 도입했다.

5. 2009-2012년: 인터넷 트래픽 관리 시행 및 기타 망 중립성 관련법

ITMP에 관한 공청회를 열기 전에 방송통신위원회는 망 중립성 시행에 대해서 확신을 갖고 있지 않았다. 예를 들면, 위원회는 통신법 제27조 제2항과 제36조를 제한적으로 적용하고자 했다.[255] 전술한 바와 같이 2009년 방송통신위원회의 ITMP 제도의 도입을 많은 망 중립 지지자들은 매우 긍정적인 변화로 보았다. 하지만 시행 초기부터 과연 이러한 새로운 규칙을 어떻게 적용할지에 대한 의문이 제기되었다. 사실, 소비자에게 똑같이 책임을 부과하는 등 위원회는 사실상 지속적으로 트래픽 속도 제한을 보장했다.

이러한 문제점 해결을 위해 위원회에 ISP 트래픽 관리에 대한 정기 감사 요청, 정부에 대한 위원회의 ISP의 트래픽 관리 지침 준수 감독 요청, 자체적으로 조사를 실시하는 소비자단체에 대한 재정지원 및 연방정부의 적극적인 개입 등 몇 가지 제안이 이루어졌다(예를 들면, 무선 인터넷 접근을 위한 망중립 마련).

2010년 초, Bell, Rogers, Shaw, Telus, Cogeco, Videotron 등 캐나다의 대형 ISP는 새로운 지침에 대해 서로 엇갈리게 대응하였다. 6개 제공자 중, Telus,

255) CRTC, Telecom Decision CRTC 2005-28: Regulatory framework for voice communication services using Internet Protocol, (Ottawa: CRTC, 2005); and CRTC's hand-off approach to the Internet regulation in CRTC, Broadcasting Regulatory Policy CRTC 2009-329: Review of broadcasting in new media, (Ottawa: CRTC, 2009), online: CRTC (http://www.crtc.gc.ca/) 참조. 뉴 미디어 결정은 인터넷과 같은 새로운 미디어 환경에 대한 캐나다의 규제 채택 방법을 결정하기 위한 위원회 구상안을 명시하고 있다. 뉴미디어 프로젝트 구상안은 뉴미디어 규제방법을 분석하고 캐나다내 컨텐츠의 제작과 배포에 대한 규제의 영향력 평가를 주요 골자로 하고 있다. 구상안은 또한 네트워크 중립성을 포함해 중요한 접근관련 상안에 대해서도 고려하고 있다.

Cogeco, Videotron은 당시 일부 애플리케이션의 속도를 제한하기 위해 트래픽 속도 제한이나 트래픽 셰이핑 기술을 사용하고 있지 않았다. 나머지 4개 제공자는 이와 관련한 자료를 공개하지 않았고 최소한 2개 제공자는 주장컨대 위원회의 요건을 준수하지 않았다. Bell은 회사의 정책 및 위원회의 지침 준수에 따른 영향에 대해 가장 상세하게 정보를 공개했다. Roger의 정책보고는 광범위한 부분을 자세히 설명하고 있지는 않지만 회사정책, 트래픽 셰이핑 빈도, 서비스 제한의 영향(속도에 미치는 영향)에 대한 내용을 포함했다. 이와는 대조적으로 Shaw, Cogeco는 위원회의 요건을 준수하지 않는 것으로 보인다. Shaw는 P2P 속도를 제한했을 때 이용자가 경험하는 실제 인터넷 트래픽 속도에 대한 정보를 회사 정책상 공개하지 않는다는 입장을 취했다. Cogeco는 회사의 트래픽 관리가 사용자의 인터넷 접속에 있어 어떠한 영향도 미치지 않는다고 주장하면서 이와 관련된 자료를 공개하지 않았다.

방송통신위원회가 망 중립성에 관한 공청회를 열고 약 2년여의 시간이 경과한 시점에서 돌아 보건데 캐나다의 망 중립성은 '실패'한 것으로 보인다. 지난 2년 동안, 실질적으로 모든 인터넷 서비스 제공자들에게 대해 불만이 접수되었지만 변화는 거의 이루어지지 않았다. 사실, 위원회는 접수된 소비자 불만에 대해 위원회의 정책범위 밖이라거나 증거 부족을 이유로 기각한 경우가 많았으며 인터넷제공자의 편을 들어 주는 사례가 많았다.[256] 망 중립성과 관련해 접수된 불만사항 중 절반 이상은 Rogers에 대한 것이었지만 제공자는 어떤 타격도 받지 않았다. 예를 들면, 2010년 가을, Rogers의 P2P 속도 제한에 대해 위원회에 공식적으로 불만을 제기하였다. 당해 제공자는 처음에 이 문제를 축소하려 하였고 나중에야 트래픽 관리와 관련해서는 먼저 공개된 회사정책을 변경해야 한다고 밝혔다.[257] 접수된 사용자 불만에 대하여 위원회는 Rogers의 정보공개가 위원회의 인터넷 트래픽 관리 정책 요건을 준수하지 않는다는 내용의 서한만을 당해 제공자에게 보냈다. Roger는 정보를 제한적으로만 공개하고 이와 관련한 문제를 해

256) Michael Geist, "Canada's Net Neutrality Enforcement Failure" (2011년 7월 8일), online: Michael Geist's Blog (http://www.michaelgeist.ca/) 참조.

257) "Rogers' BitTorrent Throttling Experiment Goes Horribly Wrong" (2010년 12월 13일), online: TorrentFreak (http://torrentfreak.com) 참조.

결함에 있어 미흡했지만 위원회는 트래픽 속도 제한이 업로드에 미치는 영향에 대한 정보만 공개하면 된다고 판단했다.[258] Rogers는 위원회가 보낸 서한에 대해 다운트림 트래픽과 관련해 더 이상 업데이트할 필요가 없다는 주장만을 되풀이했다. 정보공개 정책 변경과 관련해 Rogers가 지목된 이유에 대해 이의를 제기했고 Rogers는 계속해서 일부 애플리케이션의 경우 업로드 트래픽 셰이핑이 다운로드 속도에 영향을 미칠 수 있으며 이는 ISP의 책임이 아니라 애플리케이션 제공자의 책임이라고 주장했다. 이후 Rogers는 몇 가지만을 수정한 정보공개 정책을 발표했다.[259] 이틀 후, 위원회는 접수된 불만에 대하여 Rogers의 대응과 정보공개가 만족스러운 수준으로 이루어 졌다는 결론을 내리고 사건을 종결했다.[260]

2010년 11월, 음악제공사이트가 Bell을 상대로 다운로드 속도를 제한한다면서 불만을 접수했다. Bell은 DPI 기술이 실수로 웹사이트에서 이루어진 다운로드를 P2P 전송으로 잘못 인식해 연결 속도를 늦췄다고 인정했다. Bell은 위원회 지침을 준수하고 있다고 주장을 한했고 나중에야 시정을 약속했다.[261]

2011년 7월까지, 인터넷 서비스 제공자의 정책의 실질적이고 확실한 변경으로 이어진 불만접수는 단 한 건에 불과했다. 2010년 1월, 온타리오에 소재한 인터넷 전화회사 ExaTEL이 위성 인터넷 제공자인 Barrett Xplore을 상대로 불만을 제기하였다. ExaTEL은 Barrett Xplore가 인터넷 전화 속도를 제한해 부당하게 Barrett이 제공하는 전화서비스에 혜택을 주었다고 주장했다. 이 사건에 대해 위원회는 부당한 특혜 제공은 없었지만 시간에 민감한 트래픽의 속도제한은 위원회 지침 위반에 해당한다는 결정을 내렸다. 속도 제한 영업행위를 변경하거나 또는 위원회로부터 특별 승인을 받아야 하는 상황에 직면하게 된 Barrett Xplore는 인터넷 전화서비스에 영향을 미치지 않도록 트래픽 속도 제한 방식을 변경하였

258) An electronic copy of the letter is available online: Michael Geist's Blog (http://www.michaelgeist.ca/component/option,com_docman/task,doc_download/gid,38/) 참조

259) An electronic copy of the response is available online: Michael Geist's Blog (http://www.michaelgeist.ca/component/option,com_docman/task,doc_download/gid,45/).

260) An electronic copy of the notice of closure is available online: Michael Geist's Blog (http://www.michaelgeist.ca/component/option,com_docman/task,doc_download/gid,46/).

261) Supra note 146 참조

다.[262]

때때로 방송통신위원회는 위원회 스스로가 문제의 원인이 되기도 했다. 2010년 3월, Cogeco가 지속적으로 P2P 애플리케이션의 트래픽을 셰이핑한다면서 위원회에 불만이 접수되었다. 트래픽 속도 제한은 실질적으로 네트워크 혼잡의 원인 되는 경우에만 실행할 수 있다는 위원회의 요건을 고려할 때, Cogeco의 정책은 경종을 울리는 사건이었다. 그렇지만 위원회는 사건에 대한 진상조사를 실시하기 전에 접수자에게 더 많은 증거를 제출할 것을 요구했다. 또 다른 예로는, 2009년 12월 Bell이 MediaMonkey.com 웹사이트에 대한 접근 속도를 제한하고 있다는 불만이 접수되자 위원회는 해당 사이트는 Bell의 트래픽 관리 사이트 목록에 등재되어 있지 않다는 이유로 접수된 불만을 기각하였다.[263] 위원회가 접수된 불만을 검토할 때조차도 실질적인 조사는 거의 이루어지지 않았다. 대부분의 경우 문제가 되는 ISP에 서신을 보내거나 ISP의 입장만을 반복할 뿐이었다. 이러한 위원회의 반응은 실질적인 변화가 아니라 정보공개의 수정으로 이어졌을 뿐이다.

2011년, 온라인 게임의 트래픽 속도 제한이 심각한 문제로 대두되었다. 2011년 7월, 위원회는 Rogers에 지속적으로 논란이 제기되는 온라인 게임 사이트 World of Warcraft에 대한 트래픽 속도 제한과 관련해 해당 제공자에게 경고장을 발송했다. 위원회는 문제가 완전히 해결되고 있지 않는 점은 납득할 수 없다며 해당 제공자에게 지속되는 문제를 해결할 것을 요청했다.[264] 하지만 실질적인 개선이 이루어지지 않자 이에 실망한 온라인 게이머들은 망 중립성을 모니터하고 테스트하기 위해 새로운 그룹을 만들었다.[265] 2011년 8월, 위원회는 온라

---

262) 본 사건과 관련한 언론보도는 Xplornet Communications Inc. (formerly Barrett Xplore Inc.)참조. 저자의 Xplornet Communications Inc.,사건에 대한 견해는 "Warning to Editors re: Allegations made by Michael Geist" (2011년 7월 12일), online: CNW Group (http://www.newswire.ca/en/story/745965/warning-to-editors-re-allegations-made-by-michael-geist); and Michael Geist, "The Xplornet's Release: Digging into the Documents" (2011년 7월 14일), online: Michael Geist's Blog 참조. (http://www.michaelgeist.ca/).

263) Supra note 146 참조.

264) An electronic copy of the warning is available online: Dropbox (http://dl.dropboxusercontent.com/u/9038867/Rogers/Rogers_process_letter_13_July.pdf).

인 게이머들이 또 다른 유명한 온라인 게임사이트 Call of Duty의 트래픽 속도를 제한하고 있다며 Rogers를 상대로 불만을 접수하자 위원회는 Rogers에 다시 한 번 사건을 조사할 것을 요청했다.[266] 이후 Rogers는 '아마도' 회사가 온라인 게임의 트래픽 속도를 제한한 것 같다고 했고 위원회는 온라인 게임 사이트의 트래픽 속도 제한을 중단할 것을 요청했다.[267]

거의 2년여의 시간동안 30여 건 이상의 조사가 이루어 진 후에야 개선이 필요하다는 점이 분명해졌다. 방송통신위원회는 새로운 지침을 발표하고 2011년 9월부터 망 중립성 규칙을 시행하였다.[268] 위원회는 위원회에 접수된 불만 건수 및 내용에 대한 개요, 현재 조사가 진행 중인 사건 및 해결된 사건의 수를 분기별로 공개할 것을 약속했다. 또한, 해당 ISP명, 불만 내용을 포함해 위원회 지침 위반 사례를 위원회 홈페이지에 게재하겠다고 발표했다. 투명성 개선을 위한 노력은 환영할 만한 일이며 ISP가 지침을 준수하도록 압력을 가하는 중요한 움직임이 되었다. 새로운 지침은 이전에 Xplorenet가 트래픽 속도 제한과 관련해 수개월을 끌었던 것처럼 ISP의 늦장대응을 사전에 방지하기 위하여 정해진 시간 내에 시정을 하도록 하는 내용을 포함하고 있다.

또한 새로운 지침은 개별 불만접수에 대해서도 요건을 명확히 명시하고 있다. 공식적인 불만접수는 다음의 요건을 충족해야 한다.

- 문제가 되는 ISP가 ITMP 정책의 공개 요건을 충족하지 않음,
- ISP의 ITMP가 특정 애플리케이션 접속에 영향을 미침(예를 들면 지속적으

265) Jason Koblovsky, "Canadian Gamers Fed Up With CRTC on Net Neutrality issues", Open Media (2011년 8월 4일); 및, "It's Official: Gamers have Caught Rogers Violating Internet Openness Rules", Open Media (2011년 10월 27일) online: Open Media (https://openmedia.ca/).

266) "Rogers asked to probe possible game throttling", CBC (2011년 8월 30일) online: CBC (http://www.cbc.ca/) 참조.

267) Peter Darbyshire, "CRTC tells Rogers to stop throttling online games", The Province (2011년 9월 16일) online: The Province (http://www.theprovince.com) 참조.

268) Telecom Information Bulletin CRTC 2011-609: Internet traffic management practices – Guidelines for responding to complaints and enforcing framework compliance by Internet service providers, (Ottawa: CRTC, 2011), online: CRTC (http://www.crtc.gc.ca/).

로 접속하고자 하는 애플리케이션과의 연결이 끊겨 애플리케이션을 사용할 수 없음),

- ISP가 보다 속도를 제한하기 위해 ITMP를 변경하였거나 30일의 공지 기간도 없이 새로운 ITMP를 시행함,
- ISP가 ITMP 정책 요건을 준수하지 않거나 또는 ISP의 ITMP가 통신법을 위반함[269]

방송통신위원회는 시정청구는 반드시 다음의 증거를 제출하도록 하였다.

- 청구자가 생각하는 문제가 되는 ISP가 ITMP 제도 중 준수하고 있지 않는 부분(청구 이유의 근거가 되는 상황은 위의 예시 참조)
- 문제 발생 시기 및 재발여부,
- 영향을 받는 애플리케이션,
- 영향의 내용 및,
- 해당 ISP의 대응을 포함해 문제 해결을 위해 ISP가 직접적으로 취한 조치[270]

위의 요건은 시정청구 요청을 제대로 할 수 있는 기술적인 전문지식이 부족한 대부분의 인터넷 사용자의 역량을 넘어서는 것으로 보인다. 위원회가 이렇듯 사용자의 시정청구에 기반한 접근방식(ISP의 사전 대책 이행과는 대치 됨)을 고집하는 것은 망 중립성 규칙의 진정한 시행을 저해했다. 또한 위원회는 예를 들면, 망 중립성 위반에 대해 벌금을 부과할 수 있는 권한 등 엄격한 처벌권한이 없었다.

이러한 문제점에도 불구하고, 새로운 지침은 위원회가 보다 강력한 접근방식을 채택할 준비가 되어 있음을 시사한다. Rogers는 ISP 중 처음으로 온라인 게임의 트래픽 속도 제한으로 "강제 시행" 명령을 받았다.[271] 비슷한 시기에 Bell은 P2P 파일 공유로 인한 네트워크 혼잡이 감소였음을 밝히고 자사의 도매 인

269) *Ibid* at para 13 [각주생략]

270) *Ibid* at para 14 [각주생략]

271) CRTC는 2011년 10월 27일 Rogers에 준수 및 집행(Compliance and Enforcement Sector)관한 서한 전달, CRTC의 서한은 Open Media 사이트에서 볼 수 있음 (https://openmedia.ca/sites/openmedia.ca/files/Koblovsky_File-545613_27-10-2011.pdf).

터넷 제공 고객에게 회사가 트래픽 관리를 하지 않음을 정식으로 알렸다. Bell의 발표는 트래픽 혼잡 해소를 위한 지속적인 소매 트래픽 속도 제한이 위원회 지침을 위반할 가능성이 있음을 시사하였다.[272] Rogers와 Bell의 사례를 통해 규칙 시행측면에서 위원회가 효과적으로 대응할 수 있는지 또는 얼마나 이 문제를 심각하게 보고 있는지를 보여주고 있다.

2012년 1월, 위원회는 Rogers에 조사를 종결했고 실질적으로 ITMP 규칙을 위반했다고 통보했다. 위원회는 Rogers가 디폴트 P2P 포트를 사용해 확인되지 않은 시간이 민감한 트래픽에 기술적인 ITMP를 사용한 것은 명백한 트래픽 감소에 해당되므로 사전 승인이 요구된다고 밝혔다. 위원회는 Rogers에 2주 동안 제출된 증거에 대해 반박자료를 내거나 아니면 관련법을 준수할 것을 명령했고 Rogers는 2012년 말까지 모든 소비자에 대한 인터넷 트래픽 속도 제한을 중단하겠다고 밝혔다.[273] 또한 위원회는 약속했던 대로 홈페이지를 통해 망 중립성 관련 시정청구 통계를 발표하였다.[274] 이러한 개선을 통해 위원회는 지침 이행 의지를 보여주었고 따라서 대부분의 트래픽 속도 제한이 빠르게 중단되었다.[275]

---

272) Michael Geist, "Net Neutrality Enforcement Put to the Test" (2011년 11월 8일), online: Michael Geist's Blog (http://www.michaelgeist.ca/) 참조.

273) CRTC의 서한은 CRTC 홈페이지에서 볼 수 있음 (http://www.crtc.gc.ca/eng/archive/2012/lt120120.htm); also Rita Trichur, "Rogers vows end to Internet 'throttling' in 2012", The Globe and Mail (2012년 2월 3일) online: The Globe and Mail (http://www.theglobeandmail.com/) 참조. 서한은 CRTC 홈페이지에서 볼 수 있음 (http://www.crtc.gc.ca/eng/archive/2012/lt120229.htm)]. Rogers의 발표에도 불구하고 위원회가 회사를 모니터하고 당해 회사가 이후 ITMP 규칙 위반을 확인했다는 서한을 보냈으며 새로운 트래픽 셰이핑 문제를 즉각적으로 해결할 것을 요청했다는 점은 주목할 만하다. [an electronic copy of the letter is available online: CRTC (http://www.crtc.gc.ca/eng/archive/2012/lt120229.htm)].

274) CRTC, "Status Report – Complaints Related to Internet Traffic Management Practices (ITMPs)", online:CRTC (http://www.crtc.gc.ca/eng/publications/reports/itmp-pgti.htm) 참조.

275) Michael Geist, "How the CRTC Helped to Put An End to Internet Throttling" (2012년 3월 2일); and Michael Geist, "Celebrating the Canadian Digital Policy Success Stories" (2013년 7월 1일) online: Michael Geist's Blog (http://www.michaelgeist.ca/) 참조.

6. 결 론

캐나다의 망 중립성 규제 제정은 규제정책 수립에 있어 대중의 역할이 얼마나 중요한지 보여주고 있다. 막강한 기존의 통신사, 정부 정책입안자, 규제 당국 모두 처음에는 망 중립성 문제를 일축했지만 시간이 지나면서 다양한 성격의 소비자단체, 기술기업 및 크리에이터 단체가 연합하면서 가속도가 붙었다. 이들 단체는 정책 절차를 통해 망 중립성을 정책 의제화 했으며 합리적인 트래픽 관리와 소비자 또는 경쟁에 해로운 영향을 미치는 영업행위간에 조심스럽게 균형을 이루는 규제적 접근방식의 문을 열었다.

새로운 인터넷 트래픽 관리 정책의 여파로 효과적인 시행이 주요 관심사가 되었다. 이는 망 중립성 문제가 해결되었다는 정계의 자기만족의 위험성과 함께 정책 및 시행간의 잠재적인 분리 가능성을 보여주고 있다. 캐나다의 사례는 정책 개발이 모든 참여자 특히, 규제 당국이 새롭게 개발된 규칙 및 규제 집행에 대해 경계를 게을리 해서는 안 되는 모든 절차의 첫 단계임을 보여주고 있다.

캐나다의 망 중립성 규칙 제정은 이중 인터넷 구조 또는 인터넷 트래픽 관리에 따른 경쟁약화에 대한 단순한 우려 그 이상의 것들이 포함되어 있음을 보여준다. 트래픽 관리의 프라이버시 침해 가능성은 정책 절차 내내 중요한 사안이 되었고 이는 심층패킷분석의 사용에 관한 세부적인 규칙을 명시하고 있는 최종 지침에도 반영되었다. 프라이버시와 망 중립성의 연계는 명확하게 드러나지는 않지만 캐나다 개인정보보호국, 기술 전문가들의 참여했기에 DPI와 같은 다목적 기술이 심각하게 프라이버시를 침해 가능성에 대해 캐나다 규제당국을 설득할 수 있었다. 규제 당국은 단순히 이러한 기술의 사용을 금지하는 대신에 온라인과 오프라인에서 모두 프라이버시를 보장하기 위한 엄격한 제한을 마련하였다.

캐나다의 사례는 망 중립성 규제와 관련해 모델이 될 수 있지만 정책적 한계가 있음을 명심해야 할 것이다. 특히, 정책은 잠재적 위반에 대해 완전한 조사를 실시할 수 있는 기술적 전문지식이 부족한 사용자의 시정청구에 달려 있기 때문에 시행의 문제점 역시 해결해야 할 사안이다. 또한 망 중립성 정책은 무선 인터넷 접근이 이제 막 싹트는 단계에서 수립되었다. 일부 이해당사자들이 유선 및 무선 인터넷 서비스를 모두 포함하는 포괄적인 정책 개발의 필요성을 언급하

고 있지만 무선의 평등성은 아직 완전한 시험을 거치지 못했다.

앞으로도 해결해야 할 문제들이 있겠지만 가장 논란이 되고 있는 인터넷관련 사안에 대해 합의를 이루어 낸 캐나다의 사례는 적극적인 시민단체의 참여와 근거 기반을 마련하고 어려운 정책 사안을 해결하고자 하는 규제당국의 의지가 얼마나 중요한지를 잘 보여주고 있다.

제3절 영국과 유럽의 망 중립성 및 통신비밀에 관한 법률, 실무, 연구의 현황과 전망

Chris Marsden[276]

1. 서 론

본 연구에서는 영국과 유럽의 망 중립성 및 통신비밀에 관한 입법, 시행, 연구 실태 및 전망에 대해서 살펴 볼 것이다. 먼저 망 중립성과 관련해 미국 및 유럽의 시행법을 살펴보고 2013년 9월로 예정된 유럽위원회(European Commission)가 준비 중인 관련법 개혁 전망을 분석해 보고자 한다. 이어서 본 연구의 핵심인 "합리적인 트래픽 관리"의 정의를 분석해 볼 것이다. 대부분의 법률제도는 현재 나타나고 있는 단기간의 트래픽 혼잡, 스팸 차단 및 보안, 법 시행을 이유로 ISP의 망 중립성 적용에 있어 예외를 허용하고 있다. 하지만 망 중립성과 관련해 심각한 프라이버시 침해와 관련해 논란이 있는 것도 사실이다. 따라서 위법적인 통신비밀 침해(유럽은 통신비밀 대신 '전자 프라이버시' 또는 e-프라이버시라는 용어를 사용)에 관한 기술 및 관련법을 자세히 살펴보고자 한다. 현재 2009 통신 지침(telecoms directives)[277]에 더해 유럽내 관련법으로는 프라이버시 지침(Privacy Directive 95/46/EC), 전자 프라이버시 지침(E-privacy Directive 95/46/EC)의 개정법인 데이터 보존에 관한 지침(2006/24/EC) 등이 있다. 다음으로 전자 프라이버시 및 망 중립성과 직접적으로 연관이 있는 통신개입에 대한 영국의 관련법을 살펴볼 것이다. 프라이버시 규제당국은 컨텐츠 차별에 개인 가

276) 제3절은 이 연구과제의 공동연구진인 Chris Marsden 교수가 집필하였다. Marsden 교수는 최근까지 Essex 대학교에 재직하다 올해 초 Sussex 대학 미디어법 교수로 임용되었으며 인터넷상의 규제에 관하여 다수의 연구성과를 발표한 바 있다. 최근에는 망 중립성을 인터넷 공간의 거버넌스 문제의 차원에서 접근하면서 각 이해관계 당사자들이 모두 참여할 수 있는 공동규제 시스템을 만드는 것이 가능한 해결책이 될 수 있을 것이라는 의견을 제시하였다.

277) 역주: 정식명칭은 "DIRECTIVE 2009/136/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL"이며 2009년 11월 25일 결정되었다.
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:en:PDF

입자의 데이터를 수집·분석하는 트래픽 관리가 포함된다고 결정했다.[278] 유럽 연합 기구가 2012-2013년 유럽의 망 중립성 및 전자 프라이버시 관련법의 개혁을 제안함에 따라 이에 대한 전망을 분석해 보고자 한다. 또한 영국의 온라인 광고 솔루션업체인 '폼(Phorm)'과 영국의 3대 인터넷 서비스 제공업체(ISP)인 British Telecommunications(BT)의 심층패킷분석을 사용한 온라인 맞춤형 광고(behavioral advertising)를 둘러싼 서비스 분쟁에 대해 자세히 살펴 볼 것이다. 다음으로 영국의 전자 프라이버시 법 시행에 따른 불합리한 사용자 보호에 대해 유럽 위원회가 법적 문제를 제기하자 2011-2012년 영국 전자 프라이버시와 개입법 개혁에 대해 살펴볼 것이다. 마지막으로 프라이버시와 통신 규제 기능에 대한 강력한 국내 및 국제적 협력이 부재한 상황에서 망 중립성 규제의 어려움에 대해 살펴보고자 한다.

2. 유럽연합 내 관련 규정 및 영국 국내법[279]

가. 망 중립성 논란

망중립 정책을 두고 논란이 거세지고 있다.[280] 인터넷 서비스 제공자(ISP)가 사용하는 트래픽 관리 기술은 인터넷 컨텐츠뿐만 아니라 이용자의 권리에도 영향을 미치고 있다. 예를 들면, 가입자에게 묶음 요금제로 음성서비스도 함께 제공하는 액세스 제공자는 해당 네트워크를 이용해야 하는 ISSP/ISP에서 제공하는 경쟁 음성 인터넷 프로토콜(Voice over Internet Protocol-VoIP, 이하 VOIP라 함) 서비스의 속도를 둔화시킬 수도 있다. 이러한 트래픽 속도 둔화는 망 중립성 침

278) 지침 95/46/EC of 24 October 1995, OJ L 281/31 (1995); 지침 2002/58/EC, OJ L 201/37(2002); 공공 통신 네트워크의 공공으로 이용할 수 잇는 전기통신 서비스 제공과 함께 생성하거나 처리한 데이터 보존에 관한 2006년 3월 15일 결정된 지침 2006/24/EC 및 개정된 지침 2002/58/EC OJ L105/54 (2006) 참조.

279) 역주: 이해를 위하여 원저자의 내용을 망 중립성 관련법, 및 위반사례로 임의로 나누었다.

280) Marsden, C. (2013)Network Neutrality: A Research Guide Chapter 16 in 'Handbook Of Internet Research', I. Brown, ed., Edward Elgar, at SSRN: http://ssrn.com/abstract=1853648 참조.

해의 한 형태로 볼 수 있다. 액세스 제공자가 망 중립성을 침해하여 이용자의 통신에 개입하고 그에 따라 '폼(Phorm)'과 Comcast의 사례와 같이 통신 개입의 위법성에 대한 형사처벌의 가능성이 매우 높다는 사실은 주지할 만하다(인터넷 서비스 제공자(ISP)는 문맥에 따라 다른 뜻으로 사용되기 때문에 유럽[281]과 미국[282]에서는 법률용어로 액세스 제공자가 더 널리 사용되고 있다. 일반적으로 책임제한은 모든 ISP에게 적용되며 이 중 일부는 액세스 제공자에게만 적용된다. 따라서 ISP와 액세스 제공자의 구별이 매우 중요한데 그 이유는 망 중립성은 액세스 제공자가 자신들이 소유하고 있는 네트워크에 QoS(quality of service, 서비스 품질)을 제공하는 방법 및 최종사용자의 네트워크 접근 속도 개선 및 둔화와 밀접한 관련이 있기 때문이다.

---

281) 유럽에서는 전기통신지침(Electronic Commerce Directive, ECD)에 따라 인터넷 액세스 제공자는 전기통신 네트워크 제공자(Electronic Communications Network Provider, ECNP)라고 하며 컨텐츠와 서비스 제공자는 정보사회 서비스 제공자(Information Society Service Provider, ISSP)라고 한다. 지침 2000/31/EC, Art 2(a) (OJ L 178/1, 17 July 2000), 지침 98/48/EC (OJ/L 217/18, 1998년 8월 5일 결정)의 제1(2)(a)와 부속서 따라 수정된 지침 98/34/EC (OJ L 204/37, 1998년 7월 21일 결정)의 제1조 제2항 참조. 시청각 미디어 서비스 제공(시청각 미디어 서비스 지침)(성문화 버전) OJ/L 95/1(2010년 4월 15일 결정)에 관한 회원국의 법, 규칙 또는 행정조치에서 명시하고 있는 일부 조항의 조율에 관한지침 2010/13/EU, 제1(a)(i) 및 Art 2(2010년 3월 10일 결정) 참조. 유럽체제 지침(2002/21/EC, OJ L 108/33), 제2(c)에서 규정하고 있는 '전기통신 서비스'는 방송에서 사용하는 네트워크의 통신 서비스 및 전송 서비스를 포함한 전기통신 네트워크를 통해 전달되는 모든 또는 주요 신호에 대한 이용료 징수를 허용하는 서비스를 뜻하며 서비스 제공 또는 기존의 전기통신 네트워크 및 서비스를 사용해 전송되는 컨텐츠에 대한 편집통제권은 제외한다. 이러한 용어에 대한 정의에는 명확히 전기통신 네트워크를 이용해 모든 또는 주요 신호를 전송하지 않는 ISSP는 제외된다.

282) 미국은 디지털 밀레니엄 저작권법(Digital Millennium COpyright Act, DMCA)에 따라 액세스 제공자는 인터넷 액세스 제공자(Internet Access Provider, IAP)dlau 서비스 제공자는 온라인 서비스 제공자(Online Service Provider, OSP)라 한다. 1976년 저작권법의 수정버전으로 1998년 디지털 밀레니엄 저작권법(DMCA)의 일부분으로 통과되었으며 Title 17, United States Code, Section 512(c)(2)를 신설해 '면책조항(safe harbor provision)'으로 언급되는 온라인 저작권 침해 책임제한법(Online Copyright Infringement Liability Limitation Act, OCILLA) 참조. 1998 디지털 밀레니엄 저작권법, s 512(k)(1)(A–B): '발신 도는 수신하는 컨텐츠를 수정하지 않고 사용자가 지정한 지점간 또는 사이에 디지털 온라인 통신을 위한 전송, 경로 또는 연결을 제공하는 자,' 또는 '온라인 서비스 도는 네트워크 액세스 제공자 또는 이러한 시설의 운영자.' 통신법 193447 §201(a) 및 (b) 의 Title I 및 Title II USC 참조.

규제와 감독의 부재로 인해 ISP는 일부 컨텐츠가 ISP, 저작권자, 정부 또는 자녀를 둔 부모의 이익에 부합되지 않는다고 판단하면 이러한 컨텐츠를 차단하기 위해 심층패킷분석(DPI)를 사용할 수 있었다. ISP는 현재 스팸메일 차단 목적으로 DPI를 널리 사용하고 있으며, 일부 국가에서는 위법한 포르노와 같은 콘텐츠 차단을 목적으로 한 합리적인 트래픽 관리의 적법성을 인정하고 있다.

1999년, 인스턴트 메시지 및 동영상 차단 가능성에 대한 우려가 제기되면서 처음으로 케이블 네트워크의 망 중립성에 대한 문제가 제기되었다.[283] 네트워크 중립성 즉, 망 중립성은 모든 ISP 사용자에게 동등하게 적용되기 때문에 경쟁법에서 명시하고 있는 시장지배력평가의 대상이 아니며 사실 이러한 시장지배력의 이용이 명확하게 네트워크의 중립을 침해하는 것으로 볼 수 없다.[284] 현실을 오도하는 광고가 넘쳐나고 ISP가 시장 지배력을 악용하고 있다는 사실에 대해 소비자가 인지하지 못하는 상황에서 이루어지고 있는 단말기 독점 즉, 시장독점을 위해 이러한 시장지배력을 이용해야 하는 것은 아니다.[285] 본 연구에서는 사용자의 통신 또는 개인정보에 대한 개입에 관한 입법, 그 중에서도 합리적인 트래픽 관리의 적법성 또는 위법성 평가의 어려움에 대해 살펴보고자 한다. 또한 사용자의 프라이버시 침해에 대한 국제법적 기준과 비교해 망 중립성 관련법을 분석할 것이다.

통신미디어 관리에 관한 논쟁 중 최근 가장 쟁점이 되고 있는 것이 네트워크 중립[286]이다. 인터넷은 확산형 구조로 인해 초기에는 많은 법률 전문가와 기술 전문가들의 관심의 대상이 되었다.[287] 망 중립을 미래지향적이며 긍정적인 요소

---

283) Lemley, MA and Lessig, L. (2000) The End of the end-to-end: preserving the architecture of the nternet in the broadband era, UC Berkeley Public Law Research Paper No 37 참조. further Marsden,C. (1999) Council of Europe MM-S-PL(1999)012: 'Pluralism in the multi-channel market 참조. Suggestions for regulatory scrutiny', at S.5.1: http://www.coe.int/t/dghl/standardsetting/media/Doc/MM-SPL(1999)012_en.asp

284) Marsden (2010) Net Neutrality: Towards a Co-regulatory Solution, Bloomsbury Academic: London at p 1.

285) 일부 학자는 우선처리는 서비스 품질 저하의 전제조건이므로 품질저하와 우선처리를 구별하는 것에 대해 의문을 제기한다. Filomena Chirico, Ilse Van der Haar and Pierre Larouche, 'Network Neutrality in the EU', TILEC Discussion Paper (2007), (http://ssrn.com/abstract=1018326) 참조

286) Marsden, supra n.6. 참조,

(또는 후퇴하는 부정적인 요소)로 봐야 할지에 대한 결정은 용어에 대한 정의를 내리고 사용량에 따른 서비스 이용료 지불 또는 동일한 이용료 지불 쉽게 말해, 정액제 또는 종량제라는 두 가지 형태의 문제를 이해하기 위한 첫걸음이라 할 수 있다.[288] 네트워크 액세스 차별은 주로 소비자 가정으로 직접 연결(last mile)된 전화나 케이블 시스템 등 하나 또는 둘 이상의 ISP가 시장지배력을 갖는 통신사의 독점문제로 특정 지을 수 있다. 이러한 상황에서 수직적으로 통합된 ISP는 경쟁사의 컨텐츠를 선택적으로 차별할 수 있다. 미국은 경제적인 관점에서 망 중립성에 반대하고 있으며 트래픽 사용량에 따른 종량제를 찬성하고 있다.[289] Hahn과 Wallsten은 '망 중립성[290]을 '광대역 서비스 제공자가 소비자에게 인터넷 접근에 대해서만 서비스 이용료를 부과할 수 있고, 컨텐츠 제공자를 차별할 수 없으며, 광대역 망을 통해 최종 사용자에게 전달되는 정보에 대해 컨텐츠 제공자에게 이용료를 부과 할 수 없는 시스템'으로 정의하고 있다.

망 중립성 원칙 입법에 있어 유럽은 다른 지역보다 뒤쳐져 있고 유럽위원회는 이와 관련한 세부적인 제도 마련을 유럽전자 통신규제기구(Body of European Regulators for Electronic Communications, BEREC)[291]에 위임하고 있다. 2012년 네덜란드와 슬로베니아 의회가 망 중립성을 입법한 이후 다음해인 2013년부터 유럽연합 내 관련법 입법에 가속도가 붙었다. 따라서 이하에서는 현재까지의 망 중립성 입법에 관한 법적 논쟁을 살펴보고자 한다.

ISP의 선택적 컨텐츠 차별 가능성은 되돌아보면 이미 1999년부터 문제가 제기

---

287) 인터넷은 익명의 네트워크 시스템이다. Haddadi, Hamed et al (2009) Analysis of the Internet's structural evolution, Technical Report Number 756 Computer Laboratory UCAM-CL-TR-756 ISSN 1476-2986 참조.

288) 실질적인 문제는 상호연결의 '중간지점(middle mile)' 있다고 저자는 주장한다. Marsden supra n.6 참조.

289) David, Paul (2001) 'The Evolving Accidental Information Super-Highway', 17(2) Oxford Review of Economic Policy pp 159–187 참조.

290) Hahn, Robert and Scott Wallsten, (2006) 'The Economics of Net Neutrality' AEI Brookings Joint Center for Regulatory Studies: Washington, DC at (www.aeibrookings. org/publications/abstract.php?pid=1067) 참조.

291) generally http://berec.europa.eu/eng/about_berec/working_groups/net_neutrality_expert_working_group_/282-net-neutrality-expert-working-group 참조.

되었고 이후 2003년 Tim Wu박사가 '망 중립성'이라는 용어를 처음으로 만들었다.[292] 2004년, 마이클 파월(Michael Powell) 당시 미 연방통신위원회(Federal Communications Commission, 이하 FCC라 함) 위원장은 "광대역 업계에 1) 컨텐츠에 접근할 자유, 2) 애플리케이션을 사용할 자유, 3) 개인용 기기를 연결해 사용할 자유, 4) 서비스 요금제 관련 정보에 대한 접근 자유 등 인터넷 자유를 준수할 것을 요구 한다[293]"고 발표했다. 앞의 '네 가지 자유'는 '인터넷에 관한 정책성명서(Internet Policy Statement)[294]' 및 Madison River[295], AT&T, Verizon의 합병승인 및 Comcast 사건에 적용되었다. 광대역 서비스와 음성전화 서비스를 수직적으로 통합한 Madison River의 사례는 경쟁사를 차별하고 경쟁사의 서비스 이용자의 인터넷 접속 속도를 둔화 시켜야할 이유를 명확하게 보여주고 있다. Madison River 사례는 망 중립성의 부정적인 측면을 그대로 보여주고 있다고 할 수 있다. 사용자는 ISP와 광대역 서비스 이용 계약을 했지만 ISP는 전화 서비스의 독점권을 유지하고자 서비스의 품질을 저하시켰다. 사실 Madison River는 소규모의 지역적 인터넷 서비스 제공자이지 전국에 네트워크를 갖고 있는 대형 통신사는 아니다. 대형 통신사인 AT&T와 BellSouth는 합병 당시 자신들이 가입자에게 전송되는 경쟁사의 컨텐츠를 차단하지 않겠다고 약속했다.[296] 2008년, 미 연방통신위원회(FCC)는 대형 케이블 네트워크사인 Comcast에 대해 시정명령을 내렸다.[297] Comcast는 FCC에 제출한 소명서를 통해 샌드바인(Sandvine) 기술을 이용해 2005년 5월부터 2006년까지 BitTorrent의 P2P 파일공유 애플리케이션의 속도를 선택적으로 제한한 사실을 인정했다. 이에 대해 FCC는 Comcast에 P2P 사용자 파악을 목적으로 한 DPI 기술 이용을 즉각적으로 중단할 것을 지시하였

292) Wu, T (2003) 'Network Neutrality, broadband discrimination', 2 Journal on Telecommunications and High-Tech Law 141.

293) Powell (2004) Four Freedoms speech, at (http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-243556A1.pdf).

294) FCC (2005) Internet Policy Statement 05-151.

295) FCC (2005) Madison River Communications, LLC, Order, DA 05-543, 20 FCC Rcd 4295

296) FCC (2007) In AT&T Inc and BellSouth Corp Application for Transfer of Control, 22 FCC Rcd 5562.

297) FCC (2008) Memorandum Opinion and Order, 23 FCC Rcd 13028 ('ComcastOrder').

다.[298]

미국 경제회복 및 재투자법(American Recovery and Reinvestment Act)은 광대역 망을 서비스가 제공되지 않는 지역까지 확대하기 위한 광대역 오픈 액세스 촉진[299]에 관한 조항 및 오픈 액세스와 망 중립성 조항을 포함하고 있다.[300] FCC는 2010 Order[301]를 채택했는데 이에 대해 법원에 소가 제기되었다. 2011년부터 2013년까지 FCC는 상호접속(interconnection)과 대등접속(peering)이 망 중립성 원칙을 위배하는 불합리한 트래픽 속도 제한이라는 컨텐츠 전송 네트워크(Content delivery network, CDN)의 주장에 대해 여러 차례에 걸쳐 개입 불가 의사를 밝혔으며 현재 이 사건은 법원에서 심리가 진행 중이다.[302] 합리적인 트래픽 관리를 평가하기 위하여 자기규제(self-regulatory) 단체인 광대역 네트워크 산업 기술자문 그룹(Broadband Industry Technical Advisory Group, BITAG)가 기술적인 방법을 이용하고 있다. 이 단체의 주요 역할은 공식적인 기술 자문을 포함해 트래픽 관리에 관한 '세이프 하버(Safe Harbor)'[303] 적용과 관련해 의견을 제공하는 것이다.[304]

---

298) Karpinski, R, Comcast's Congestion Catch22, 23 January 2009, at <http://telephonyonline.com/residential_services/news/comcast-congestion-0123/index1.html> 참조.

299) American Recovery and Reinvestment Act 2009, at Division B, Title VII, Section 6001(k)2, A, D, E.

300) FCC (2009) Report on a Rural Broadband Strategy, 22 May 2009, at pp 15–17 especially footnotes 62–63 참조.

301) FCC (2010) Report and Order Preserving the Open Internet, 25 FCC Rcd 17905.

302) Frieden, Rob (2012) Rationales for and Against Regulatory Involvement in Resolving Internet Interconnection Disputes 14 Yale J.L. & Tech 266 at: http://yjolt.org/sites/default/files/FriedenFinal.pdf

303) 역주: 1995년 유럽연합이 개인정보보호지침을 제정하면서 당해 지침에 따라 '적합한(adequate)' 수준의 개인정보보호 조치가 이루어지고 있음을 확인한 경우에만 유럽경제지역(European Economic Area) 역외 제3국으로의 개인정보 이전을 허용함에 따라 특정 분야에 한정해 법을 시행하고 자율규제를 적용하고 있는 미국이 EU 기준을 충족하기 위하여 세이프하버 협정을 체결하였다. 이에 관한 자세한 내용은, 미 상무성에서 발행한 "Safe Harbor Privacy Principles" 참조.

304) Broadband Industry Technical Advisory Group (2011) By-laws of Broadband Industry Technical Advisory Group S. 7.1

나. 유럽의 망 중립성 관련법 및 규칙

유럽연합은 2009년 선거 통신법(2009 Election Communication Framework)을 통해 ISP의 트래픽 관리의 투명성을 의무화하고 있고 자발적으로 최소한의 서비스 품질을 보장하도록 하고 있다. 28개 유럽경제지역(European Economic Area) 회원국과 47개 유럽평의회 회원국은 인권 및 기본적 자유의 보호에 관한 유럽협약(Convention for the Protection of Human Rights and Fundamental Freedoms)의 제8조 사생활 및 가족생활을 존중받을 권리[305], 제10조 사용자의 표현의 자유를 준수하여야 한다. 이에 더해 유럽연합은 현행 데이터정보 관련법으로 이를 보충하고 있으며 관련법은 각국 법원 및 유럽재판소[306]의 판단의 근거가 되며 유럽연합 프라이버시 위원회(European Union privacy commissioners)[307]의 권고안을 고려한다. ISP의 위법행위와 특히, '최고 속도, 합리적인 사용'이라며 소비자를 오도하는 내용의 광고에 대한 소비자의 분노가 계속되자 2007년부터 2008년까지 미국, 영국, 캐나다, 노르웨이의 규제 개혁안의 양도 함께 증가하였다. 사실 ISP가 말하는 '합리적인 사용'이라함은 월 단위의 용량 제한, 모바일의 경우 총 100MB의 느린 다운속도를 의미한다.[308] 특히 ISP가 싫어하는 컨텐츠에 대한 차별 또는 ISP와 관련이 있는 컨텐츠에 대한 특혜에 대해 우려가 제기되었다.[309]

---

305) Koops, Bert-Jaap and Sluijs, Jasper P. (2012) Network Neutrality and Privacy According to Art. 8 ECHR, European Journal of Law and Technology 2(3); at http://dx.doi.org/10.2139/ssrn.1920734; Sluijs, Jasper P. (2012) From Competition to Freedom of Expression: Introducing Art. 10 ECHR in the European Network Neutrality Debate, Human Rights Law Review 12(3) at http://dx.doi.org/10.2139/ssrn.1927814 참조.

306) Case C-461/10: Bonnier Audio AB and others v Perfect Communication Sweden AB, OJ C 317, 20/11/2010 P. 0024.0024 final judgment 19 April 2012 at http://curia.europa.eu/juris/document/document.jsf?doclang=EN&text=&pageIndex=0&mode=DOC&docid=121743&cid=848081 참조.

307) Marsden C. [2012] Regulating Intermediary Liability and Network Neutrality, Chapter 15, pp701-750 in 'Telecommunications Law and Regulation' (Oxford, 4th edition)

308) Leading to a significant emphasis in SEC(2007) 1472 Commission Staff Working Document: Impact Assessment at 90.102.

309) Jasper P Sluijs, Florian Schuett and Bastian Henze, Transparency regulation in broadband markets: Lessons from experimental research, (2011) 35 Telecommunications Policy 592.602

유럽연합은 2002 전기통신서비스(Electronic Communications Services, ECS) 종합법을 개정한 2009년 개정안에 따라 전문규제청(National regulatory authority, 이하 NRS라 함)이 ISP의 서비스 품질을 규제하도록 하고 있다[310]. 유럽위원회는 2002 지침[311]의 검토 이유로 미국의 논쟁을 언급했다. 2009년 5월, 입법안이 유럽의회에 상정되었을 때 망 중립성을 가장 중요하게 다루었다. 소비자 투명성 및 네트워크 개방에 대한 개정안은 전자통신 네트워크 및 관련 시설에 대한 개입 등에 관한 지침 2009/140/EC[312]에 첨부한 유럽위원회의 정책선언의 형태로 이루어진 '망 중립성 선언'[313]에 따라 조정절차로 유럽의회에 상정되었다. 지침의 내용은 다음과 같다.

"위원회는 인터넷의 개방성과 중립성 유지를 매우 중요하게 생각하며, 망 중립성을 NRS(기본지침 제8조(4)(g)[314])가 증진해 나가야 할 정책 목표이자 규제원칙으로 포함시켜야 한다는 입법자들의 의지, 이와 관련한 투명성 강화[315] 및 서비스 품질 저하 및 공공네트워크 내 트래픽 속도 제한을 방지하기 위한 NRA의 감독권한 부여 등을 충분히 고려했다(보편적 서비스 지침(universal service directive) 제22조(3))[316]."

---

for an experimental analysis of transparency regulation in broadband 참조.

310) 지침 2009/140/EC (OJ L 337/37 18 December 2009); 지침 2009/136/EC (OJ L 337/11 18 December 2009) 참조.

311) COM (2006) 334 Review of the EU Regulatory Framework for electronic communications networks and services, Brussels, 29 June 2006 at section 6.2.6.4.

312) 역주: 자세한 내용은 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0037:0069:EN:PDF 참조.

313) European Commission (2009) Declaration on Net Neutrality, appended to Directive 2009/140/EC, O J L 337/37 at p 69, 18 December 2009 at (http://eurlex. europa.eu/LexUriServ/LexUriServdo?uri=OJ:L:2009:337:0037:0069:EN:PDF)

314) 역주: 조항의 원문 내용은 다음과 같다.
Article 8(4)(g) FD: explicitly recognizes that NRAs should promote the interests of the citizens by, inter alia, "promoting the ability of end-users to access and distribute information or run applications and services of their choice" (Article 8(4)(g) Framework Directive).

315) Articles 20(1)(b) and 21(3)(c) and (d) Universal Service Directive

316) 보편적 서비스 지침 제22조(3)는 규제당국이 최소한의 서비스 품질 기준을 수립할 수 있어야 한다고 명시하고 있다. '서비스 품질 저하, 네트워크 내 트래픽 속도 제한 또는 둔화를 방지하기 위해

2011년 5월 발효[317]된 법에 따르면, 직접(접속 차단 또는 속도 제한 행위) 또는 간접(ISP와 제휴를 맺은 컨텐츠에 대해서만 서비스 속도를 높이는 행위)적으로 특정한 컨텐츠가 차별 받지 않도록 회원국이 관련 조치를 취해야 한다고 명시하고 있다. 위원회는 '연례 중간보고서에 유럽시민의 '망 자유(net freedom)'를 보장하기 위한 방법'을 유럽 의회와 이사회에 상정'하겠다고 밝혔다. 지침의 법률조항은 일부 주요 서비스제공자가 아닌 모든 서비스 제공자에 대한 더욱 확대된 '균형 잡힌(symmetric)' 규제를 허용하고 있다. 이는 회원국 간의 시설 및 서비스 상호 이용에 관한 논쟁을 해결을 위한 근거로 향후 활용할 수 있을 것이다.

위의 선언을 비롯해 보다 법률적인 내용을 담고 있는 지침은 국가 차원에서의 이행 및 위원회의 자발적인 사전 감독, 각국 법원, 가입자 정보를 수집하는 트래픽 관리 실무를 포함하고 있으며 지침 이행의 성패는 컨텐츠 차별을 규제하는 프라이버시 규제당국에 달려 있다 할 것이다. 인권 및 기본적 자유의 보호에 관한 유럽협약(Convention for the Protection of Human Rights and Fundamental Freedoms) 제8조와 제10조제2항에 부합하는 트래픽 관리는 제한적으로만 적용할 수 있으며 정보통신위원회와 통신규제 당국에서 이를 규제 하여야 한다.[318] 경쟁정책이 아닌 소비자 정보보호 및 프라이버시 규제에 따라 유럽 연합법에 망 중립성에 관한 조항이 삽입되었다. 유럽데이터보호감시국(European Data Protection Supervisor)은 최근 망 중립성과 관련해 문제로 제기되고 있는 프라이버시 침해 가능성에 대해 의견을 표명하였다.[319] 비비안 레딩 EU집행위원회 부위원장은 새로운 통신법에 대한 투표에 앞서 다음과 같이 말했다.[320]

"새로운 규칙은 명백하고 분명하게 인터넷 접근을 표현의 자유 및 정보접근의

회원국은 전문규제청(NRA)에 최소한의 서비스 품질 요건 수립 권한을 부여해야 한다.'

317) 2009년 11월 25일 결정된 지침 2009/136/EC(the 'Citizens Rights Directive') 및 지침 2009/140/EC(the 'Better Regulation Directive')는 반드시 18개월 내에 시행하여야 한다.

318) BoR (10) 42 at p 20.

319) European Data Protection Supervisor (2011) Opinion on net neutrality, traffic management and the protection of privacy and personal data, at <http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinion s/2011/11-10-07_Net_neutrality_EN.pdf>

320) Reding (2009 undated).

자유와 같은 기본권으로 보고 있다. 따라서 규칙은 서비스 및 애플리케이션에 대한 접근 또는 사용에 관한 어떠한 조치도 프라이버시권, 표현의 자유, 정보접근의 자유, 교육을 받을 권리 및 공정한 재판을 받을 권리를 포함해 자연인의 기본권리 및 자유로서 반드시 준수되어야 한다."

유럽의회는 시민의 프라이버시 및 표현의 자유와 관련해 회원국에게 연성법을 발표했다.[321]

다. 합리적인 네트워크 관리 및 규제에 관한 논의

ISP의 트래픽 관리와 관련해 '합리적(reasonable)'이라는 용어는 미국 FCC 인터넷 정책성명서(FCC Internet Policy Statement)[322] 주석 15에 처음으로 등장하였다. 이는 네트워크 관리의 목적이 합리적이며 이러한 네트워크 관리를 최소한으로 제한하고 있음을 ISP가 스스로 입증하도록 하고 있는데, '합리적'이라는 표현은 사실 언론의 자유에 대한 미국 법원의 접근 방법에서 차용되었다. 따라서 ISP는 '네트워크 관리가 국익을 위해 매우 중요하며 좁게는 이러한 이익에 부합하기 위함임을' 입증해야 한다.[323] FCC는 이러한 원칙을 확대해 2009년 예외사항을 규정했는데 그 내용은 다음과 같다.

"ISP는 스팸, 서비스 공격 차단, 위법한 컨텐츠 차단 및 기타 위해한 인터넷 활동 방지를 위한 조치뿐만 아니라 속도 향상을 위한 캐싱(catching), 애플리케이션 중립적인 광대역 할당 등 모든 소비자에게 합당한 서비스 제공을 위해 일반적으로 허용되는 기술을 이용할 수 있다."[324] 다시 말해, ISP는 제3자의 온라

---

321) 2010년 9월 29일 채택된 망 중립성에 관한 각료회의 선언 참조. 제1094차 각료회의에서 망 중립성 규칙 적용에 관한 대한 회원국의 이행을 위한 연성법 채택: 유럽인권협약 제6조, 제8조, 제10조

322) 20 FCC Rcd 14986 (2005) ("Internet Policy Statement")

323) Free Press와 Public Knowledge Against Comcast Corp가 비공개로 이루어지는 P2P 애플리케이션 속도 제한에 대해 이전에 제기한 불만, Free Press의 청구에 대한 인터넷 애플리케이션에 대한 속도 제한이 FCC의 인터넷 정책성명서를 위반하고 '합리적인 네트워크 관리'의 예외에 해당되지 않는다는 선언적 판결, 의견서 및 명령 FCC Rcd 13028(2008년 8월 20일 발표)("Comcast Order"), p. p47.

324) Broadband Initiatives Program; Broadband Technology Opportunities Program Notice, 74 Fed. Reg. 33104, 33110.11 (July 9, 2009) (Broadband NOFA).

인 맞춤형 광고를 차단하기 위해 이러한 기술을 사용할 수 있지만 영국에서 있었던 BT와 PHORM사의 사건처럼 온라인 맞춤형 광고제공 목적으로 이러한 기술을 사용하여서는 안 된다. 통신 서비스 거부(Denial of Service, 이하 DoS라 함)는 트래픽 혼잡을 야기하는 트래픽 폭주를 이용해 웹사이트에 피해를 가하는 기술이다.

FCC는 동축 케이블, 기존의 구리선을 이용하는 통신시스템, 광섬유 케이블 광대역, 무선 시스템 간에는 분명 기술적 차이가 있음을 인정하면서도 모든 중요하지 않은 트래픽 관리를 금지하고자 하는 이유를 분명히 밝혔다. FCC는 "선택적 차별과 관련해 합리적인 네트워크 관리 및 상세한 예외사항을 명시하고 있는 명확한 규칙이 불분명한 규칙보다 인터넷의 특성에 훨씬 부합된다고 생각한다"고 밝혔다. 하지만 이는 "불필요하게 제한적인(unnecessarily restrictive)"이라고 묘사한 2005년의 '좁은 해석(narrowly drawn)' 및 '매우 중요한(critically important)'이라는 표현보다는 덜 명확하다.

그렇다면 '일반적으로 허용되는 기술 조치'에 해당하지 않는 '위해한 활동(harmful activities)'이 무엇인지에 대한 의문이 제기된다. 일반적으로 사용하는 특정 조치에 대해 업계가 합의를 하게 된다는 점을 고려할 때 시간이 지나면서 위해한 활동의 범위는 변할 수밖에 없다. 위해한 활동이라 함은 네트워크의 건전성 및 특정 조치에 따라 그 의미가 결정되며, 그 일예로 통신 서비스 거부(DoS)를 들 수 있다. 따라서 ISP의 DoS의 차단을 위한 개입이 적법하게 될 것이다(비록 이러한 활동은 시간이 지나면서 변하게 된다. 2003년 다이얼 방식에서 백만 명이 한꺼번에 접속하면서 ISP 서비스가 마비가 되었지만 10년이 지난 현재 광대역망에서는 한꺼번에 접속한다해서 폭주로 인해 서비스가 마비되지는 않는다). 마이클 코프(Michael Copps) EU집행위원회 위원은 "네트워크 속도가 768Kbps였던 때와 50 또는 100Mbps 때의 합리적인 네트워크 관리는 상당히 다를 수밖에 없다"고 하였다.[325]

2009년 캐나다 규제당국 역시 합리적인 트래픽 관리에 대해 정의하면서 "ISP는 입증된 차별에 대해 사례별로 이러한 차별이 합리적이었음을 반드시 입증해

325) Copps, Michael, quoted in FCC (2009) 09-93 at pp.94-95.

야 한다"고 설명하였다. "이러한 컨텐츠 차별, 특혜 또는 불이익이 불공정하거나, 부당하거나 또는 불합리하지 않음을 밝힐 입증 책임은 전적으로 ISP에 있다."[326] 캐나다 규제당국은 데이터 상한제로 알려져 있는 사용량에 따른 요금제(usage based billing) 즉, 종량제를 허용하고 있는데 그 이유는, 이러한 요금제가 타당하며 사용자의 선호에 따라 트래픽을 차별하기 때문이다.[327] 2009년부터 2012년까지 요금 종량제, MMORPG, 게임에 대해 147건의 소비자 불만이 접수되었고 당시 캐나다 방송통신위원회 위원장 대행은 "대형 ISP인 Bell과 Rogers가..... 마침내 2012년 말까지 트래픽 속도 제한을 중단하겠다고 발표했다. 두 회사는 네트워크 용량 확대를 위한 신규 투자가 트래픽 관리를 하지 않도록 하는데 도움이 될 것이라고 했다"고 발표했다. 게임 사이트와 같이 과도한 트래픽 발생의 원인의 되는 사이트에 대한 트래픽 속도 제한은 분명 불합리하다. 2013년 방송통신위원회는 많은 문제를 일으켰던 Bell과 Rogers가 더 이상 문제를 발생시키지 않기 위해 실질적으로 용량을 확대하는 등 위원회의 결정을 완전히 이행하고 있는지 또는 앞으로 추가적으로 이를 시행할지 등에 대해서는 함구하고 있다.

유럽 전자통신 규제기구(Body of European Regulators for Electronic Communications, 이하 BEREC라 함)은 '합리적'이라는 의미에 대해 분석하고 다음의 결론을 내렸다.

"트래픽 혼잡 시간대에 예를 들면, 시간에 민감한 애플리케이션을 원활히 이용할 수 있도록 하기 위해 P2P 애플리케이션의 속도를 선택적으로 제한하는 것은 합리적이다. 선택적 속도 제한에 따른 부작용이 적다는 점을 고려할 때 특정 애플리케이션을 모두 차단하는 것보다 훨씬 합리적이라 할 수 있다."[328] 2010년

---

326) 캐나다 방송통신위원회(CRTC, 2009) Review of the Internet traffic management practices of Internet service providers, Telecom Regulatory Policy CRTC 2009-657, File No.8646-C12-200815400 (최종접속일: 2009년 10월 21일), available at http://crtc.gc.ca/eng/archive/2009/2009-657.htm

327) CRTC (2011) Telecom Decision CRTC 2011-44, Ottawa, 25 January 2011: Usage-based billing for Gateway Access Services and third-party Internet access services, File number: 8661-C12-201015975

328) BEREC (2012) Differentiation practices and related competition issues in the scope of net

9월 30일, 유럽 집행위원회는 망 중립성 시행에 관한 논의를 종결하였다.[329] BEREC는 2010년 9월 유럽집해위원회의 논의에 대한 답변을 발표하였다. BEREC는 무선 네트워크 역시 망 중립성 위반 사항에 대해 명시하고 있는 망 중립성 조항의 규제대상이 되어야 한다는 결론을 내렸다.

"유선과 무선 네트워크의 망 중립성에 대해 다른 접근 방식을 취해야 할 이유에 대해서는 충분한 논의가 이루어지지 않았다. 특히 망 중립성과 관련해 향후 접근방식은 네트워크 형태를 구별해서는 안 된다."[330] 2011년 12월, BEREC는 서비스의 투명성과 품질에 대한 가이드라인[331]을 발표하였다. 투명성과 관련해 BEREC는 '단일방식으로는 충분치 않다'[332]고 밝히면서 NRA의 한계에 대해 지적했다. 소비자 단체와 정보위원회 기구 역시 중요한 역할을 해야 한다.

2009년 지침에 따라 NRA에 부여된 권한은 회원국마다 큰 차이가 나며 2012년 말까지 망 중립성과 관련해 입법을 한 국가는 핀란드, 네덜란드, 슬로베니아 등 3개 회원국에 그쳤다. 2012년 관련법을 입법한 네덜란드와 슬로베니아는 몇 가지 예외사항을 제외하고는 트래픽 관리를 금지하고 있다.[333] 네덜란드의 망 중립성 법은 다음과 같이 명시하고 있다.

a) 트래픽 혼잡을 최소화하는데 있어 동일한 형태의 트래픽은 동일하게 취급하여야 하고,

---

neutrality, BoR (12) 132 at p.56 paragraph 265.

329) (http://ec.europa.eu/information_society/policy/ecomm/library/public_consult/net_neutrality/index_en.htm)

330) BoR (10) 42 BEREC Response to the European Commission's consultation on the open Internet and net neutrality in Europe, p3 at (http://www.erg.eu.int/doc/berec/bor_10_42.pdf).

331) Documents BoR 53(11) Quality of Service and BoR 67(11) Transparency, at (http://erg.eu.int/documents/berec_docs/index_en.htm)참조.

332) BoR 67 [11] at p 5 참조.

333) 네덜란드 통신법 제7조(4)(a) 및 슬로베니아 전기통신법 No. 003-02-10/2012-32 제203조에 대한 비공식 번역. 네덜란드 통신법은 네덜란드 정부에서 번역한 것임. http://www.government.nl/files/documents-and-publications/notes/2012/06/07/dutchtelecommunications-act/tel-com-act-en-versie-nieuw.pdf (not official legal translation) 참조. 슬로베니아 통신법은 No. 003-02-10/2012-32, 20 December 2012, http://www.uradnilist.si/1/content?id=111442 Helpful translation of key aspects at https://wlansi.net/en/blog/2013/06/16/net-neutrality-in-slovenia/ 참조.

b) 서비스 제공자 또는 사용자의 단말기에 있어 네트워크의 완전성 및 보안을 유지하고,
c) 스팸을 차단하며 법적 의무를 이행한다.[334]

슬로베니아 법은 다음과 같이 명시하고 있다.

1. 인터넷 네트워크의 원활한 사용을 위해 필요한 기술적 조치(예를 들면, 트래픽 혼잡 방지)를 취하며,
2. 네트워크의 완전성 및 보안 유지를 위해 필요한 사전예방 조치를 시행하고,
3. 이에 더해 스팸을 차단하고 법적 의무를 이행한다.

슬로베니아의 망 중립성 관련법은 이러한 트래픽 관리를 "필요한 범위에 한해, 합당하고, 차별 없이 제한된 시간 동안"만 문제를 해결하기 위해 제한된 범위 내에서만 사용하도록 하고 있다. 네덜란드와 슬로베니아 모두 모바일 제공자 등 특정한 제공자에 대한 인터넷 트래픽 제한을 명백히 금지하고 있는데 이와 관련해 네덜란드는 "ISP는 모바일 서비스를 통해 제공되거나 또는 사용되는 서비스 및 애플리케이션에 따라 인터넷 접속 서비스의 사용료를 부과해서는 안 된다"고 명시하고 있다. 유럽연합의 망 중립성 규제안 역시 '합리적' 의미에 대해 이와 비슷한 설명을 하고 있다.

2013년 9월 11일, 집행위원회는 망 중립성 조항에 실질적으로 영향을 미칠 수 있는 전문을 채택했고 '특별한 서비스'의 우선처리를 허용하면서 ISP의 제3자가 제공하는 컨텐츠의 선택적 차단 또는 속도제한을 금지하였다.[335] 이러한 내용을 주 골자로 하는 법안은 2013년 7월 작성된 초안과 비교해 망 중립성을 보다 포괄적으로 다루고 있으며 내용 중 일부는 망 중립성 정책 시행에 있어 동시에 긍

334) 네덜란드 규제당국은 2013년 여름까지 망 중립성 관련법을 시행하지 않았으며 관련 부처가 규제당국이 당해버의 이행을 위해 필요한 제2차 입법 및 규칙을 발표할 수 있도록 하기 위해 시행일이 연기되었다. 따라서 네덜란드 법의 시행에 대한 결론을 내리는 것은 시기상조이다.

335) COM(2013) 627 final 2013/0309 (COD) Proposal for a Regulation laying down measures concerning the European single market for electronic communications and to achieve a Connected Continent 참조.

정적인 영향과 부정적인 영향을 미치고 있다. 망 중립성 시행에 대해 명시하고 있는 제23조(5)는 네덜란드와 슬로베니아 법과 맥락을 같이하고 있는데, "데이터 용량 또는 인터넷 접속 속도에 대해 합의된 허용치 내에서 인터넷 서비스 제공자는 합리적 트래픽 관리가 필요한 경우를 제외하고 특정 컨텐츠, 애플리케이션, 또는 서비스를 선택적으로 차단하거나 트래픽 속도 둔화, 차별의 방법으로 전항에서 명시하고 있는 자유를 제한하여서는 안 된다"고 명시하고 있다. 또한 동법은 "투명성, 비차별성, 필요성이라 함은 a) 법 또는 법원의 명령 이행, 심각한 범죄의 방지 또는 차단, b) 네트워크를 통해 소비자의 단말기에 전달되는 네트워크의 완전성 및 보안 유지, c) 사전에 광고 차단 조치에 동의한 인터넷 사용자에게 직접 마케팅을 목적으로 한 원치 않는 통신의 전송 방지 및 d) 일시적 또는 예외적으로 발생하는 트래픽 폭주로 인한 트래픽 혼잡을 애플리케이션을 차별하지 않는 방법으로 완화하기 위한 조치로 정의하고 있다." 또한 "합리적인 트래픽 관리는 동 조항에서 명시하고 있는 목적을 위해 필요하고 적합한 데이터 처리만을 의미한다"고 명시하고 있다. 제21조부터 제24조는 불합리하게 차별을 하는 제공자를 바꿀 수 있는 사용자의 계약상의 구제방법에 대해서도 명시하고 있다.

모든 통신사에 대해 허가제를 실시하고 있고 망 중립성은 물리적으로 사용할 수 있는 용량에 의해 결정되기 때문에 용량을 업그레이드 한다 할지라도 특별서비스는 제한된 시간동안에만 제공될 수 있다.[336] 정보처리 상호운용의 가능성 요구는 ISP의 애플리케이션 차단의 근거가 된다.[337] 특히, ISP의 소비자의 인지부족 악용 및 맞춤형 광고 제공이 만연한 상황에서 ISP의 시장 점유율과 단말기 독점만으로는 남용의 충분한 근거가 되지 않는다.[338] 2009년 지침은 주요 ISP뿐

336) GN Docket No 09-191 Broadband Industry Practices WC Docket No 07-52 'In the Matter of Further Inquiry into Two Under-Developed Issues in the Open Internet Proceeding Preserving the Open Internet', 그리고 Andersen et al, Joint Reply Comments Of Various Advocates For The Open Internet, 4 November 2010, Comments on Advancing Open Internet Policy Through Analysis Distinguishing Open Internet from Specialized Network Services. 참조.

337) Marsden (2010) Net Neutrality, at p 1 참조.

338) 일부 학자는 우선처리는 서비스 품질 저하의 전제조건이므로 품질저하와 우선처리를 구별하는 것에 대해 의문을 제기한다. Filomena Chirico, Ilse Van der Haar and Pierre Larouche, 'Network

만 아니라 모든 서비스 제공자에 대한 '일관된' 규칙 적용을 허용하고 있다. 제5조 제1항은 NRA는 최종 사용자가 ISP 서비스를 상호 이용할 수 있도록 하는 의무를 ISP에 부과할 수 있다고 명시하고 있다. 유럽 통신기본지침 제20조는 ISP와 컨텐츠 제공자 간의 분쟁해결에 대해 명시하고 있다. 투명성 의무에 기초한 잠재적인 분쟁은 이러한 의무를 이행하는데 있어 '확실한 위협(credible threat)'이 될 수 있는데 그 이유는 위반행위가 보편적 서비스 지침 제22조 제3항에 따라 최소한의 품질 요건의 시행을 촉발할 수 있기 때문이다.

라. 통신 차단을 위한 기술 도입

ISP가 트래픽을 관리해야 할 이유는 많으며 다음과 같이 요약할 수 있다.

1. 네트워크 제공자는 네트워크 혼잡 시간대에 사용자가 네트워크를 과도하게 사용하는 것을 막기 위해 특별한 서비스를 채택하고 있으며 비디오 파일과 같이 용량을 많이 필요로 하는 컨텐츠 소유자에게 별도의 요금을 부과하고 있다.
2. 네트워크 제공자는 이미 스팸과 같이 명확한 형태의 원치 않는 상업적 통신을 걸러내기 위한 필터를 제공하고 있다.
3. 네트워크 제공자는 인터넷에서 이루어지는 잠재적인 테러 활동을 추적하기 위해 국가정보국과 협력하고 있다.
4. 네트워크 제공자는 스카이프 등 암호화되지 않은 인터넷 전화(VoIP)를 추적할 수 있다.
5. 법집행 및 보안을 위해 필요하다.[339]

이렇듯 상황이 변화면서 네트워크 제공자는 파일 전송을 차단하거나 대용량

Neutrality in the EU', TILEC Discussion Paper (2007), (http://ssrn.com/abstract=1018326) 참조.

339) generally Bendrath (2009) 'Deep Packet Inspection Reading List', at http://bendrath.blogspot.com/2009/03/deep-packet-inspection-reading-list-and.html and the Syracuse DPI project papers at http://dpi.ischool.syr.edu/Papers.html 참조.

파일 전송에 대해 사용자에게 전송비를 부과할 수 있게 되었다. 이처럼 인터넷에서 특정 컨텐츠를 다른 컨텐츠에서 분리하는 것을 '자사의 폐쇄망(walled garden)'이라고 부른다. ISP는 이른바 '블랙박스'를 이용해 패킷과 컨텐츠를 검사하고 있으며 점차 규제와 관련해 심각한 문제를 야기하는 심층패킷분석(DPI)를 사용하고 있다.

유럽연합 회원국의 경우 국내법으로 반드시 이행해야 하는 유럽연합의 네트워크 및 정보보안으로 인해 비용이 발생한다. 이미 스팸 필터 및 과도한 트래픽을 유발해 서비스 장애를 일으키는 서비스 거부(distributed denial of service, DDOS) 공격, 피싱, 기타 '맬웨어'를 차단에 많은 비용이 소요되고 있는 것이 사실이다. 점차 정보 인프라의 중요한 구성요소인 광대역망에 대한 의존이 확대되고 인터넷이 일반화되면서 보안의 중요성이 커지고 있다. 또한 점차 범죄가 복잡해지고 고도화되면서 문제가 더욱 심각해지고 있다. 인터넷에서 프라이버시 침해, 개방성, 연결성 역시 보안에 있어 잠재적인 위험요소가 되고 있다.

ISP는 혼잡 시간대에 또는 데이터 사용량을 제한하는 요금제를 이용해 사용자의 통신접속을 차단해 트래픽 속도를 제한하거나 아니면 전송하는 데이터가 P2P인지를 확인하기 위해 패킷을 검사하는 방법으로 컨텐츠를 확인할 수 있다. 현재 정부는 DPI 설비 구입을 위한 보조금을 ISP에 제공하고 패킷을 감시하도록 독려하고 있을 뿐만 아니라 이러한 패킷검사가 유럽과 영국의 사생활보호법을 위반하기 때문에 매우 위험한 영업행위가 된다(영국의 경우 스파이 활동을 방지하기 위한 목적으로 DPI를 허용하고 있다). 이 분야의 저명한 학자인 Felten은 예를 들면, BitTorrent는 회사가 아닌 프로토콜이며 차별적으로 취급을 받는다는 점을 고려할 때 규제당국으로 하여금 기관 및 기업의 기준을 마련하도록 하는 점에 대해 우려의 목소리를 내고 있다.[340] 프로토콜 설계자들이 암호화 또는 다른 기술을 이용해 다른 방법을 찾을 것이기 때문에 결국 BitTorrent나 P2P의 차단은 실패하게 될 것이다.

340) http://www.freedom-to-tinker.com/blog/felten/comcast-and-bittorrent-why-you-cant-negotiate-protocol 참조.

마. 심층패킷분석(DPI) 및 트래픽 차단 규제

차단을 포함해 여러 가지 형태의 트래픽 셰이핑은 현재의 네트워크 관리 툴을 살펴보았을 때 매우 노골적인 툴이기 때문에 많은 논란을 불러일으키고 있다. 예를 들면, 일정한 프로토콜을 사용하는 P2P 트래픽을 선택적으로 차단할 수 있다. 차단을 피해가기 위해 P2P는 암호화하거나 다른 파일인 것처럼 위장할 수 있는데 위반자를 찾기 위한 보안 소프트웨어 간의 경쟁 즉, '무기 경쟁'을 촉발할 수 있다. 또한 네트워크는 P2P를 보다 효율적으로 차단하기 위해 노력할 것이기 때문에 또 다시 P2P 컨텐츠 암호를 위한 소프트웨어와 DPI를 이용해 P2P 트래픽 찾고자 하는 ISP간의 무기 경쟁으로 이어지게 될 것이다.[341]

ISP의 컨텐츠를 전달하는 '단순한 통로'로서의 역할에는 책임이 제한되지만 불법 컨텐츠에 대한 실질적인 인지에 있어서는 책임이 제한되지 않는다. 이러한 이유로 인해 ISP의 트래픽은 마치 판도라의 상자와 같다. 즉, DPI를 이용해 ISP가 패킷을 조사한다면 아동포르노에서부터 저작권 침해 및 프라이버시 침해에 대한 모든 법적책임이 ISP에 있게 된다. 캐나다 개인정보 보호국(Office of the Privacy Commissioner of Canada)이 트래픽 관리와 관련해 방송통신위원회에 제출한 의견서는 이에 대한 심각성을 보여주고 있다. "DPI는 인터넷을 통해 전달되는 메시지의 내용을 조사할 수 있다. 쉽게 말하자면 DPI 사용은 우편배달부가 수신자에게 우편물을 배달하기 전에 우편물의 봉투를 열어 내용물을 확인하는 것과 같다. 컨텐츠 조사가 네트워크 관리를 위해 필요한지는 명확하지 않으며 이는 개인의 프라이버시를 불합리하게 침해할 소지가 있다."[342]

Cooper는 ISP 네트워크에 DPI 설비를 도입을 포함해 용량을 확장하는 대신 할 수 있는 트래픽 제한과 광대역망을 확대하지 않고 DPI 및 기타 트래픽 관리 서버에 대한 투자를 분석하였다. 그는 미국의 통신사는 2005년 인터넷 정책 성

341) 2009년 5월, uTorrent는 UDP에 대한 프로토콜 교체 계획을 발표하였는데 이는 TCP가 주요한 P2P 트래픽 프로토콜이 아니며, TCP를 이용한 유투브 접속을 방해하고, ISP에 문제를 야기할 수 있으며 차별이 심화될 것으로 예상된다. UDP 필터링이 많은 ISP 고객에서 있어 출발점이 되기 때문에 서로 더 강력한 무기를 갖추려고 하는 이른바 '무기경쟁'이 계속되게 된다.

342) http://www.theregister.co.uk/2008/12/01/richard_bennett_utorrent_udp/ 참조.

명서가 발표될 당시 ISP가 합리적으로 영업하고 있다는 가정 하에 기술이 합리적으로 사용되고 있지 않음을 입증할 입증 책임이 소비자에 있기를 희망했다고 지적했다. 하지만 미국과 캐나다 모두 인터넷 서비스 제공자에게 입증책임이 있다. 즉, ISP가 DPI와 같은 기술사용이 합리적인지 입증해야 하고 Comcast는 회사가 샌드바인(Sandvine)사에서 개발한 DPI 설비를 합리적으로 사용하고 있음을 입증하지 못하였다. 미국의 ISP는 Comcast 사례를 통해 알 수 있는 봐와 같이 DPI의 사용이 합리적이지 않은 것으로 보고 있다. Cooper는 마케팅 담당자가 여전히 DPI 기술의 사용을 장려하고 소비자에 대한 온라인 맞춤형 서비스 제공을 위해 이러한 기술사용에 따른 비용을 승인한다 할지라도 규제당국이 DPI 기술사용을 사용하지 못하도록 한다면 결국 기술사용의 효율성이 떨어져 기술을 사용하지 않게 될 것이라고 주장한다..[343] ISP와 규제당국의 입장 차이에 대해 더 많은 연구가 이루어져야 하겠지만 ISP 마케팅 부서의 데이터보호법 및 트래픽 개입의 위법성에 대한 지식과 교육 부족이 ISP가 고객의 컨텐츠를 분석하고 조사하기 위해 DPI를 설치하도록 하는 원인이 될 수도 있다. 이와 반대로, Cooper의 연구를 통해 알 수 있는 바와 같이 대부분의 엔지니어들은 상세한 트래픽 관리보다 광대역망 확대를 지지한다.

또한 Cooper의 연구에서 주목할 점은 외국의 컨텐츠 제공자는 국내 ISP의 트래픽 관리에 영향을 미칠 수 없다는 것인데 따라서 World of Warcraft와 같은 대규모 다중사용자 온라인 롤 플레잉 게임(Massively Multiplayer Online Role Playing Game, MMORPG) 제공자는 ISP의 불합리한 트래픽 관리로 인해 종종 서비스를 제대로 제공할 수 없게 되며 이는 미국보다 DPI 및 기타 트래픽 관리 기술이 보다 광범위하게 사용되는 영국에서 문제가 심각하다.[344] Cooper의 이러한 연구결과는 무료로 MMORPG 게임을 이용하는 한국의 많은 게이머들에게는

343) Cooper, Alissa (2013) How Regulation and Competition Influence Discrimination in Broadband Traffic Management: A Comparative Study of Net Neutrality in the United States and the United Kingdom, Thesis submitted for the degree of DPhil, University of Oxford, September 2013. PP.122-132. Cooper interviewed 70 elite decision-makers in ISPs, regulators and content companies in the period 2011-12, the broadest sample known.

344) Cooper 2013: 200-204

좋지 않은 소식인데 그 이유는 MMORPG 설계자들이 외국의 ISP가 트래픽 속도를 제한하는 것에 대해 불만을 제기하고 이러한 문제를 바로 잡을 수 있을 가능성이 희박하기 때문이다.

Cooper는 각국 규제당국의 법적 소송 및 강제 집행에 대한 견해에 따라 '합리적' 트래픽 관리의 의미가 결정되고 관련법이 해석된다고 주장한다. 따라서 미국의 규제당국은 법적 소송이나 법의 집행을 두려워하지 않으며 위반 사례를 보다 엄격히 고발하지만 영국의 규제당국은 집행보다는 다른 대안을 찾고자 하며 마지막 수단으로 소를 제기할 것이라고 주장했다. 영국의 규제당국인 정보위원회(Information Commissioner)은 폼(PHORM)사와 BT의 불법적인 DPI 사용이 불거졌을 때에도 이들에 대해 소를 제기할 의지가 없어보였다. 반면 미국의 규제당국인 연방통상위원회(Federal Trade Commission)는 2012년 8월 가입자의 개인정보를 이용한 구글과 페이스북 등 합의사항을 위반한 소셜 네트워크에 수백만 달러의 벌금을 부과했다.[345] 구글의 사례와 관련해 통상위원회는 "연방통상위원회의 합의 명령에 따라 회사는 가입자의 정보에 담겨있는 프라이버시 보호를 위해 종합적인 프라이버시 프로그램을 시행해야 한다. 또한 위원회가 미국과 영국의 세이프 하버협약[346]에 의거한 프라이버시 요건을 실질적으로 침해한 것으로 본 것은 이번이 처음이다"라고 판시하였다.[347]

망 중립성 위반 및 기타 ISP 사용자들의 신뢰를 저버리는 행위에 대한 민·형사소송의 가능성은 실제로 규제를 집행하고자 하는 규제당국의 의지에 달려있다 할 수 있다. 미국은 초기부터 소송으로 대응했지만 영국은 그렇지 않았다. 이론적으로 취약한 미국은 자국의 개인정보보호 규칙이 지침 95/46/EC에 의거한 유럽의 개인정보호법을 충족할 수 있음을 확신시켜야 하는 상황이지만 실질적으로

345) CLardinois Frederic (2012) Facebook And FTC Settle Privacy Charges – No Fine, But 20 Years Of Privacy Audits, Tech Crunch, August 10th, http://techcrunch.com/2012/08/10/facebook-ftc-settlement-12/

346) 면책조항의 프라이버시 보호원칙에 따른 보호의 적절성에 관한 유럽의회와 위원회 지침 95/46/EC에 의거한 집행위원회 결정 2000/520EC(2000년 7월 26일) 및 미국 연방통상위원회의 Official Journal of the European Communities(L-215, 7-47, 2000년 8월 5일)에서 제기한 질문 참조. www.export.gov/safeharbor 참조.

347) 본 보고서 작성이 끝날 때 쯤하여 FTC와 FCC 웹사이트는 미국 정부가 폐쇄했기 때문에 사용되지 않고 있었다.

미국은 영국보다 법적 대응에 있어 더욱 적극적이다. 2013년 스노든 사건이 발생하면서 미국 기업은 기업 정책을 이유로 스스로 세이프 하버 협약을 위반하고 있고 사법집행기관의 요구 및 첩보활동이라는 명목 하에 유럽과 한국을 포함해 몇몇 국가의 국민의 개인정보를 감시하고 있다. 비록 늦은 감이 있지만 2013년 개인정보 감시는 '세이프 하버 협약' 및 유럽 개인정보보호 규제안의 검토에 있어 중요한 사안이 되었다.[348]

바. 2014년 유럽데이터보호규제안과 지금도 진행 중인 스노든 사건

유럽의 망 중립성 관련법은 시민의 프라이버시와 자유의 보호를 목적으로 한다. 지침 95/46/EC[349]는 기업의 위법한 행위로부터 시민의 정보를 보호할 권리 및 책임을 회원국에 부여하는 법적 근거가 되고 있다. 유럽연합법은 데이터 보호에 있어 엄격한 기준을 적용하고 있으며 미국과 비교해 훨씬 엄격하다 할 수 있다. 국가데이터보호국은 상임 합동실무그룹(Working Group 제29조)를 두고 있으며 가능한 동일한 수준에서 지침을 시행해야 하며 보호국은 지속적인 규제 개발을 위한 유럽집행위원회 및 타 기관과 투명하게 공조하고, 높은 수준으로 개인정보 및 프라이버시를 보호하고, 공공통신 네트워크의 완전성 및 보안을 유지할 수 있도록 최선을 다해야 한다.[350] 유럽기관은 관련법에 의거해 2002년 설립된 유럽데이터보호감시국(European Data Protection Supervisor)의 입법안에 대해 의견을 제출해야 한다. 지침 2002/58/EC('Electronic Privacy Directive')[351]는 2004 스팸 통신[352]을 보충하는 스팸차단을 위한 조치를 포함한다.[353] 지침 2002/58/EC와 1995/46/EC는 지침이 없었다면 침해될 가능성이 있는 가입자의

348) European Commission (2012) Consultation on the Commission's comprehensive approach on personal data protection in the European Union",http://www.netcompetition.org/antitrust/ftc-googleprivacy-settlement-takeaways#sthash.TvMNpXvP.dpuf 참조.

349) 지침 95/46/EC.

350) 지침 2002/21/EC.

351) 지침 2002/58/EC.

352) 위원회 의사결정 및 이사회의 결의안은 유럽연합의 법이 아니며 회원국에 대해서 구속력을 갖고 있지는 않지만 회원국 및 관련 기업에 대한 '신호탄'이 되는 등 이른바 '연성법'의 역할을 한다.

353) COM/2004/0028.

프라이버시를 보호 하도록 하는 가입계약을 선택할 수 있도록 하고 민감한 데이터는 승인을 받거나 익명으로 제공되는 경우를 제외하고 제3자에게 이전하지 못하도록 하는 내용을 주요 골자로 하고 있다.

새로운 유럽의 통합 데이터 보호법에 따라 지침 2002/58/EC가 정비 될 것이며 새로운 법이 통과되면 지침 1995/46/EC는 폐지될 것이다. 2014년 3월 유럽의회는 전체 투표를 위해 총회를 열 예정이다.[354] 위원회와 각국의 전문가로 구성된 각료회의는 현재 당해 사안을 검토하고 있으며 법은 수천 개에 달하는 수정조항으로 인해 매우 복잡해질 것으로 예상된다.[355] 규제초안(COM/12/11)은 특히 유럽연합 외 지역으로의 데이터 전송에 관한 Section 42-43을 포함하고 있으며 데이터보호국의 사법집행의 대상이 되는 전송에 대한 기업 규칙(Binding Corporate Rules, BCR)을 포함하고 있다.[356]

일명 '5개의 눈(five eyes)'라고 불리는 다국적 스파이 연합[357]이 ISP 사용자들을 불법적으로 감시했던 일이 세상에 알려지자 유럽규제당국은 망 중립원칙 위반과 같은 잠재적인 개입 가능성을 조사했다. 국가가 이들의 활동에 필요한 재원을 지원했다할지라도 망 중립성에 있어 사용자의 이익에 반하는 행위를 한 ISP를 포함해 인터넷 기업의 협조를 받았다는 점은 주지할만한 하다. 유럽, 라틴아메리카 및 기타 국가에서 적법 또는 위법하게 이루어진 개인정보 수집은 에드

---

354) 동 사안에 대한 상황변화는 2012/0011(COD), http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2012/0011(COD)#tab-0

355) 유럽 의회 위원회의 진행상황은 http://www.europarl.europa.eu/RegistreWeb/search/simple.htm?language=EN&reference=LIBE%2F7%2F08739&relName=DOSSIER&currentPage=2 참조

356) COM (2012) 11 final Draft Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). COM/2012/09 final Safeguarding Privacy in a Connected World: A European Data Protection Framework for the 21st Century. IP/12/46 (2012) Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses, 2012년 1월 25일 at http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en

357) Campbell, Duncan (1999) The state of the art in communications Intelligence (COMINT) of automated processing for intelligence purposes of intercepted broadband multi-language leased or common carrier systems, and its applicability to COMINT targetting and selection, including speech recognition European Parliament Ref.: EP/IV/B/STOA/98/1401

워드 스노든이 2013년 가디언지를 통해 폭로하면서 세상에 알려졌다.[358] '5개의 눈(또는 공식적으로 AUSCANNZUKUS)'은 이러한 정보수집 활동을 영어사용권에서는 미국연합 대 바르샤바조약의 대결로 불리는 냉전시기에 있었던 앵글로색슨의 정보보국간의 협력으로 설명했다.[359] 미국, 영국, 캐나다. 호주, 뉴질랜드, 기존 협력국 및 기타 동맹국은 일정한 수준의 정보공유 협력을 체결하였다.[360] 연방수사국(FBI)가 이메일과 전자통신을 감시하기 위해 사용한 시스템인 'Carnivore'와 같은 패킷 스니핑 계획은 최소 1997년부터 시작되었고 Carnivore는 감시 표적이 되는 사용자의 모든 인터넷 트래픽을 감시하기 위해 맞춤형 패킷 스니퍼(packet sniffer)를 이용하였다.[361] 이보다 규모가 큰 감시시스템으로는 이른바 'Echelon'이 있는데 이 시스템은 몇몇 서방국가 만든 것으로 2001년 9월 5일 유럽의회는 이에 대한 조사 보고서를 발표하였다.[362] 국가안보국 기술보조원이었던 에드워드 스노든이 제공한 내용을 통해 밝혀진 바와 같이 정보기관의 감시활동은 점차 확대되고 있다.[363] Echelon은 이후 미국 프로그램

358) Bowden, Caspar (2013) The US National Security Agency (NSA) surveillance programmes (PRISM) and Foreign Intelligence Surveillance Act (FISA) activities and their impact on EU citizens' fundamental rights, European Parliament Civil Liberties Committee, 24.9.2013.

359) Richelson, Jeffrey T., Ball, Desmond (1985) The Ties That Bind: Intelligence Cooperation Between the UKUSA Countries. London: Allen & Unwin. ISBN 0-04-327092-1.

360) The initial formal UK-US agreement was signed in 1947 after the successful conclusion of the Second World war and just prior to the outbreak of the Korean War of 1950-53, with final partner New Zealand joining only in 1980. See AUSCANNZUKUS (2013 undated) History, at http://www.auscannzukus.net/history.html

361) 프라이빗 패킷 감청의 법적측면에 대해서는 Frieden, Rob (2007) Internet Packet Sniffing and its Impact on the Network Neutrality Debate and the Balance of Power between Intellectual Property Creators and Consumers, Available at SSRN: http://ssrn.com/abstract=995273 or http://dx.doi.org/10.2139/ssrn.995273 참조.

362) European Parliament (2001) Final Report on the Existence of a Global System for the Interception of Private and Commercial Communications (ECHELON Interception System), Temporary Committee on the ECHELON Interception System, 2001년 9월 5일 승인, Brussels: EP, at http://www.fas.org/irp/program/process/rapport_echelon_en.pdf

363) Borger, Julian (2013) Inquiry into snooping laws as committee clears GCHQ Intelligence and security committee also confirms GCHQ's use of NSA Prism surveillance material for first time, 18 July 2013 at http://www.theguardian.com/world/2013/jul/17/prism-nsa-gchq-reviewframework-surveillance 참조.

프리즘(PRISM)[364]으로 바뀌었고 2011년 영국과 미국은 템포라(Tempora · 라틴어 '시간'의 복수)라고 불리는 공동작전을 통해 대서양을 연결하는 광섬유 케이블을 이용해 오고가는 모든 통신을 감청했다[365]. 템포라는 "글로벌 텔레콤 개발(Global Telecoms Exploitation)" 및 "인터넷 관리운용(Mastering the Internet)"이라는 서브프로그램과 함께 사용되었다. 미국과 영국의 데이터보호 법은 공공 및 민간의 기술전문 단체로부터 즉각적으로 공격을 받았고 이후 스노든의 폭로에 대해 영국 의회 위원회 중 하나로서 중앙부처 산하 정보기관의 대외활동(지출 · 행정 · 정책)을 감독하는 정보보안위원회(Intelligence and Security Committee)는 다음과 같이 설명했다. "비록 감청기관인 정보통신본부(GCHQ)가 감청 및 개인정보에 관한 국내법을 위반하거나 위반을 시도한 적은 없었지만 정보보호법과 인권법, 조사권한규제법(Regulation of Investigatory Powers Act)과 이를 위반하는 위법적인 정책 및 절차에 대해 면밀히 검토하고 있다. 또한 통신감청감독처(tInterception of Communications Commissioner)도 이 사안을 검토하고 있다."[366]

언론을 통해 영국정부는 정보통신본부가 어떠한 위법활동도 하지 않았다고 발표했지만 부총리가 이끄는 진상위원회의 조사가 올해 하반기에 시작될 예정이다.

이전 유럽의회의 조사 결과를 뒷받침하는 스노든의 폭로 이후 위법적인 ISP 트래픽 감청에 대해 형법 위반이라는 내용의 불만이 제기되면서 유럽인권재판소, 각국 의회 및 정보위원회의 관심이 집중되었다고 한다.[367] 대부분 국가의 감청관련 국내법은 외국정보국을 비롯해 제3자에 의한 감청 허용을 금지하고 있다. Brown은 '5개의 눈'의 동맹국을 포함해 일부 국가의 관련법을 요약했다.[368]

---

364) Government code name for a data-collection effort known officially by the SIGAD US-984XN 참조.

365) Shubber, Kadhim. "A simple guide to GCHQ's internet surveillance programme Tempora". Wired.com, 24 June 2013 at http://www.wired.co.uk/news/archive/2013-06/24/gchq-tempora-101 참조.

366) Intelligence And Security Committee Of Parliament (undated July 2013) Statement on GCHQ's Alleged Interception of Communications under the US PRISM Programme, paragraphs 6-7.

367) Brown Ian (2013a) Expert Witness Statement for Big Brother Watch and Others Re: Large-Scale Internet Surveillance by the UK Application No: 58170/13 to the European Court of Human Rights. Available September 27 at SSRN: http://ssrn.com/abstract=2336609

비(非)유럽연합 회원국에 의한 유럽연합 시민의 개인정보 수집은 1995년과 2002년 법 및 새롭게 상정된 법안에 따라 유럽법의 심판 대상이 된다는 점은 주지할만하다.[369] 유럽의회, 영국, 네덜란드, 벨기에, 프랑스, 독일, 룩셈부르크 등 유럽연합회원국의 조사를 포함해 내년에는 유럽지역 전역에서 이루어진 인터넷 사용자의 트래픽 감청에 대한 면밀한 조사가 이루어질 예정이다. 이번 조사는 해외에서 이루어지는 스파이활동을 중점을 다루게 되겠지만 감청에 사용된 기술에 대해 보다 자세한 조사 결과가 나오게 되면 '5개의 눈'을 대신해 ISP가 사용한 기술의 형법 위반 여부에 대해 관심이 집중되게 될 것이다.

이러한 형태의 감청만으로는 망 중립성 위반요건에 해당되지는 않지만 정부 명령에 따라 이루어졌고 사법집행기관과도 관련이 되어 있을 수 있다는 점을 고려해 이러한 행위가 위법하다는 것이 입증되면 이는 위법한 목적을 위해 사용자의 개인정보를 감청한 것에 해당한다 할 수 있다. 규제당국은 ISP 및 관련자들에게 외국의 정보기관에 정보를 제공하지 말라는 내용의 지침을 내려야 할 필요가 있다. 극단적인 경우, ISP에 미국 및 영국에 기반을 두고 있는 ISP와 상호연결하지 못하도록 하는 상황이 발생할 수 도 있을 수 있다. 2014년 4월, 브라질의 호세프 대통령은 인터넷 거버넌스와 패킷 감청을 논의하기 위한 국제회의를 제안했다.[370] 감청에 대한 문제는 2011년 런던회의와 2012년 부다페스트 회의에 이어 2013년 서울 사이버스페이스 총회[371]에서도 논의될 예정이다.

경제협력개발기구(OECD)는 최근 프라이버시 가이드라인의 개정본을 발표하였고 인터넷 정책에 사용자의 기본권 보호를 포함시켜야 할 필요성을 명시하였다.[372] 사용자의 기본권 존중에 관한 선언이 이루어진 2011년 파리회의에서 한

368) Brown Ian (2013b) Lawful Interception Capability Requirements, in Computers and Law, at http://www.scl.org/site.aspx?i=ed32980

369) Rauhofer, Judith and Caspar Bowden (2013) Protecting Their Own: Fundamental Rights Implications for EU Data Sovereignty in the Cloud, Edinburgh School of Law Research Paper No. 2013/28: Available at SSRN: http://ssrn.com/abstract=2283175 or http://dx.doi.org/10.2139/ssrn.2283175

370) Agence France-Presse 보도(2013년 10월 9일, 17:31) Brazil to host Internet governance summit next year

371) http://www.seoulcyber2013.kr/en/program/speakers_4.html 참조

국대표는 OECD 회원국이 망 중립성을 위해 보다 활발한 연구가 이루어져야 하며 정책 조율의 필요성에 더 많은 관심을 기울여 줄 것을 요청하였다.

사. 전자 프라이버시 관련 영국의 통신감청의 위법성

감청법에 따라 ISP는 자신들이 소유한 네트워크에 대해 적법한 방법으로 통신감청을 하려고 시도하고 있다. 하지만 이들 ISP는 다른 기관을 대신한 감청이나 자신들의 목적을 위한 감청권을 제3자에게 허용하지 않을 것이다. 영국법은 이와 관련해 명확하게 명시하고 있다. 통신감청은 조사권한규제법 Section 2(2)의 적용대상이 되며 동법은 다음과 같이 명시하고 있다.

본 법의 목적 및 아래의 조항에 따라 다음 각호에서 명시한 행위를 한 자는 통신시스템을 이용해 통신과정에서 통신을 감청한 것으로 간주한다.

통신이 전송되는 동안 통신의 수신자 또는 발신자 외에 제3자에게 통신내용의 모두 또는 일부를 볼 수 있도록 하기 위한

a) 시스템 또는 시스템 운영을 변경 또는 개입하는 행위
b) 시스템을 이용한 통신을 감시하는 행위, 또는
c) 시스템을 구성하는 장치에서 수신 또는 발신하는 무선 전신을 통해 이루어지는 전송을 감시하는 행위는 감청으로 간주한다.

감청은 통신 수신자 또는 발신자 외에 제3자에게 통신내용의 일부 또는 전부

372) OECD (2013) Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (2013) [C(80)58/FINAL, as amended on 11 July 2013 by C(2013)79] at http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf. See also OECD (2007) Recommendation on Cross-Border Co-operation in the Enforcement of Laws Protecting Privacy; OECD (2008) The Seoul Declaration for the Future of the Internet Economy; OECD (2011) Recommendation on Principles for Internet Policy Making at http://www.oecd.org/internet/ieconomy/49258588.pdf. OECD (2013) also referred to European law and the Asia Pacific Economic Cooperation's Cross-Border Privacy Rules System (APEC CBPR).

에 대한 지득 및 공독을 구성요건으로 하고 있다. 통신 내용의 일부를 ISP 또는 제3자가 볼 수 있게 된다면 이는 다시 말해 수신자나 발신자 외에 제3자가 볼 수 있다는 것을 의미한다. 영국법은 엄격하게 적용되며 감청은 발신자와 수신자의 사전 동의를 받은 경우에만 할 수 있다.

온라인 광고 솔루션업체인 '폼(Phorm)'사가 영국의 3대 인터넷 서비스 제공업체(ISP)인 BT, Talk-Talk, 버진 미디어(Virgin Media)[373] 그룹 등과 제휴를 맺어 온라인 맞춤 광고 제공을 목적으로 시범 서비스를 실시한 사실이 밝혀지면서 사용자의 사전 동의 없이 이루어지는 네트워크 소유자에 의한 통신 내용 감시가 논란을 불러 일으켰다. 폼사는 BT를 포함해 ISP가 구글보다 효율적으로 타겟 사용자에게 온라인 맞춤 광고를 제공할 수 있도록 하기 위해 사용자들의 웹서핑 기록을 추적하였다. 이러한 기술은 미국의 무선 ISP가 처음으로 개발하였다.[374] 폼사는 ISP와 웹사이트 고객에게 보다 정확한 사용자의 서핑 기록을 제공하고 이러한 기록을 기반으로 더욱 근접한 타겟 광고를 제공할 수 있도록 하기 위해 웹와이즈(WebWise)라고 불리는 온라인 맞춤형 광고 시스템을 운영했다.

폼사는 ISP 가입자에게 맞춤형 광고를 제공하고자 이들의 웹서핑 기록을 복사하기 위해 DPI 기술을 이용하였다. 이미 2006년과 2007년 BT는 사용자의 사전 동의 없이 2차례에 걸쳐 폼의 Web wise 시스템에 대한 모의 테스트를 실시하였다.[375] 전자통신 감청을 담당하는 정부부처는 이러한 사실을 알고 도움이 될 만한 시범운영 및 온라인 맞춤형 광고 제공에 대한 규제 지침을 BT에 제공하였다. 2007년 8월, 폼사가 담당부처에 연락을 하였을 때 담당부처는 'DPI 사용을 허용하면 당사의 현 사용자와 잠재 사용자의 편의가 향상될 것으로 생각하는가?'[376] 라는 질문으로 답변한 사실이 2009년 4월에 밝혀졌다. 이를 통해 폼사와 담당부처간의 협의가 광범위하게 이루어졌고 비록 감청이라는 점에 대해서는 의문이

373) http://www.theregister.co.uk/2009/04/22/virgin_media_phorm_nma/

374) http://energycommerce.house.gov/cmte_mtgs/110-ti-hrg.071708.DeepPacket.shtml

375) Dubious value is given to such permission in BT internal documents, see http://wikileaks.org/wiki/British_Telecom_Phorm_PageSense_External_Validation_report

376) BBC (2009) Home Office 'colluded with Phorm', 28 April at http://news.bbc.co.uk/2/hi/technology/8021661.stm

있지만, 만약 이것이 '감청'에 해당되고 ISP 이용약관에 사용자가 동의하였다면 이는 Section 3에 의거해 합법적인 활동이 된다는 점에 대해서는 귀하와 의견을 같이 한다'는 내용을 통해 합의가 이루어진 것으로 볼 수 있다. 2008년 1월 22일 내무성 담당자가 폼사에 보낸 이메일에는 '함께 첨부한 문서를 확인하시고 귀하의 의견을 알려주시기 바랍니다'라고 쓰여 있다. 이메일 기록과 내용이 발표되면서 2009년 상원은 이와 관련한 사안에 대해 논의하였다. 당시, 바로니스 밀러(Baroness Miller) 상원의원은, "내무성이 담당기업에게 조사권한규제법의 해석이 맞고 당해 회사의 행위가 실제로 법 적용 대상이 아닌 것이 맞는지를 묻는 것 자체가 정말 어처구니없는 일이다"라고 하였다.[377]

2008년 초, 사용자를 대상으로 실시한 시범운영에 대해 법적논란이 일자 문제가 된 ISP와 폼사는 향후 있을 수 있는 시범운영 및 기술의 사용 공지 및 동의를 이용약관에 삽입하겠다는데 합의하였고 BT는 2008년 세 번째 시범운영을 실시하였다. 법적으로 보았을 때, 웹서핑 기록 추적시스템은 1995 유럽연합 프라이버시 법 및 2002년 지침에서 요하는 허가에 위배될 뿐만 아니라 영국 조사권한규제법에 따라 위법한 감청에 해당된다. 2008년 3월, 정보정책연구재단(Foundation for Information Policy Research, FIPR)은 폼사의 시스템은 조사권한규제법을 위반하는 위법한 감청이라는 내용의 서한을 정보권한 책임자에게 보냈다.[378] 인터넷 서비스 제공자의 온라인 맞춤형 광고에 대해 접수된 불만 사항은 영국 정보보호위원회(Information. Commissioner Office, ICO)가 담당하는데 위원회는 개인정보 보호 권한 및 위법한 통신 감청에 대해 조사를 실시할 수 있는 수사권을 갖고 있다. 하지만 위원회의 힘이 약하기 때문에 위법성에 대해서는 수사를 하지 못하고 과태료만을 부과했다. 위원회는 2006-2007년 이루어진 BT의 시범운영이 '구체적인' 위법행위에 해당된다고 판단하였고 2008년 이루어진 시범운영과 관련해 회사가 제출한 설명서에 대해 강한 의구심을 표명하였지만 이후 어떠한 조치도 취하지 않았다.

---

377) LINX Public Affairs (2009) https://publicaffairs.linx.net/news/?p=993

378) FIPR (2008) Continuing concerns about Phorm, 6 April at http://www.fipr.org/press/080406phorm.html

캠브리지대학의 보안 전문가 Clayton은 기술 정확성을 위해 폼사가 사용한 시스템에 대한 연구보고서를 제출했다.[379] 그는 "자세한 사항을 조사해 보니 초기에 내렸던 판단이 옳음을 확인하였다. 웹사이트 데이터를 감청한 것이다. 국내법은 감청을 금지하고 있다"고 했다. 직접적으로 데이터보호법을 위반했을 뿐만 아니라 시스템이 인터넷 트래픽을 감청했다는 사실만으로도 명백한 위법이다. BT는 사전에 사용자뿐만 아니라 자신들이 감청한 웹사이트 운영자, 웹기반 메일, 포럼 또는 기타 소셜네트워크 사이트를 통해 사용자와 통신하는 제3자에게 사전에 동의를 받을 경우에만 감청이 적법하다는 사실을 간과하고 있는 듯하다.

정보보호위원회가 시범운영에 대해 사전 동의를 구하지 않음으로써 지침을 위반한 사실에 대해 폼사와 BT를 기소하지 못하자 이에 대한 시민들의 불만이 커지자 유럽집행위원회는 영국 정부에 조치를 취하지 않은 이유에 대해 소명할 것을 요청하였다. 유럽집행위원회는 지침 2002/21/EC 전자 프라이버시 지침(EPD)[380]에 따라 회원국의 유럽연합법 이행을 감독한다. 1995년 유럽 데이터보호 지침(Data Protection Directive)은 EPD[381]에 명시된 바와 같이 충분한 정보를 제공받은 후에 사용자들이 자유의지에 따라 동의해야 한다고 명시하고 있다. EPD와 DPD의 주요 내용은 가입자가 자유롭게 개인의 프라이버시를 침해하지 않는 가입계약을 선택할 수 있으며 민감한 데이터는 승인을 받거나 익명으로 제공되는 경우를 제외하고 제3자에게 이전하지 못하도록 하는 것이다[382]. DPD 제24조에 따라 회원국은 침해가 발생하는 경우 이에 대한 적절한 제재조치를 수립해야 한다. 제28조는 감독을 위한 독립감독기관의 운영을 규정하고 있다. DPD 조항은 통신비밀에도 적용된다.

---

379) Clayton, R. (2008) The Phorm\Webwise System, at http://www.cl.cam.ac.uk/~rnc1/080404phorm.pdf and later version http://www.cl.cam.ac.uk/~rnc1/080518-phorm.pdf

380) The Electronic Privacy Directive supplemented by the 2004 Communication on unsolicited commercial communications ('spam') COM(2004)0028.

381) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data: Article 2(h)

382) 지침 2002/58/EC on Privacy and Electronic Communications: Article 5(1) http://www.theregister.co.uk/2009/02/11/ phorm_eu_action_threat/104 See Press Release IP/09/570.

영국이 제출한 답변이 만족스럽지 않자 집행위원회는 더욱 강력한 어조로 보다 자세한 설명을 요구하였다. 두 번째 답변도 별 다른 내용이 없자 위원회는 2009년 1월 법적 조치[383]를 취하고 2009년 4월 영국을 상대로 침해와 관련해 소송을 제기하였다.[384](IP/09/570) 비비안 레딩(Viviane Reding) EU 집행위원장은 "국내법을 개정할 것을 영국정부에 요구한다. 관련법 개정을 통해 영국은 이번 폼사의 사례에서 제기된 바와 같이 전자 프라이버시 및 개인정보 보호 등 새로운 문제에 더욱 적극적으로 대처할 수 있을 것"이라고 밝혔다.

2009년 10월 집행위원회는 유럽연합법에 따라 관련법이 제대로 이행되고 있지 않다고 판단하고 다음의 세 가지 부문에 대해 영국당국에 국내법을 개정할 것을 요청하였다.

- EPD 및 DPD에 따라 통신감청을 감독하고 특히, 통신감청에 대해 불만이 제기되었을 경우 이를 판단할 독립기관의 부재
- 현행 영국법은 인터넷 사용자가 감청에 동의한 경우뿐만 아니라 자신의 정보가 감청되는 당사자가 조사권한규제법 2000(Regulation of Investigatory Powers Act 2000, RIPA)에 따라 자유의지로 감청에 동의했다고 '믿을만한 근거"가 있는 경우 감청을 허용하고 있다. 하지만 영국의 국내법은 EPD 이전에 입법되었다. 따라서 동의를 "충분한 정보를 제공받은 후 자유의지에 따라 이루어지는 사용자의 동의"로 정의하는 EPD에 위배된다.
- 영국 국내법에서 명시하고 있는 위법한 감청 금지 및 이에 대한 제재는 국제감청에만 제한되지만 유럽연합법은 보다 광범위하게 적용되고 국내외 등 지역적 한계를 벗어나 위법한 감청에 대해 처벌 하도록 하고 있다. 영국법은 전자통신의 비밀을 정확하게 이행하고 있지 않으며 정보보호위원회에 위반사실이 밝혀질 경우 이에 대해 과징금을 부과할 수 있는 권한을 부여하고 있지만 이는 DPD 제28조에 따른 적절한 대응이 아니다.

유럽연합법은 시민의 프라이버시와 자유의 보호를 목적으로 하며 전문규제청의 업무를 명시하고 있는 기본지침을 포함하고 있다. 전문규제청의 주요업무는

383) http://www.theregister.co.uk/2009/02/11/phorm_eu_action_threat/

384) 언론보도 IP/09/570 참조

지속적인 규제 개발을 위한 유럽집행위원회 및 타 기관과의 투명한 공조, 높은 수준의 개인정보 및 프라이버시의 보호, 공공통신 네트워크의 완전성 및 보안 유지를 포함한다.[385]

유럽재판소에 영국을 제소한 이유를 설명하고 있는 IP/10/121 문서는 영국이 DPD 및 EPD에서 명시하고 있는 의무를 위반하고 있다고 보는 위원회의 견해를 반영하고 있으며 영국에서 시행 중인 1998년 데이터 보호법과 2003년 프라이버시 및 전자 통신 규칙(EC 지침)에 대해 각각 "위원회는 영국 국내법은 감청 동의 및 감독기관의 운영에 대한 EU 지침을 이행하고 있지 않는 것으로 판단하다"고 밝혔다. 따라서 이번 사건은 영국의 통신 프라이버시 보호 조치의 적법성 및 이러한 규칙 및 관련법을 이행할 정보보호위원회와 사법수사기관의 권한에 대해 문제를 제기하고 있다.

아. 영국의 감청법 개혁

2012년 1월 26일, 유럽연합집행위원회는 침해 관련 사건에 대해 결정을 내렸고 영국이 이메일, 인터넷 브라우징과 같은 통신비밀에 관한 유럽연합법을 올바르게 이행할 수 있도록 하기 위해 국내법을 개정해야 한다고 판시했다.[386] 2010년 해당 사건을 유럽재판소[387]에 회부한 위원회의 2010 결정 이후 영국은 조사권한규제법 2000을 개정하였으며 감청을 행한 자가 피감청자의 동의를 받았다고 판단할 만한 '합리적인 근거'가 있다면 동의한 것으로 본다는 조항을 삭제하였다. 또한 동법 Section 1A와 부칙 A1[388]에 위법한 감청에 대한 처벌 규정을 신설하였는데 통신감청위원회(Interception of Communications Commissioner, ICC)가 처벌을 집행하고 새로운 기능 집행에 대한 지침을 발표한다.[389] 개정법에 따

385) 지침 2002/21/EC, Article 8(4)f at: http://eurlex. europa.eu/LexUriServ/LexUriServ.do?uri =CELEX:32002L0021:en:NOT.

386) European Commission - Press release IP/12/60, 'Digital Agenda: Commission closes infringement case after UK correctly implements EU rules on privacy in electronic communications' 참조

387) 언론보도 IP/10/1215 참조

388) 조사권한규제(벌금부과 고지 및 감청 동의) Regulations 2011, SI 2011/1340.

라 위반 시 최고 과징금액은 5만 파운드며 ICC 지침 2.15은 "통신감청위원회는 조사를 거쳐 피조사자가 합법한 동의 없이 통신을 감청하였거나, 감청 영장 집행 목적이 아닌 경우, 조사권한규제법 제1조에서 명시하고 있는 위반행위를 하지 않은 경우에 한해서만 벌금형을 고려할 수 있다"고 명시하고 있다.

3. 통신개입 사례

가. BT와 폼사에 대한 형사수사 중단

폼사의 시범운영에 대한 범죄수사는 공교롭게도 영국 정부가 관련법 개혁 및 재정비를 발표한 2011년 4월 8일 중단되었다. 2008년 런던시경은 조사를 시작해 이를 검찰에 송치하였고 검찰은 2011년 "사건의 기소가 국가의 공공이익에 반한다"는 이유로 수사 중단을 발표하였는데 그 내용은 다음과 같다.

- BT와 폼사는 감청을 위한 소프트웨어 사용과 관련해 충분한 법률자문을 받았고 기술의 사용이 조사규제권한 Section 1에서 명시하고 있는 규정에 위배된다고 볼 수 없다. 내무성은 또한 동일한 내용의 법률자문을 제공하였다. 두 번째 시범운영 후 BT는 이전의 법률자문 내용과 상충되는 자문 결과를 받고 시범운영을 중단하였다. 따라서 BT가 고의적으로 이를 위반하였음을 입증할 수 있는 증거가 없으므로 문제가 되는 감청은 실수나 관련법에 대한 잘못된 이해에서 비롯되었다고 판단할 만한 충분한 이유가 있다.
- BT와 폼사 모두 경찰 조사에 충실히 협조하였다.
- 문제가 되는 감청행위가 반복될 가능성이 없다. 처음 두 번의 시범운영 이후 BT는 기술의 시범운영을 공개하였고(2008년 말) 또한 폼사는 현재 사용자의 동의를 요청하고 있다.

---

389) Interception of Communications Commissioner, Investigation of Unintentional Electronic Interception: Monetary Penalty Notice, Exercise Of Powers Under Section 1a And Schedule A1 Of The Regulation Of Investigatory Powers Act 2000, (2011) at (http://www.intelligencecommissioners.com/docs/Interception_Commissioner_Guidance_RIPA.pdf)

- 시범운영은 제한된 기간 동안 제한적으로 이루어졌다. 수집한 자료는 모두 익명으로 처리되었으며 사람의 개입이 없었고 이후 모두 폐기되었다.
- 규제당국인 정보보호위원회도 조사를 실시하였고 위원회는 '관련자의 악의를 입증할만한 증거 불충분' 결정을 내렸고 이후 어떤 조치도 취하지 않았다.
- 시범운영으로 인해 개인의 피해나 손실이 발생하였음을 입증할 증거가 불충분하다.
- 위의 사항을 모두 고려해 보면 법원이 명목적인 처벌만을 결정할 가능성이 매우 높다.[390]

유럽연합집행위원회가 기능 수행에 적합한 권한을 갖고 있지 못하고 위법한 행위에 대해 벌금을 부과할 역량이 부족하다고 판단한 ICO의 평가서에 이러한 내용이 포함되어 있다는 점은 주지할 만 하다. 2009-2010년 ICO는 논의가 이루어진 후에야 BT와 폼사가 폼사의 시스템을 시범운영하지 않기로 결정한대 대해 그리고 Talk Talk과 버진미디어는 가입자의 통신을 감청한대 대해 P2P 파일과 스트리밍 차단은 망 중립성에 위배된다며 ISP들을 질책했다(유럽연합 규칙에 따라 이러한 감청행위는 2014년부터 위법한 것으로 간주된다). Talk Talk과 관련해 정보위원회는 "BT사의 웹와이즈(WebWise) 서비스에 대한 여론에 비추어 보았을 때 최근 회의에서 조차도 이러한 서비스의 시범운영에 대해 담당자들에게 설명하지 않았다는 것이 매우 실망스럽다"고 발표했다.[391] 영국의 관계당국은 ISP의 통신비밀 위반에 대해 기소하지 않고 경고만 했다.

ISP와 폼사가 수집한 정보는 가입자와 사용자의 동의를 얻었다 할지라도 위법하다 할 수 있다. 2009년 미의회와 영국의회 모두 온라인 맞춤형 광고에 대한

390) 검찰이 발표한 웹 서핑 기록에 대한 BT와 폼사의 수사 중단 이유(2011년 8월 4일) http://blog.cps.gov.uk/2011/04/no-prosecution-of-bt-andphorm-for-alleged-interception-of-browsing-data.html

391) 정보위원회 위원회 크리스토퍼 그라함(Christopher Graham) 경이 Talk Talk을 질책한 내용 인용. ICO는 멜웨어 시범운영에 대한 자세한 정보를 제공하지 않자 인터넷 서비스 제공자를 비난하였다. 멜웨어 시범운영은 사용자가 방문한 웹사이트 기록을 추적한다. Daily Telegraph, 2010년 9월 08일 보도. http://www.telegraph.co.uk/technology/internet/7989262/Information-Commissioner-reprimands-Talk-Talk.html 참조.

조사를 실시하였다.[392] ECD 제15조에 따라 유럽연합회원국은 2002년부터 ISP에 부당한 제한을 가할 수 없는데[393] 이로 인해 회원국들은 범죄근절, 테러방지 법 시행이라는 명분하에 전기통신지침이나 관련 조항을 국내법에 적용하지 않고 있다. 도감청 및 테러방지 법은 2001년 이후 통과되거나 수정되었고 테러방지법이 개정되면 정부를 대신해 ISP가 통신 감청을 하려면 전술한 ECD 제15조에 따라 28개 회원국이 국내법을 수정해야 한다는 점을 고려하였을 때 현재 유럽연합 회원국 내에만 수많은 관련 조항이 개정된 것으로 볼 수 있다. 유럽재판소는 2012년 이루어진 Sabam v Netlog NV[394] 판결에서 회원국의 저작권 침해 감시와도 관련이 있는 감시 의무제한에 대해 설명하였다. 재판소는 ISP의 저작권 필터 시스템 운영은 감시에 관한 일반의무 금지를 위반하고 있으며, "이는 서비스 제공자가 사용자의 정보적 자기결정권 및 인권을 침해하는 것이다. 실로, 문제가 되고 있는 필터링 시스템의 설치에 필요한 명령은 확인, 시스템적인 분석, 사용자가 소셜네트워크에서 만들어낸 파일에 관한 정보의 처리를 포함한다"고 판시하였다. 유럽집행위원회는 E-Europe 행동계획에서 제15조를 포함한 ECD의 개혁을 중단하였다. 행동계획은 어떠한 정부기관이나 법원도 감청 또는 통신데이터 감시에 관한 일반의무를 부여할 수 없는데 그 이유는 이러한 행위가 프라이버시 권리를 침해하기 때문이다.

---

392) http://www.theregister.co.uk/2009/04/24/deep_packet_inspection/ on the US investigation, and http://www.apcomms.org.uk/category/Activities/ announcing 'Can we keep our hands off the net?' apComms to investigate the role for Government over Internet traffic.

393) 지침 2000/31/EC 제15조는 다음과 같이 명시하고 있다. "트래픽을 감청할 의무가 없다. 1. 회원국은 제12, 제13, 제14조에서 규정하고 있는 서비스 제공에 있어 서비스제공자에게 전송하거나 보관하고 있는 정보의 감청을 의무화해서는 안 되고 위법한 행위가 있었음을 보여주는 사실이나 정황 파악을 의무화해서도 안 된다. 2. 회원국은 관계당국에 서비스를 제공받는 사용자들이 제공한 정보나 위법한 활동이 의심되는 경우 이에 대한 고지를 의무화하고 ISP가 사전에 동의를 받은 서비스 사용자 파악에 필요한 정보를 요청할 경우 이에 대한 연락을 의무화해야 한다."

394) Case C. 360/10, REFERENCE for a preliminary ruling under Article 267 TFEU from the rechtbank van eerste aanleg te Brussel (Belgium), 2010년 6월 28일 결정되었고 2010년 7월 19일 법원에 제출, in the proceedings Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV, at http://curia.europa.eu/juris/document/document.jsf?text=&docid=119512&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=161927

나. 통신감청 관련 기타 형사수사

글로벌 미디어 거물 루퍼트 머독이 소유한 언론사에서 고용한 사설탐정은 컴퓨터와 전화해킹을 통한 통신감청 위반혐의로 기소되었다.[395] 하지만 이는 망 중립성과는 직접적인 관련이 없으며 머독이 소유한 Sky Broadband는 고객의 통신 감청에는 직접적으로 연루되지 않았다. 공공기관에 의한 네트워크 감청에 대해 일반인도 수사권 재판소(Investigatory Powers Tribunal)에 소를 제기할 수 있으며 재판소는 주요한 사건의 판결문을 웹사이트에 공개하고 있다.[396] 그러나 ISP를 포함한 민간인이나 단체를 대상으로는 소를 제기할 수 없지만 대신 ICO나 경찰에 이를 신고할 수 있다. Bowden[397]과 Davies의 연구를 통해 영국법이 정부, 민간기업에 의한 감청으로부터 시민을 완전히 보호하고 있지 못함을 확인할 수 있었고 이들은 유럽의회의 결정 내용을 인용했다. "유럽연합 내 시설에 대한 미국의 감시프로그램 운영에 대하여 완전한 조사를 실시할 것이다. 이러한 프로그램이 유럽연합법과 양립할 수 있는지에 대해 조사할 것을 촉구한다. 조사를 위해서는 유럽과 미국간 민감한 신호정보, 특히 미국, 독일, 영국의 비공개 협력에 관한 정보를 공개해야 할 것이다."[398]

망 중립성 침해에 대한 형사책임으로는 저작권침해 및 위조 관련 조항을 적용할 수 있을 것이다. 민사책임으로는 저작권이 있는 저작물의 전재 및 전단에 대한 잠재적 피해보상, 소송 진행에 따른 소송비용청구, '악의적인' 저작권 침해에 따른 징벌적 손해배상이 포함된다. 이와는 대조적으로 2012년까지, 형사 책임은 '일정한 형태의 저작권 침해에 대한 조사로 제한되며 영국은 매우 이에 대해 매

395) BBC (2013) Phone hacking: Arrests by investigation, 13 June at http://www.bbc.co.uk/news/ukpolitics-17014930

396) 재판소는 "이러한 절차는 조사권한규제 제69조(6)(b)와 조사권한재판규칙(Invetigatory Powers Tribunal Rules- 행정입법 2000 No.2665) 규칙 6(1)에 반하여 이러한 절차로 인해 정보가 공개될 위험은 없다"고 판시하였다.

397) Bowden, Caspar (2013) PRISM: The EU must take steps to protect cloud data from US snoopers, The Independent 10 July 2013 at http://www.independent.co.uk/voices/comment/prism-the-eu-musttake-steps-to-protect-cloud-data-from-us-snoopers-8701175.html

398) Davies, Simon (2013) European Parliament votes to hold inquiry into US spying 4 July 2013, at http://www.privacysurgeon.org/blog/incision/european-parliament-votes-to-hold-full-inquiry-into-usspying/

우 신중한 입장을 취하고 있다.'[399] 하지만 2012년 1월 뉴질랜드에서 메가업로드(MegaUpload) 경영진이 체포된 후 미국에 대한 범죄인인도 요청은 형법 적용의 불확실성[400]을 야기했는데 그 이유는 2005년 사법집행 정책 개정이 이루어진 후에 사건이 발생했기 때문이다.[401] 형법상 '악의적' 요건을 충족하려면 반드시 합리적인 의심 이상이 요구된다.[402] 그럼에도 불구하고 위조 및 '저작권 침해' 혐의가 있는 웹사이트에 대한 적극적인 기소는 2011년 이른바 해외 '불량 사이트'의 도메인 네임을 추적하면서 시작되었다.[403] 메가업로드 사건 조사 시 이루어진 각 국가의 사법집행기관간 공조는 위조에 대한 적극적인 사법처리 의지를 보여주고 있다 할 수 있을 것이다. 하지만 2011년 하반기 있었던 미의회와 상원의 적극적인 감청방지 법안에 대한 논쟁을 간과하고 있다.[404]

4. 결론: 망 중립성 시행을 위한 규제의 문제점

망 중립성의 프라이버시 침해 문제는 규제 부재에 따른 것이 아니라 '불합리한' 차별로 인해 소비자가 입게 될 잠재적 피해를 분석할 수 있는 분석 기술이 부족하기 때문이다. 망 중립성이 규제 당국에게는 또 다른 어려운 과제를 제시하고 있고 문제 해결을 위해서는 국제공조와 협력을 통해 필요한 기술을 습득하

399) Dowling v United States, 473 US 207, 222 (1985).

400) Department of Justice Office of Public Affairs (19 January 2012) Justice Department Charges Leaders of Megaupload with Widespread Online Copyright Infringement 참조.

401) US ATTORNEY BULLETIN (2005) Novel Criminal Copyright Infringement Issues Related To The Internet available at (http://www.cybercrime.gov/usamay2001_5.htm) 참조.

402) US Attorney Prosecuting IP Crimes Manual, Criminal Copyright Infringement Issues, §II.B.2 (2006), available at (http://www.cybercrime.gov/ipmanual/02ipma.html#II.B.2.a) 참조.

403) Affidavit in Support of Application for Seizure Warrant Pursuant to 18 USC §§2323, 981, United States v Domain Names (defendants in rem), (31 January 2011) (No 18 MAG 262).

404) Law Professors (2011) Letter in Opposition to 'Threats to Economic Creativity and Theft of Intellectual Property Act of 2011' Draft 27 June 27 2011, available at (http://www.scribd.com/doc/59241037/PROTECT-IP-Letter-Final) 참조.

고 개발해야 할 것이다. 무엇보다도 통신규제당국 또는 관계부처에서 이를 규제하는 것이 중요하다. 규제당국은 트래픽 차별을 방지하기 위해서는 가입자와 서비스제공자와의 계약 및 ISP의 트래픽 셰이핑을 감독해야 할 것이다. 이론상으로 어떤 법적조치가 있건 이러한 규칙의 실질적인 적용 및 증거 수집이 규제당국에게는 상당한 부담이 될 수 있다. DPI는 사용자의 프라이버시를 불합리하게 그리고 부당하게 침해하는 기술이 되기도 하고 다른 한편으로는 사용자의 권리를 침해하는 행위를 조사하는데 사용될 수도 있다. 현재 ISP는 P2P 애플리케이션을 차단할 때 이를 사용자에게 고지하지 않아도 되며 통신사 규제당국의 권한에 정보보안도 포함되지 않는다. 제3자에 의한 온라인 맞춤형 광고의 증가 역시 프라이버시 규제당국에는 큰 고민거리가 되고 있으며, 온라인 맞춤형 광고와 관련한 폼사 사건 및 EU의 최근 의견발표[405] 이후 ISP와 관련 기업은 제휴를 통해 수익을 배분하려면 반드시 모든 사용자의 동의를 받아야 한다. 보안을 이유로 한 ISP의 P2P 트래픽 차단에 대해 내무성과 산업부에서 우려하고 있지만 규제당국은 데이터 보안과 관련해 전문지식이 부족하기 때문에[406] 상급기관의 지시만 따르고 있을 뿐이다. 망 중립성, 프라이버시 침해 방지를 위해서는 보다 긴밀한 협력과 공조가 필요하다 할 수 있다.

---

405) 회원국에 대한 프로파일링 맥락에서 자동으로 처리되는 개인정보와 관련해 프라이버시 보호에 관한 유럽평의회 권고안(CM/Rec(2010), 2010년 11월 23일 결정), 제한에 관한 Article 29 Working Party WP203, 00569/13/EN Opinion 03/2013, p45; Article 29 Working Party (2011) 유럽위원회 위원 프랑수아즈 르 배일(Françoise Le Bail)에게 보낸 서한- 국ㅈ가적 차원에서 이루어지는 현재 실무, 지침 시행 및 기타 데이터처리("민감한 데이터")와 관련이 있는 개선 또는 변경에 대한 제안 이행의 어려움에 대한 정보 및 지침 Directive 95/46/EC of 20.04.2011의 제28조 제6항의 고지 및 이행; EASA/IAB의 온라인 맞춤형 광고제공에 대한 가장 이상적인 실무를 위한 권고안에 대한 Article 29 Working Party (2011) 의견 Opinion 16/2011, 언론보도(2011년 12월 11일): "adherence to the EASA/IAB Code on online behavioural advertising and participation in the website www.youronlinechoices.eu does not result in compliance with the current e-Privacy Directive".참조.

406) Brown, I. Edwards, L. and Marsden, C. (2006), Legal and institutional responses to Denial of Service Attacks, Communications Research Network/Department for Trade and Industry joint seminar on Spam/DDoS, 13 November, at www.communicationsresearch.net/object/download/1846/doc/marsden-edwards.ppt and on file with the author.

5. 별첨: 정부의 통신데이터 감청

올 여름 통신감청위원회(Interception of Communications Commissioner, ICC)는 총리에게 전년도 연례 보고서와 2012년에 대한 최근 보고서[407]를 2013년 7월에 제출하였다. 2013년 6월 정보통신본부의 템포라 프로그램(Tempora programme)의 잠재적 위법성이 대중에서 폭로되는 등 사안에 대한 시급한 대처가 요구되었음에도 불구하고 ICC는 정보통신본부의 템포라 프로그램에 의한 통신감청을 조사해 2014년 7월에 제출하는 2013년 연례보고서에 조사 결과를 기재하겠다고 밝혔다.

"ICC는 조사권한규제법 제58조제4항에 따라 총리에게 연례 보고서를 제출해야 한다. 총리는 보고서 내용 중 민감한 사항을 제외하고 이를 의회에 제출하는데 총리는 공개하지 않을 정보를 스스로 결정한다."[408]

이에 더해 위원회 위원장은 "조사권한규제 법 제58조제4항에 위원회의 역할이 명시되어 있다. 위원장은 임명되지 않으며 동법 제58조제7항에 명시된 정보기관의 모든 활동을 감독할 권한을 갖고 있지 않다. 조사권한규제법 제1편 제1장은 영국 내에서 이루어지는 적법한 통신감청에 대한 권한을 규정하고 있다. 에드워드 스노든의 폭로에 따른 통신감청에 대한 언론보도를 조사하고 있다"고 밝혔다.

감청이 이루어지는 대부분의 데이터는 메타데이터로 이는 기계로 읽을 수 없고 막대한 양을 정밀 분석하기에는 시간이 너무나 촉박한 통신 컨텐츠보다 정보수집 및 온라인 맞춤형 광고에 더욱 적합하다. 조사권한규제법 2000의 제1편 제2장은 통신 데이터의 수집 및 공개에 대해 명시하고 있다. 이에 대해 ICC는 "통신데이터법안 마련을 위한 공동위원회에 권고안을 면밀하게 검토했다. 조사권한규제법 제1편 제2장에 따라 연례 조사는 2014년 1월에 시작된다"고 설명했다. 따라서 공공기관의 메타데이터 사용에 대한 조사는 2015년 시작되고 같은 해 7

407) HC 571 2012 Annual Report of the Interception of Communications Commissioner, Ordered by the House of Commons to be printed on 18th July 2013, SG/2013/131

408) ICC (2013) Sir Anthony May's response to the Article published in the Independent, 16 July 13, at http://www.iocco-uk.info/sections.asp?sectionID=8&chapter=4&type=top

월 결과가 발표된다. 메타데이터는 또한 유럽연합 전자프라이시법 개혁을 위한 2013/2014 제29조 실무그룹의 주요과제이다[409].

제4절 망 중립성과 통신비밀에 대한 호주의 입법 현황[410]

1. 호주의 망 중립성

가. 망 중립성 정의

망 중립성은 다양한 기술 및 법적 의미에 따라 다르게 규정할 수 있다. 인터넷 거버넌스계에서는 망 중립성을 규제를 받지 않고 자유롭게 접속할 수 있는 기본 원칙 또는 권리로 보고 있지만 일부에서는 망 중립성을 기업의 활동을 규제해야 하는 경제경쟁으로 보고 있다(Hahn & Wallsten 2006). 이렇듯 망 중립성의 정확한 의미에 대해 합의된 정의는 없다. 망 중립성의 기본 개념은 인터넷 서비스 제공자와 네트워크를 이동하는 정보와 데이트를 분리하는 것이다. 다시 말해, 모든 데이터를 동등하게 취급하며 전송된 데이터가 차별 없이 자유롭게 한 지점에서 다른 지점으로 이동할 수 있어야 한다.

망 중립성 찬성론자들은 망 중립성 원칙이 온라인 프라이버시에 악영향을 미칠 수 있다는 생각에 대해 우려를 표하고 있다. 반면, 망 중립성 반대론자들은 차별과 규제가 인터넷 사용 전반에 걸쳐 혜택을 가져다 줄 것이라고 주장한다. 지금까지 제기된 호주의 망 중립성 관련 논의들을 살펴보면, 주요 거론되는 주제는 크게 가격모델, 인권, 정부규제 및 기술로 요약할 수 있다. 호주의 경우 망 중립성에 관한 명확한 규정이나 규제는 없지만 현재 법과 정책은 잠재적으로 영

409) Article 29 Working Party (2010) Opinion 2/2010 on online behavioural advertising WP 171, at p7 (22.06.2010): "Article 29 Working Party is deeply concerned about the privacy and data protection implications of this increasingly widespread practice."

410) 호주의 망 중립성 정책 관련 입법현황은 Australian National University 박사과정에 재학 중인 Steve Chon과 Alice Hutchings의 적극적인 도움으로 이 보고서에 포함될 수 있었다. 또한 호주 국내법과 관련해 Gregor Urbas교수와 Peter Grabosky교수의 조언이 보고서 작성에 반영되었다.

향을 미칠 것으로 보인다. 본 연구는 인터넷 서비스 제공자들의 인터넷 트래픽 차단, 개입, 감독 및 데이터 보유에 대해 살펴보고자 한다. 이는 검열 및 인터넷 컨텐츠 필터링에 대한 우려를 불러일으킬 수도 있다.

나. 연구 목적

본 연구는 호주의 향후 망 중립성 관련법, 규제 및 정책에 관한 것으로 먼저 호주의 인터넷 현황에 대해 간단하게 소개하고 다음으로 인터넷 차단의 개념 및 심층패킷검사(DPI)과 관련해 최근 통계를 살펴보았다. 본 연구의 주제는 순차적으로 프라이버시, 모니터링/감시, 온라인 콘텐츠 규제이며 주제와 관련해 두 가지 사례를 분석해 보았다. 마지막으로 인터넷 서비스 제공자들이 사용하는 자기 규제 모델을 살펴보고 데이터 보존 의무와 경쟁에 대해 개선방안을 제안하고자 한다. 본 연구는 특히, 형사정책('범죄'는 악영향을 미칠 수 있는 일정한 범주를 벗어난 위반행위로 해석)과 망 중립성(인터넷 패킷 차원), 프라이버시(고객과 일반 대중) 및 통신비밀(온라인에 기초) 사이의 교차점에 대해서 살펴보았다. 마지막으로 이 장의 서술은 호주 현황에 대한 설명을 목적으로 함을 밝힌다.

다. 호주 현황

호주는 인터넷 사용과 관련해 지리적인 면에서나 인프라 면에서 많은 어려움에 직면하고 있는데 그 이유는 인구가 넓은 영토에 산재해 있기 때문이다. 전(前) 호주정부는 특히 지방과 산간지역의 인터넷 연결 속도를 높이고자 국가고속통신망 네트워크(National Broadband Network)를 추진했다.[411] 그러나 새롭게 출범한 정부는 특히 연결 속도와 관련해 국가고속통신망의 전달에 영향을 미칠 것으로 예상된다.

2012년 12월 현재, 호주의 인터넷 가입자 수는 1220만 명에 이른다. 가입자 수가 1,000명 이상인 인터넷 서비스 제공자(이하, ISP) 수는 76개에 이르며 가입

411) NBN Co 2011. *National Broadband Network - Information Pack.* North Sydney: NBN Co. http://nbnco.com.au/news-and-events/news/national-broadband-network-information-pack.html

자 수가 100,000명 이상인 대형 ISP는 8개에 이른다. 8개 대형 ISP의 총 가입자 수는 1130만 명으로 전체 시장의 93%에 이른다(2013년 호주 통계청).

국가고속통신망 네트워크 구축에 따라 데이터 요청이 증가했다. 가입자 1,000명 이상인 ISP의 보고에 따르면, 2012년 12월 31일 끝난 4/4분기 동안 총 데이터 다운로드 양은 554,771 테라바이트로 전년도 동기간 대비 무려 189.2%(총 191,839 테라바이트) 성장했다(2013년 호주 통계청).

2010년, 호주 일반가정의 인터넷 가입률은 62%로 경제협력개발기구(OECD) 회원국 중 22위를 기록했지만 사실 통계수치는 2008년에 집계된 것이다. OECD 회원국 중 인터넷 가입률은 한국(97.5%), 아이슬란드(87.0%), 노르웨이(82.6%), 스웨덴(82.6%), 덴마크(80.1%) 순으로 높다.[412]

같은 해 호주는 기업과 비영리 단체의 인터넷 보급률에 있어 OECD 회원국 중 3위를 차지했으며 피고용인 10명 이상인 사업장의 인터넷 초고속 인터넷 가입률은 96.6%를 기록했다. OECD 회원국 중에는 한국이 1위(98.6%)를 차지했으며 스페인(95.4%), 아이슬란드(95.3%)로 뒤를 이었다.[413]

Net Index는 국가간 인터넷 속도를 비교하기 위해 Speedtest.net의 테스트 결과를 이용했다. 2011년 3월 10일부터 2013년 9월 8일까지의 기간 동안 호주의 평균 인터넷 속도는 13.74 Mbps로 회원국 중 48위를 차지했다. 인터넷 속도에 있어 상위 5개국은 홍콩(61.61 Mbps), 룩셈부르크(47.06 Mbps), 싱가포르(41.18 Mbps), 한국(40.77 Mbps), 일본(40.72 Mbps)순으로 나타났다. 업로드 속도에서 호주는 92위를 차지했으며 파일의 평균 업로드 속도는 2.50 Mbps이다.[414]

412) OECD 2011a. OECD Broadband statistics. 2a Households with broadband access 2000-10. http://www.oecd.org/internet/broadbandandtelecom/oecdbroadbandportal.htm

413) OECD 2011b. OECD Broadband statistics. 2d Business use of broadband, 2003-2010 or latest available year. http://www.oecd.org/internet/broadbandandtelecom/oecdbroadbandportal.htm

414) Net Index 2013. Household download index. http://www.netindex.com/

라. 인터넷상에서의 차단을 위한 기술적 방법

목적에 맞는 다양한 방법을 이용해 인터넷 트래픽과 사이트 접속을 차단할 수 있다. 특정한 사이트에 접속하는 것을 차단하기 위해 가장 보편적으로 사용되는 방법이 블랙리스트(Blacklist)이다. 블랙리스트에 오르는 사이트는 일반적으로 특정한 목적에 따라 선정되며 지속적으로 접속을 차단하기 위해 이후에도 교차참조를 하게 된다. 인터넷 검열은 규제와 관련이 되어 있으며 특히 특정한 종류의 콘텐츠에 접속하지 못하도록 한다. 필터링은 특정한 사이트나 데이터에만 접속할 수 있도록 허용하며 나머지 사이트나 콘텐츠는 차단한다. 차단, 검열, 필터링의 용어는 사실 의미상 미묘한 차이가 있으나 대부분 혼용해서 사용되고 있다. 가장 흔한 예로, 아동 포르노와 같은 금지 콘텐츠의 차단을 들 수 있으며 이는 많은 국가에서 실질적으로 사용되고 있다. 또한, 인터넷 속도의 성능을 일부러 낮추어 품질을 떨어뜨리는 인터넷 또는 초고속인터넷의 속도 제한(throttling)도 이용되고 있다.

컨텐츠, 웹사이트 주소, 또는 패킷 필터링 등 하나 또는 두 개 이상의 기술이 트래픽 차단에 사용되고 있다.[415] 특정 단어 또는 URL을 이용하는 웹사이트 필터링은 다양한 차단기술 중에서도 가장 간단한 방법으로 보편적으로 사용되고 있다. 인터넷상에서 정보는 데이터의 유닛 형태, 즉 패킷의 형태로 전송되기 때문에 이러한 정보를 사전에 검사하거나 사전에 확인할 수 있으며 또한 속도를 늦추고 완전히 차단할 수 있다. 심층패킷분석(이하 DPI)은 미국과 캐나다에서 이용되는 비트토렌트(BitTorrent) 트랙픽의 속도를 늦추기 위해 패킷을 모니터하는 기술이다.[416]

---

415) Varadharajan V 2010. Internet filtering-Issues and challenges. *Security & Privacy, IEEE, 8*(4), 62-65.

416) Mueller M L & Ashgari H 2012. Deep packet inspection and bandwith management: Battles over BitTorrent in Canada and the United States. *Telecommunications Policy, 36*(6), 462-475.

마. 호주 인터넷 서비스 제공자들의 심층패킷검사 활용

M-Lab은 사용자의 참여를 바탕으로 하는 크라우드 소스드 데이터(Crowd sourced data)를 수집하여 심층패킷검사를 이용해 비트토렌트 등 개인 간 파일 공유 프로토콜을 차단하거나 속도를 늦추는 IPS를 파악했다. M-Lab의 프로젝트, '글라스노트(Glasnost)'는 10번 중 1번꼴로 오류나 에러가 발생했다고 보고했다. M-Lab은 글라스노트의 분석 결과에 대한 이해를 돕기 위해 가이드라인을 제공했으며 그 내용은 다음과 같다. 여러 번에 걸친 검사 결과가 10% 미만일 경우 심층패킷검사를 이용해 비트토렌트를 차단하거나 속도를 늦춘 가능성이 매우 낮다. 동 기간 동안 11~50%일 경우 피크타임, 특정 네트워크나 특정 사용자 그룹 등을 지정해 제한해 차단 또는 속도를 늦추었을 가능성이 높으며, 50% 이상일 경우 모든 비트토렌트 데이터를 조작했을 가능성이 매우 높다.

글라스노트의 검사는 2009년부터 2012년 1사분기까지 호주를 포함해 59개국을 대상으로 실시되었으며 M-Lab 웹사이트[417]에서 확인할 수 있다. 검사 결과를 종합해 보면 심층패킷검사를 이용해 비트토렌트를 조작한 ISP의 비율은 19%에 달한다(중간값=10%). 호주 평균은 13%로 전체평균보다 낮다(중간값=9%). 호주의 경우, 12개 ISP 중 절반 이상이 DPI를 이용했지만 그 비율이 높지는 않았다.[418]

위의 데이터를 통해 호주 ISP가 비트토렌트를 차단하거나 속도를 늦추기 위해 DPI를 이용한다는 것을 알 수 있지만 검사기간 동안 이른바 'DPI를 이용한 비트토렌트 차단 또는 속도제한 최상위 ISP(Top Throttler)'에는 포함되지 않았다. 2012년 1사분기 동안 필리핀에 소재한 ISP들이 가장 많이 심층분석패킷을 이용했으며 다음으로 에스토니아, 일본, 캐나다, 대만, 영국, 말레이시아, 한국, 아르헨티나가 그 뒤를 이었다.[419]

호주 ISP의 DPI 이용 범위를 측정하기는 현실적으로 매우 어렵다. 이와 관련

417) http://dpi.ischool.syr.edu/ISPtable.html

418) Mueller M 2013. The network is aware: Social science research on deep packet inspection. http://dpi.ischool.syr.edu/Home.html

419) Ibid, Muller M 2013.

한 기사 내용을 인용하면 다음과 같다.

“ISP는 심층패킷분석의 활용에 대해 침묵하려 하는데 그 이유는 이로 인해 사용자의 불만을 야기할 수 있을 뿐만 아니라 DPI 사용이 감청의 구성요건에 해당되는지에 관한 골치 아픈 법적문제에 휘말리고 싶지 않기 때문이다.”[420]

이와 관련해서는 후술하겠지만 호주의 인터넷 서비스 제공자인 텔스트라(Telstra)는 P2P 서비스 이용으로 인한 인터넷 트래픽 혼잡을 줄이기 위한 DPI의 이용 가능성을 현재 시험하고 있다고 발표했다. iiNet를 포함해 호주의 일부 ISP가 DPI를 이용해 가입자에게 전체 데이터 사용량에 포함되지 않으면서 데이터에 접속할 수 있도록 허용하는 소위 ‘무료’ 서비스를 제공하고 있다는 사실은 잘 알려져 있다.

Telstra의 사례를 통해 알 수 있듯이 DPI의 이용은 대역폭 제한 등을 포함한 이용약관을 시행하려는 ISP의 첫 번째 조치로 볼 수 있다. 하지만 이용약관에 따라 저작권을 침해하는 컨텐츠 다운을 금지하고 있는지, 실제로 DPI가 사용되고 있는지 또는 ISP의 DIP 사용이 정당한지에 대해서는 알려진 바가 없다. 실제로 DPI의 사용과 관련해 가장 논란이 되고 있는 것은 수사기관, 국가보안기구 또는 정부의 인터넷 트래픽 개입이다. 모니터링, 감시 및 도감청 관련법은 지금까지 아날로그 방식의 통신에 적용되어 왔다. 때문에 과연 이들 법을 인터넷 통신에도 적용할 수 있는 지에 관한 논의가 현재도 활발하게 진행되고 있다. 모니터링의 한 형태로 볼 수 있는 DPI의 사용을 의도했건 또는 의도하지 않았건 ISP의 인터넷 통신관련 데이터 또는 ‘메타데이터(metadata)’의 수집은 향후 논의가 되어야 할 부분이다.

420) Saarinen J 2010. Analysis: The murky world of deep packet inspection. http://www.itnews.com.au/News/163435,analysis-the-murky-world-of-deep-packet-inspection.aspx

2. ISP와 호주 정부의 감시 및 모니터링

가. 1988 사생활 보호법 및 인터넷 필터링과 데이터 보존의 함축적 의미

1988년 사생활보호법은 개인정보보호원칙(National Privacy Principles, NPPs)을 명시하고 있다. 개인정보보호원칙은 사생활보호법 부칙3에 명시되어 있으며 데이터 수집, 이용 및 공개, 데이터 품질, 데이터 보안, 개방, 접근, 수집, 식별자, 익명성, 국가간 데이터 유통, 민감한 정보에 대해 규정하고 있다.

사생활보호법은 온라인 정보와 일부 관련이 있지만 잘못 이해되는 경우가 있다. 예를 들면, 이 법은 수사기관의 인터넷 남용 조사를 금지하고 있지 않다. 실제로 나중에 다시 한 번 언급하겠지만 1997년 전기통신법(Telecommunications Act) 제313조는 ISP에 인터넷 남용을 방지할 법적 의무를 부여하고 있다. 또한 형법 제474.25조에 따라 ISP는 아동포르노 위반 사항을 호주 연방경찰에 보고하여야 한다. 이와 관련하여 부칙3의 개인정보보호원칙 1.1은 다음과 같이 명시하고 있다.

> 1.1 기관은 개인정보를 수집하여서는 안 된다. 단 개인정보가 이러한 조직의 하나 또는 그 이상의 기능 또는 역할을 수행하는데 있어 반드시 필요한 경우는 제외한다.

Vaile와 Watt[421]에 따르면 개인정보보호원칙 1.1은 ISP가 저작권 침해 방지 목적으로 DPI를 이용한 인터넷 컨텐츠 필터링을 금지하고 있다고 한다.

호주의 저작권 필터(copyright filter)는 ISP 차원에서 시행되어야 하는데 그 이유는 ISP는 호주 인터넷 이용자들에게 인터넷 서비스를 제공할 뿐만 아니라 호주의 인터넷 트래픽이 만나는 중간접속점이기 때문이다. 법인격체로서 ISP는 조직에 해당된다. '수집'은 '모으다' 또는 '집합시키다'라는 원래의 의미를 그대로

421) Vaile D & Watt R 2009. Inspecting the Despicable, Assessing the Unacceptable: Prohibited Packets and the Great Firewall of Canberra. UNSW Law Research Paper 2009-35. http://ssrn.com/abstract=1477816

내포하고 있으므로[422], DPI는 법률로 정한 범위 내에서 자료를 수집한다. DPI가 패킷 발신인과 수신인의 IP 주소를 확인하기 때문에 특정 개인의 자료를 수집한 데이터는 '개인정보'에 해당한다.(사생활보호법 s 6[423])

ISP의 기능 또는 활동의 목적은 최종 이용자에게 인터넷 연결을 제공하는 것이다. 저작권이 있는 자료에 대한 연결 필터링은 '반드시 필요한 행위가 아니며' '저작권 침해 방지'에도 해당되지 않는다. 필터링의 필요성과 관련해 살펴보면 앞에서 언급한 두 가지 가치 사이에는 애매한 중간영역이 존재하는데 DPI는 ISP가 본연의 기능 또는 업무를 수행하기 위해 명백히 '필요한' 것은 아니다. 또한 이용자의 브라우징과 관련된 정보는 상업적 가치(이동자의 정치, 도덕 및 기타 성향을 파악하는데 있어 상당한 가치가 있음)가 있으므로 필요성에 대한 기준을 강화해야할 '민감한' 정보이다[424] 이 사안과 관련해서는 다시 설명하겠지만 호주 연방 정보 및 보안 합동위원회에서도 2013년 올해, 정부의 이동통신사의 데이터 보존 의무화 제안과 관련해 이러한 원칙을 논의한 바 있다.

나. 1997년 통신법(Telecommunications Act 1997)에서 명시하고 있는 통신사와 통신서비스 제공자의 의무

1997년 통신법(호주 연방)은 전화 및 인터넷 서비스를 제공하기 위해 통신 서비스를 이용하는 '통신서비스제공자'를 포함해 통신사와 관련한 사항을 자세히 명시하고 있다. 통신법 제313조는 통신사는 연방정부, 주정부, 지방정부의 위법 행위 및 이들과 관련해 통신사의 네트워크 및 시설의 사용행위를 방지하기 위하

422) Federal Court Strengthens Privacy Enforcement: Seven Network (Operations) Limited v Media Entertainment and Arts Alliance [2004] FCA 637' (2005) 33 Australian Business Law Review 45, 45.

423) Telecommunications (Interception and Access) Act 1979-SECT 6

Interception of a communication

(1) For the purposes of this Act, but subject to this section, interception of a communication passing over a telecommunications system consists of listening to or recording, by any means, such a communication in its passage over that telecommunications system without the knowledge of the person making the communication.

424) Tenants Union 2004, 49 및 Ibid, Vaile & Watt 2009, 23-24).

여 “최선을 다할” 의무가 있다고 명시하고 있다. 또한 서비스 제공자는 형사사건, 국고수입보호 및 보안 유지를 위해서는 국가기관에 필요한 지원을 제공해야 할 의무가 있다. 이러한 지원에는 1979 통신감청접근법(Telecommunications (Interception and Access) Act 1979)에서 규정하고 있는 국내 또는 해외 통신기록 보존 통지 준수, 저장된 통신기록 영장 집행, 통신감청영장 집행을 포함한다. 통신감청접근법 제313조는 다음과 같이 명시하고 있다.

313. 통신사 및 통신서비스 제공자의 의무

(1) 통신사 또는 통신서비스 제공자는
(a) 통신사 또는 이동통신 네트워크 또는 시설 제공자의 운영, 및
(b) 통신사 또는 이동통신 서비스 제공자의 서비스 제공과 관련하여 연방정부와 주정부가 법에 반하여 이동통신사의 네트워크 및 시설을 이용하지 못하도록 최선을 다하여야 한다.
(2) 통신서비스매개자는 연방정부와 주정부가 법에 반하여 이동통신사의 네트워크 및 시설을 이용하지 못하도록 최선을 다하여야 한다.
(3) 통신사 또는 통신서비스 제공자는
(a) 통신사 또는 이동통신 네트워크 또는 시설 제공자의 운영, 및
(b) 통신사 또는 이동통신 서비스 제공자의 서비스 제공과 관련하여 연방정부 및 주정부 관계자 및 당국에 다음 각 호의 목적을 위해 합리적으로 필요할 경우 지원을 제공하여야 한다.
(c) 형법 및 처벌에 관한 법 지행
(ca) 해외에서의 형법집행 지원
(d) 국고수입 보호
(e) 국가안보 보호

주의: 제314조는 지원 제공의 조건에 대해 명시하고 있다.
(4) 통신서비스제공자의 통신서비스 제공을 매개하는 통신서비스매개자는
(a) 통신사 또는 이동통신 네트워크 또는 시설 제공자의 운영, 및
(b) 통신사 또는 이동통신 서비스 제공자의 서비스 제공과 관련하여 연방정부 및 주정부 관계자 및 당국에 다음 각 호의 목적을 위해 합리적으로 필요할 경우 지원을 제공하여야 한다.
(c) 형법 및 처벌에 관한 법 지행
(ca) 해외에서의 형법집행 지원
(d) 국고수입 보호
(e) 국가안보 보호

주의: 제314조는 지원 제공의 조건에 대해 명시하고 있다.
(5) 통신사 또는 통신서비스 제공자는
(a) 제(1)항, 제(2)항, 제(3)항 또는 제(4)항에서 명시하고 있는 의무 이행
(b) 호주통신미디어청(ACMA)가 제312조에서 명시하고 있는 의무 이행을 위하여 시행하거나 시행하지 않은 조치에 관해 또는 이와 관련하여 피해보상소송이나 절차에 있어 면책된다.
(6) 통신사 또는 통신서비스 제공자의 피고용인, 직원 또는 관련자는 전항에서 명시한바와 같이 통신사 또는 통신서비스 제공자가 행하거나 시행하지 않은 조치에 관해 또는 이와 관련하여 피해보상소송이나 절차에 대해 법적책임을 지지 않는다.
(7) 당해 조항의 지원제공에 대한 내용은 다음 각 호의 방법에 따른 지원제공에 대한 내용을 포함한다.
(a) 1979년 통신감청접근법에 따른 통신감청영장 집행 업무를 포함한 통신감청 서비스 제공
(b) 1979년 통신감청접근법에 따른 저장된 통신기록 영장집행
(c) 이하에 관한 관련 정보 제공

(ⅰ) 감청영장에 따라 합법적으로 감청한 통신
(ⅱ) 저장된 통신기록 영장에 따라 합법적으로 접근한 통신
(ca) 1979년 통신감청접근법 Part 3 1A에 따른 국내기록보존통지 또는 해외기록보존통지 준수
(d) 1979년 통신감청접근법 Division 3 또는 Part 4 1에 따른 권한 행사, 또는
(e) 당해법 제280조에 따른 정보 또는 문서의 공개

주의: 감청능력 및 제공능력에 관한 추가 의무를 1979년 통신감청접근법에 따라 통신사 또는 통신서비스 제공자에게 부과하거나 부과할 수 있다.

통신법 제313에서 명시하고 있는 의무는 이하에서 설명할 통신감청접근법에 적용된다. 또한 본 조항은 호주의 온라인 컨텐츠 규제와 관련하여 적용된다.

다. 1979년 통신감청접근법의 감청영장, 저장된 통신기록 영장, 국내 및 해외 기록보존통지 및 통신데이터 접근

1979년 통신감청접근법(이항 통감법)은 통신감청영장, 국내 및 해외 보존통지, 저장된 통신기록 접근을 주요 내용으로 하고 있다. 감청법에 따르면 호주 통신 네트워크에 대한 감청과 저장된 통신기록에 대한 접근은 영장이 발부된 경우를 제외하고 금지되지만 통신데이터는 영장 없이 수사기관에 공개할 수 있다. '감청'은 다음과 같이 정의된다.

이 법의 목적에 따라, 그러나 당해 조항을 전제로 하여, 통신시스템에 대해 이루어지는 통신감청이라 함은 통신을 하는 사람이 인지하지 못한 상태에서 이루어지는 통신 시스템을 통과하는 통신을 감청 또는 기록하는 행위를 말한다.

법무부에 따르면[425] 저장된 통신기록에는 보이스 메일, 이메일, SMS 메시지 등이 포함된다. 국내 또는 해외 기록보존통지에 따른 통신사의 통신기록 보존 의무화를 주요 골자로 하여 2012년 통감법이 개정되었다. 일별 또는 특정기간 기록에 대한 국내 보존통지는 3년 이하의 징역이나 금고 또는 180단위 벌금[426]

425) Attorney-General's Department 2012b. *Surveillance Devices Act 2004 Report for the year ending 30 June 2012*.

426) 호주는 벌금 단위에 따라 벌금을 부과하며 1단위는 170 호주 달러이다. 따라서 180단위 벌금은 170 ×180 = 30,600 호주 달러의 벌금을 의미한다. 자세한 내용은 호주형법 CRIMES ACT 1914 - SECT 4AA 참조.

에 처해질 수 있는 죄를 범하였다고 의심되는 사건의 조사를 위해 연방 또는 주 수사당국 또는 호주 보안정보기구(ASIO)가 발부할 수 있다. 일일기록 통지는 통신사가 보유하고 있는 특정일의 통신기록을 말하며 특정기간기록 통지는 30일간의 통신기록을 말한다. 해외 기록보존통지는 통신사가 보유하고 있는 특정일의 통신기록에 한하며 사형, 무기, 3년 이하의 징역 또는 금고, 또는 900단위 벌금에 처해질 수 있는 중대한 해외 범죄와 관련해 외국 수사당국의 요청이 있는 경우에만 호주 연방경찰청이 발부할 수 있다. 국내 또는 해외 기록보존통지에 따라 영장을 발부 받아야만 보존된 기록에 접근할 수 있다.

감청법은 통신감청영장 및 저장된 통신기록 영장에 대해 명시하고 있다. 일반적으로 통신감청에 대한 조항이 저장된 통신기록 영장에 관한 조항보다 엄격하다. 예를 들면, 통신감청영장은 범죄수사대(Australian Crime Commission), 법집행청렴위원회(Australian Commission for Law Enforcement Integrity), 연방경찰 및 기타 감청법 제34절에서 규정하고 있는 사전통지 의무가 있는 주당국 등 '감청기관'에만 제한적으로 발부된다. 이와 비교해, 저장된 통신기록 영장은 국고수입을 보호하거나 벌금형 등 상대적으로 가벼운 위반행위를 수사하는 '수사당국'에 발부된다. 좀더 자세히 살펴보면 감청영장은 살인, 마약, 테러, 7년 이상의 구금형에 처할 수 있는 중대범죄, 아동성범죄, 자금세탁, 사이버범죄 및 조직범죄 등 중죄의 조사 지원을 위해 필요한 경우에만 신청할 수 있다.

감청법에 따라 감청영장은 법원 또는 지정된 행정심판관만이 발부할 수 있다. 저장된 통신기록영장은 치안판사 또는 판사 또는 법무부에서 지정한 담당자가 발부할 수 있다. 두 영장 모두에 대해 전화로 긴급승인을 요청할 수 있다. 해외보존통지와 관련해서 저장된 통신기록 영장은 사법공조 요청에 따라 법무부가 발부할 수 있다.

2011년과 2012년 사이 법집행기관에서 신청한 감청영장 건수는 3,764건에 이르며 이중 3,755건에 대해서는 영장이 발부되었다. 이전과 비교해 영장발부 건수는 약 7.7% 증가하였다. 동기간 동안 저장된 통신기록 영장신청은 485건이며 이중 단 2건만을 제외하고 483건에 대해서는 영장이 발부되었다.(법무부 2012b)

통신데이터에는 가입자의 개인정보와 관련이 있는 메타데이터, 통신일, 시간, 기간 및 위치, 인터넷 식별자 또는 서비스 식별자(이메일주소, 전화번호 또는

VoIP 번호)가 포함될 수 있지만 통신 내용은 포함되지 않는다(법무부 2012b). 통감법에 따라 법집행기관, 벌금형을 부과할 수 있는 수사당국, 국고수입보호 기관은 범죄의 심각성에 관계없이 저장된 통신데이터 공개를 승인할 수 있다. 반면 예상자료(prospective data)는 3년 이상의 징역이나 금고형에 처해 질 수 있는 범죄사건의 수사와 관련해서만 수사당국이 승인할 수 있다.

2011년과 2012년 사이, 형사사건과 관련하여 총 293,501건의 일별 통신데이터 접근 요청이 있었으며, 벌금형을 부과할 수 있는 수사당국, 국고수입보호 기관의 데이터 접근요청은 총 144건에 이르렀다. 또한 수사당국 및 반부패기관의 요청뿐만 아니라 연방정부, 주정부 및 지방정부에서도 통신데이터 접근을 요청했다. 예상자료와 관련해서 동 기간 동안 수사당국의 기록접근 요청건수는 5,811건에 이르렀으며, 요청 승인까지 걸린 시간은 평균 28일이다.(법무부 2012b)

라. 2004년 감시장치법에 따른 데이터 감시장치에 대한 별도 영장

2004년 감시장치법에 따라 명시된 연방, 주, 지역 수사당국은 관련 사건의 수사를 위해 감시장치사용을 요청할 수 있다. 관련사건은 3년 이상의 징역이나 금고에 해당되는 범죄로 국외 사건도 포함된다(단 외국 관련당국의 동의를 받아야 한다). 감시장치법에 따라 호주당국은 외국정부에 관할권내에서의 감시장치 사용 허가를 요청할 수 있다. 이 법에 따라 법무부장관의 승인을 받아 감시장치 사용을 위한 사법공조도 요청할 수 있다. 주와 지방의 수사기관은 연방법과 관계없이 자체적으로 법률조항을 제정할 수 있다. 감치장치는 감청, 추적, 데이터 감시를 할 수 있는 기기를 말한다. 데이터감시장치란 다음과 같이 정의된다.

"데이터감시장치"란 컴퓨터에서 정보의 입력 또는 출력을 기록 또는 감시하는데 사용할 수 있는 기기 또는 프로그램을 말하며 시각적 감시장치는 포함하지 않는다.[427]

427) SURVEILLANCE DEVICES ACT 2004 - SECT 6
"data surveillance device" means any device or program capable of being used to record or monitor the input of information into, or the output of information from, a computer, but does not include an optical surveillance device.

위의 감시장치에 대한 정의는 데이터의 기록 또는 감시 시점, 또는 사용할 수 있는 기술에 대해서는 명시하지 않고 있다. 예를 들면, 데이터감시장치에 대한 정의는 소프트웨어와 하드웨어 키로거, 전자기방사선기에도 똑같이 적용할 수도 있다.

감시장치는 법원 또는 지정된 행정심판관이 영장을 발부한 경우에만 사용할 수 있다. 영장은 연장되거나 철회된 경우를 제외하고 발부일로부터 90일 동안 유효하다. 긴급 상황 시 긴급조치가 시행될 수 있으나 반드시 48시간 내에 영장을 발부 받아야 한다.

2011-2012년 사이, 감시장치법에 따라 642건의 영장이 발부되었다. 이중 601건(93.6%)는 다양한 종류의 감시장치에 관한 것이며 데이터 감시장치에 대한 영장청구건수는 단 두건(0.3%)에 불과 했다. 감시장치 사용허가는 호주연방경찰청에서 승인하였다[428].

마. 데이터보존 및 유럽의회 사이버범죄방지조약

2012년 11월 30일, 호주 정부는 유럽의회의 사이버범죄방지조약에 가입했다. 사이버범죄방지조약은 국제협력 강화를 위해 해킹, 사기, 아동포르노, 저작권 침해물과 관련해 일관된 법적용을 위한 국내법의 수용과 별도의 입법조치를 가입국에 요구하고 있다(호주 조약에 관한 의회 상임위원회(Parliament of Australia Joint Standing Committee on Teaties) 2011). 조약에 가입하기 위해 2013년 3월 1일 발효된 2012년 사이버범죄입법개정법(the Cybercrime Legislation Amendment Act 2012)에 따라 형사사법공조법(Mutual Assistance in Criminal Matters Act 1987), 형법(the Criminal Code Act 1995), 통신감청법, 통신법을 개정하였다. 법무부에 따르면 사이버범죄입법개정법의 내용은 다음과 같다.

- 국내기관 또는 외국 기관을 대신해 호주 연방경찰국이 요청할 경우 특정인의 저장된 통신기록을 제공할 통신사와 통신서비스 제공자의 의무

428) Attorney-General's Department 2012a. *Surveillance Devices Act 2004 Report for the year ending 30 June 2012*. Barton: Commonwealth of Australia. http://www.ag.gov.au/NationalSecurity/TelecommunicationsSurveillance/Pages/Annualreports.aspx

- 호주관계당국의 해외 조사를 위한 통신데이터 및 저장된 통신자료 입수 또는 공개,
- 통감법에서 규정하고 있는 특정범죄의 해외적용,
- 적용범위를 명확히 하기 위한 형법(Criminal Code Act 1995)상의 컴퓨터 범죄관련 조항 개정
- 통신데이터 공개 승인과 관련한 기밀유지 조항 신설

3. 호주의 온라인 컨텐츠 규정

가. 2008-2012 등급거부컨텐츠 필터링 의무화 제안

2008년, 호주의 브로드밴드통신경제개발부(Department of Broadband, Communications and the Digital Economy)는 온라인 컨텐츠의 필터링 의무화 계획을 발표하였다. 제안서에 따르면, 등급거부컨텐츠에는 '아동포르노, 폭력물, 성폭력, 범죄에 관한 자세한 지침, 약물 또는 마약 및 테러를 독려하는 내용의 자료'가 포함되며 이러한 컨텐츠는 ISP가 사전에 차단해야 한다는 것이다.(브로드밴드부 2009) 또한, 호주 통신미디어청(ACMA: Australian Communications and Media. Authority)에 등급거부컨텐츠 목록을 작성해 보관할 것을 제안했다. 이러한 목록에는 통신미디어청에 불만이 접수된 URL, 해외 관계당국이 보유하고 있는 아동포르노 사이트가 포함된다.[429]

2009년 위키리크스는 통신미디어청이 보유한 등급거부컨텐츠 목록을 발표했으며 2,395개 사이트가 목록에 올라있다고 주장했다.

"... 목록에 게재되어 있는 사이트 중 절반 이상은 아동 포르노와 관련이 없었으며 상당수는 온라인 포커 사이트, 유투브링크, 게이 또는 일반 포르노 사이트,

429) Department of Broadband, Communications and the Digital Economy 2009. Consultation paper: Mandatory internet service provider (ISP) filtering: Measures to increase accountability and transparency for Refused Classification material
http://www.archive.dbcde.gov.au/2013/july/transparency_measures/consultation_paper

위키피디아 항목, 안락사 사이트, 악마숭배, 주물숭배, 기독교 사이트 등 비주류 종교사이트 등이 포함되어 있으며 여행사와 퀸슬랜드주에 소재한 치과사이트도 포함되어 있다."[430]

하지만 미디어청의 이러한 제안은 정치적 공감대를 형성하지 못했을 뿐만 아니라 이에 반대하는 해커그룹 어나니머스가 호주연방의회 사이트 접속을 차단하는 'Operation Titstorm' 공격을 감행했었다. 인터넷 필터링에 대한 우려는 그 본질상 필터링이 검열이 될 수 있다는 것이었으며 기술적 한계 및 차단을 피해갈 수 있는 방법 등에 관한 것이었다. 인터넷 필터링에 대한 반대가 거세지자 브로드밴드국은 계획을 철회하였으며 주요 ISP(인터넷 연결의 90% 이상을 차지)는 인터폴에서 제공하는 블랙리스트(Worst of)를 이용해 아동 포르노를 자발적으로 차단한다는데 동의했고, 통신법에 따라 모든 ISP에 이러한 위해 사이트의 차단에 대해 고시하도록 했다고 발표했다.[431]

나. 온라인 컨텐츠 규제에 관한 통신법 s.313 적용

전술한 바와 같이 2012년 법 개정 이후 호주 ISP는 인터폴에서 제공하는 블랙리스트를 이용해 아동포르노물을 차단해오고 있다. 리스트에 올라 있는 사이트에 대한 접속 요청은 인터폴 웹사이트로 전송된다.[432] 2013년 2월 11일 러들럼 상원의원이 차단통지와 관련해 내무부 장관에게 한 질문을 보면 호주 연방경찰청은 인터폴 블랙리스트에 올라있는 도메인에 대한 접속을 차단하기 위해 통신법 제313조 제3항에 따라 통지서 또는 요청서를 21개 ISP에 발송했다. 2013년 1월 31 현재, 인터폴 블랙리스트에는 1,216개 사이트가 올라 있다.[433]

러들럼 상원의원은 상원 예산안 입법위원회(Senate Legislation Committees

430) Moses A 2009. Leaked Australian blacklist reveals banned sites. http://www.smh.com.au/articles/2009/03/19/1237054961100.html

431) Conroy S 2012. Media release: Child abuse material blocked online, removing need for legislation. http://www.minister.dbcde.gov.au/conroy/media/media_releases/2012/180

432) Parliament of Australia 2013. Question on Notice 2821. http://www.aph.gov.au/Parliamentary_Business/Chamber_documents/Senate_chamber_documents/qon/question?number=2821

433) Ibid, Parliament of Australia 2013.

considering Budget Estimates) 회의에서 한 추가 질문에서, “현재 우리가 알고 있기로는 차단 목적으로 제313조를 적용하는 기관은 단 세 곳뿐인 것으로 알고 있다”고 밝혔다(호주연방 2013a: 15). 먼저 호주 연방경찰청은 2004년 5월부터 멀링(muling), 피싱, 기타 멀웨어 사이트를 호스팅하고 있는 해외 IP 주소를 차단하기 위해 호주 최첨단사이버범죄센터의 합동 은행 및 재무팀과 당해 조항을 적용하고 있다(호주연방 2013b: 42). 하지만 제313조가 더 이상 원래의 목적을 위해 사용되지 않고 있음을 확인할 수 있었다.

그 이유는 IP 주소를 이용한 차단만으로는 부족하기 때문이다. 오랜 시간에 걸쳐서 유해 컨텐츠를 호스팅하는 사이트에 접속하고 원천적으로 이러한 사이트를 차단 및 폐쇄하고, 해외에서도 마찬가지로 도메인이 위치한 국가 및 회사와 공조하는 것이 훨씬 유용하는 사실을 알게 되었다. 다시 말해, 호주에서 단순히 차단만 하는 것보다는 훨씬 더 큰 효과를 볼 수 있다.[434]

두 번째 기관은 호주증권투자위원회(Australian Securities and Investments Commission)로 제313조를 적용해 ISP에 10차례에 걸쳐 특정 도메인에 대한 접속차단을 요청하였다.[435] 하지만 위원회의 도메인 차단요청은 후에 논란이 되었는데 그 이유는 약 1,200개 사이트를 “지나치게 차단(overblocked)”한 것으로 밝혀졌다. 세 번째 기관은 법무부내 기관으로 “국가 보안”을 이유로 이름은 밝혀지지 않고 있다[436]. 기관에 따르면 호주 연방정부는 통신법에 따라 통신감청이 허용되기는 하지만 수사당국이나 반부패기관 등 기타 국가, 주, 또는 지방 정부 기관이 통감법 제313조를 적용하는지 알 수 없다고 밝혔다.[437]

다. 호주 내 금지내용 게재 규제(prohibited material)

현재 호주는 컨텐츠를 관리되는 지역에 따라 두 가지 방법으로 규제하고 있다. 금지내용이 게재된 사이트가 호주 내에 위치한 경우 통신미디어청(ACMA)이

434) Ibid, Parliament of Australia 2013b. p.43.

435) Ibid, Parliament of Australia 2013a. p. p.15.

436) Ibid, Parliament of Australia 2013b. p.44.

437) Ibid, Parliament of Australia 2013.

직접 서비스 제공자에게 서버에서 해당 컨텐츠를 삭제하도록 한다. 호주 방송 서비스 법(Broadcasting Services Act 1992) 부칙 7에 따라 금지내용을 규제하고 있으며 여기에는 '등급거부(X 18+, R 18+)'도 포함되지만 단, 제한적으로 접근할 수 있으며 MA 15+은 상업 목적으로 게재할 수 있으나 단 제한적으로만 접근할 수 있다(예: 이용요금 징수).

라. 호주 외 지역의 금지내용 게재 규제

호주 외 지역에서 관리되는 사이트에 게재된 금지 컨텐츠와 관련해 통신미디어청은 "공인된 필터에게 금지 컨텐츠에 대한 자세한 내용을 알려주는데 이는 필터링을 통해 금지 컨텐츠에 대한 접속 차단"에 그 목적이 있다고 설명했다.[438]

4. iiNet 사건과 저작권 침해를 방지할 수 있는 ISP의 권한

2012년 호주 항소법원은 34개 호주 및 미국 영화산업관련 기업이 항소한 사건에 대해 제1심 법원의 원고 패소 판결을 유지했다. 당시 원고는 저작권법(the Copyright Act 1968)에 따라 호주 ISP인 iiNet을 상대로 소를 제기하였다. 원고는 iiNet이 자사의 고객이 P2P 파일공유 사이트인 비트토렌트 사이트에 접속하도록 허용함으로써 원고의 저작권을 침해했다고 주장했다(Roadshow Films Pty Ltd v iiNet Limited [2012] HCA 16)[439]. 당시 항소법원은 연방법원과 마찬가지로 iiNet의 손을 들어 주었다.

호주저작권보호연맹(Australian Federation Against Copyright Theft, 이하. 'AFACT'라 함)는 영화 및 텔레비전 프로그램 제작사 및 저작권자를 대표해 2008

438) Department of Broadband, Communications and the Digital Economy 2009. Consultation paper: Mandatory internet service provider (ISP) filtering: Measures to increase accountability and transparency for Refused Classification material http://www.archive.dbcde.gov.au/2013/july/transparency_measures/consultation_paper

439) http://www.hcourt.gov.au/assets/publications/judgment-summaries/2012/hcasum16_2012_0 4_20_iiNet.pdf

년부터 2009년까지 세 차례에 걸쳐 iiNet에 시정을 요구하는 공식서한을 보냈다. “저작권 침해 통보”라는 제목의 서한과 함께 iiNet의 고객명단을 함께 첨부했다. AFACT는 Dtecet Agent라는 프로그램을 이용하는 DtecNet Software APS를 고용했다. DtecNet Agent는 비트토렌트에 가입해 토렌트 파일을 공유한 고객의 IP 주소 등 고객관련 정보를 수집했다. 이후 수집한 정보를 저작권 침해 통보와 함께 iiNet에 전달하였으나 정보수집 방법에 대해서는 어떤 설명도 없었다. 하지만 iiNet은 이용자들의 계정 정지 또는 삭제 등의 조치를 취하지 않았다. 법원은 이 사건에 대해 다음과 같이 판시하였다.

“iiNet과 고객간에는 기술적으로 관계가 있지만 고객이 저작권법 s 86(c)를 위반하여 비트토렌트 시스템을 이용해 원고의 영화를 다운받음으로써 원고의 영화가 온라인상에 유포되는 결과를 초래하게 되었다 할지라도 iiNet이 이용자들의 저작권 침해를 기술적으로 방지하거나 예방할 수 있는 직접적인 권한은 없다 (Roadshow Films Pty Ltd v iiNet Limited [2012] HCA 16, 65)”.[440]

또한 법원은 “iiNet은 고객과의 계약관계를 철회함으로써 고객의 원고의 저작권 침해를 예방할 수 있는 간접적인 권한만을 가지고 있다”고 덧붙였다 (Roadshow Films Pty Ltd v iiNet Limited [2012] HCA 16, 78). 항소법원이 iiNet의 DPI 사용을 비트토렌트 감지, 차단 또는 속도 제한 등을 위한 향후 기술적 조치로 본지 않았기에 사생활보호법에 따른 개인정보보호원칙(NPP) 1.1의 적용은 심리하지 않았다.

5. 텔스트라(Telstra)의 트래픽 관리 및 DPI 실험

2013년 2월 호주 최대의 인터넷 서비스 제공자인 텔스트라는 빅토리아 주내 일부 고객을 대상으로 네트워크 관리를 시범운영할 계획이라고 발표했다. 특히 시범운영에는 ‘특정한 상황, 특정 시간대, 특정 서비스(비트토렌트를 포함해 일

440) http://www.afr.com/rw/2009-2014/AFR/2012/04/20/Photos/f5b0c2ee-8a80-11e1-b8f3-89181177a90a___www.austlii.edu.au_au_cases_cth_HCA_2012_16.pdf

부 P2P 트랙픽 타입)'의 속도 최적화를 위한 DPI 사용이 포함되었다. 다음은 텔스트라의 발표 내용이다.

텔스트라는 네트워크의 다양한 트래픽타입에 맞게 관리할 수 있는 네트워크 방법을 현재 시중이다. 현재 사용되는 현재 트래픽의 형태를 파악하기 위한 데이터 패킷 감청 기술의 특성을 중점적으로 살펴볼 것이다. 다시 말해, 트래픽의 형태를 알기 위해 각각의 패킷의 특성을 알아 볼 것이지만 그 내용을 살펴보지는 않을 것이다. 이를 통해 예를 들면, P2P 등 패킷의 종류를 파악할 것이지만 패킷에 포함되어 있는 어떠한 정보나 컨텐츠에 대해서 알지도 못하거니와 기록도 하지 않을 것이다.

텔스트라는 이번 시범운영의 목적이 네트워크 혼잡을 해결하기 위한 것으로 저작권을 침해하거나 저작권 침해 관련 정보를 수집하는데 있지 않다고 밝혔다. 망 중립성에 관한 질문에 대하여 텔스트라는 다음과 같이 답했다.

호주의 이동통신 상황은 미국과 매우 다르다. 미국은 인프라 접속과 관련해 규제가 없는데 이는 미국의 인터넷 서비스 제공자가 고객의 요구에 부적합한 네트워크 관리 실무를 채택할 경우 소비자가 택할 수 있는 대안이 거의 없게 된다.

호주의 경우, 접속 규제는 고객이 다양한 네트워크 관리 실무를 시행하고 있는 수많은 ISP 중 원하는 제공자를 선택할 수 있음을 말한다. 경쟁을 통해 ISP는 고객의 요구에 부합하는 최상의 네트워크를 제공하게 된다. 호주의 ISP가 고객의 요구나 관심에 부합하지 않는 네트워크 관리 실무를 채택한다면 고객은 자신의 의지에 따라 다른 ISP로 이동할 것이다.

호주처럼 접근 시스템을 갖춘 국가들(예: 영국)은 대부분 이러한 ISP의 실무 규제의 필요성을 고객보호를 위한 시장 규제로 보지 않는다.

호주 정책입안자와 네트워크 운영자에게 가장 중요한 것은 고객이 구매하는 네트워크에 대해 고객이 정보를 바탕으로 최상의 결정을 내릴 수 있도록 네트워크를 효율적이고 투명하게 관리하는데 있다.

텔스트라는 고객이 요구에 가장 부합하는 상품과 서비스를 고객이 스스로 선택할 수 있도록 모든 정보를 제공하기 위해 노력하고 있다.[441]

441) Telstra 2013. Trialling new network management techniques - Myth buster.

6. iCode 및 호주 인터넷 보안 계획(Australian Internet Security Initiative, AISI)

호주인터넷보안계획(AISI, 이하 보안계획이라 함)는 처음 통신미디어청이 수립하였으며 2005년 시범운영을 시작하였고 이듬해 인 2006년부터 확대되었다. 보안계획은 호주 내 인터넷에 접속하는 악성봇에 감염된 컴퓨터의 IP 주소를 확인하고 고객의 문제 해결을 위한 지원 제공을 위해 ISP에 이와 관련된 정보를 제공하는데 있다. 보안계획의 주요 기능은 호주 내 일명 '보트넷' 활동을 억제하는데 있다. 보안계획은 자발적 참여를 원칙으로 하고 있으며, 2013년 9월 현재 ISP와 16개 대학을 포함해 134개 기관이 참여하고 있다. 보안계획은 직접적으로 감염된 컴퓨터의 활동을 파악하거나 인터넷 트래픽 및 패킷을 감시하지는 않는다. 일부정보는 Shadowserver Foundation, 호주 Honeynet Project, SORBS[442]에 의해 잘 알려진 소스 리스트에서 수집된다. 통신미디어청은 다른 소스에서 악성소프트웨어에 감염된 것으로 보이는 컴퓨터를 파악하는데 있어서는 거의 아무런 정보도 제공하고 있지 않다.

2013년 5월 현재, 12개 소스가 보안계획에 정기적으로 수집한 데이터를 제출하고 있다. 이들 소스가 제공하는 데이터의 양은 단 몇 개에서 수천에 이르기까지 차이가 많다. 입수가 가능하게 되면 다른 소스도 포함되며 신뢰할만한 정보로 판단되고 있지만 다른 소스의 경우 시간이 지나면서 수가 줄어들거나 사라지고 있다.[443] 보안계획에 참여하는 ISP에 보고된 감염 컴퓨터의 수는 증가 추세에 있는데 2009-2010년에는 일일 평균 11,215대가 보고되었으나 2010-2011년에는 16, 464, 2011-2012년 16,571로 증가했다.[444]

보안계획의 두 번째 주요 기능은 호주 인터넷에 영향을 미치는 스팸메일에 대한 데이터베이스를 구축하는 것이다.[445]. 외부 소스를 이용해 스팸메일을 지속

---

http://exchange.telstra.com.au/2013/02/08/telstra-broadband-experience-trial-mythbuster/

442) Matthews B 2011. *International Training Program 2011: The Australian Internet Security Initiative*: Australian Communications and Media Authority. http://www.acma.gov.au/webwr/_assets/main/lib100656/4.2australian_internet_security_initiative%28bruce_matthews%29.pdf

443) Australian Communications and Media Authority (ACMA) 2013a. Communications report 2011–12. http://www.acma.gov.au/webwr/_assets/main/lib550049/comms_report_2011-12.pdf

444) Australian Communications and Media Authority (ACMA) 2011,2011, 2012

적으로 수집한다. 이러한 스팸메일의 상당수는 호주 내 알려지지 않은 피해자의 감염된 컴퓨터에서 악의적으로 발송되는 것으로 보고 있다. 또한 수집된 이메일에는 호주 IP를 타겟으로 하는 것들도 있다. 보안계획은 외부 소스에서 수집한 스팸메일을 수집하는데 있어 사후 대응하는 역할을 하지만 호주 국민의 개인메일에 접근할 수 있는 권한은 갖고 있지 않다.

보안계획을 보완하고자 호주인터넷산업협회(Internet Industry Association of Australia, IIA)가 ISP를 위해 iCode를 개발하였다. 2010년 시작된 iCode에는 ISP가 감염된 컴퓨터에 대해 보안계획으로부터 통지를 받았을 때 서비스약관에 따라 시행할 수 있는 방법을 포함하고 있으며 그 중 일부는 다음과 같다.

(a) 고객에게 직접 연락(전화, 이메일, 문자 또는 기타 방법)
(b) 고객이 지원센터에 연락하도록 고객 계정의 비밀번호를 재설정해 지원 서비스에 직접 연결
(c) 고객의 인터넷 서비스 속도를 최적화하는 '남용' 계획 시행
(d) 일시적의 고객의 서비스 차단, 예를 들면 '자사의 폐쇄망(walled garden)'과 같이 통제된 환경에 두고 감염된 컴퓨터의 보안 시스템을 복구할 때까지 지원을 제공할 수 있는 관련 시스템 링크 제공
(e) 스팸메일의 출처인 경우, 메일발송 제한(간이 전자 우편 전송 프로토콜(Simple Mail Transfer Protocol, SMTP), 및
(f) ISP의 이용약관에 따른 기타 조치[446]

iCode의 원칙은 다음을 포함한다.

실무적인 부분에 있어 "전자평등(electronic equivalence)"이 실현되어야 한다(전자평등이란 현실세계에서 이루어지는 행위 및 거래는 추가적인 요건이나 제한 없이 인터넷상에서도 이루어져야 함을 의미한다). [중략] 고객의 프라이버시가 가장 중요하다.[447]

---

445) Matthews B 2011. *International Training Program 2011: The Australian Internet Security Initiative*: Australian Communications and Media Authority. http://www.acma.gov.au/webwr/_assets/main/lib100656/4.2australian_internet_security_initiative%28bruce_matthews%29.pdf

446) Internet Industry Association 2010. iCode. p.9 http://iia.net.au/userfiles/iiacybersecuritycode_implementation_dec2010.pdf

보안계획 및 기타 “신뢰할 수 있는 제3의 소스”로부터 보고서를 받는 것 외에 iCode에 따라 악성활동 및 감염된 컴퓨터를 알아내기 위한 방법으로는 “고객의 컴퓨터가 감염된 것으로 보이는 IP 주소의 비정상적인 트래픽 패턴을 파악하기 위한 네트워크 관리” 등이 포함된다(인터넷산업협회 2010년 8월). iCode에서 명시하고 있는 네트워크 관리는 다음과 같다.

고객의 컴퓨터가 감염되었는지 파악하는데 있어 ISP는 현재의 업무기준 및 재원을 활용할 것을 권고한다. 다음과 같은 방법을 포함하나 이에 국한하지는 않는다.

(a) 큐에 쌓인 메일 및 비정상적인 네트워크 트래픽 또는 알려져 있는 보트/악성 활동 검토
(b) 수신(ingress)와 발신(egress) 주소 유효성 및 스팸체크
(c) 게이트웨이 IPS/IDS
(d) 내부 보안벽 시스템
(e) 잘 알려진 전송 제어 프로토콜(Transmission Control Protocol, TCP) 및 UDP 포트 번호를 이용하는 악성코드 트로이목마/바이러스를 파악하는데 사용되는 내부 시스템
(f) 고객의 신고[448]

7. 통신사의 데이터보존 의무화 제안

2013년 호주연방 정보 및 보안 합동위원회는 통신사의 데이터보존 의무화 제도에 대한 자체 의견을 발표했다. 호주 법무부는 유럽연합 데이터보존 지침을 따라 최대 2년간 통신데이터를 보존하도록 하는 제안과 관련해 이에 대한 의견을 요청했다. 통신사 데이터는 다음과 같이 정의할 수 있다.

통신데이터는 통신과정에 대한 정보로 그 내용과는 별도로 한다. 이러한 정보는 발신자와 수신자의 신원, 관련 가입자 정보, 통신사 또는 인터넷 서비스 제공

447) Ibid, Internet Industry Association 2010. p.7
448) Ibid, Internet Industry Association 2010. p.14

자가 계정을 만들 때 수집한 정보를 확인할 수 있는 계정 식별정보 및 통신 시간, 일자, 기간, 위치 및 형태를 포함한다.[449]

위원회는 프라이버시, 자유권, 보존해야 할 데이터의 보안, 가능성, 실용성 및 비용을 고려해 제안을 검토했다. 특히 프라이버시, 수사당국 및 보안기관의 권한 확대와 관련해 우려가 제기되었다. 특히 통신사의 정보 보존 제안이 사생활 보호법(Privacy Act 1988)에서 명시하고 있는 개인정보보호원칙 1.1을 위반한다는 우려의 목소리가 컸다. 전술한 바와 같이 개인정보보호원칙 1.1은 개인정보가 이러한 기관의 하나 또는 그 이상의 기능 또는 역할을 수행하는데 있어 반드시 필요한 경우를 제외하고는 개인정보 수집을 금하고 있다.

텔스트라는 ISP가 통신데이터를 캡처하고 보유해야 한다 할지라도 "스카이프와 기타 인터넷 전화 서비스를 이용하는 기타 음성서비스, 유투브, 또는 구글"의 데이터는 캡처할 수 없다고 했다. 텔스트라는 또한 "텔스트라가 데이터풀에 포함되지 않는 정보를 추가로 요청할 경우 데이터정보 보존 의무를 이행할 수 있는 현실적으로 가능한 방법은 DPI이다"라고 덧붙였다. 법무부에 따르면 별도 서비스와 관련해 미국의 인터넷 서비스 제공자는 사법공조조항에 따라 보존하고 있는 정보에 접근할 수 있다.[450]

마지막으로 위원회는 아직까지 그와 관련해 입안된 법률안이 없기 때문에 검토가 제한적으로 이루어질 수밖에 없다고 설명했다. 데이터 보존 의무화가 국가안보와 법집행에 있어 커다란 혜택을 가져다 줄 수 있다고 하면서도 다음과 같이 언급했다.

데이터 보존 의무화 제도는 근본적으로 프라이버시 침해 문제를 야기할 수 있고, 논란이 되고 있는 바와 같이 시민에 대한 국가의 권한 확대로 이어질 수 있다. 따라서 프라이버시와 시민의 자유권에 대한 우려가 해소되지 않는다면 이러한 제도를 수립해서는 안 된다.[451]

통신사의 데이터 보존을 의무화할지에 대해 위원회는 "데이터 보존 의무화와

449) Parliament of Australia Joint Standing Committee on Treaties 2013, p.140.

450) Ibid, Parliament of Australia Joint Standing Committee on Treaties

451) Ibid, Parliament of Australia Joint Standing Committee on Treaties

관련해 위원회 내에서도 의견이 분분하다. 이는 정부의 결정에 달려있다. 정부가 데이터 보존 의무화를 진행해야 한다고 판단하면 위원회는 정부에 입법안을 공개하고 검토를 위해 입법안을 호주연방 정보 및 보안 합동위원회에 제출할 것"을 권고한다. 입법안은 다음의 내용을 포함하여야 한다.

- 데이터 보존 의무화 제도는 통신데이터인 메타데이터에만 적용하며 통신 컨텐츠 즉, 내용은 포함하지 않는다.
- 통신 데이터 접근에 대한 규제는 현재 제도와 동일하게 유지한다.
- 인터넷 브라우징 데이터는 분명히 제외한다.
- 정보에 데이터와 분리할 수 없는 컨텐츠가 포함되어 있는 경우 해당 정보는 컨텐츠로 간주하며 합법적으로 해당 정보에 접근하려면 반드시 영장을 발부 받아야 한다.
- 암호화를 의무화해 데이터를 안전하게 저장한다.
- 2년 이상 데이터를 관련 기관이 보존할 수 있도록 허용하는 규정을 제외하고 새로운 제도에 따라 보존해야 할 데이터는 2년 이상 보존해서는 안 된다.
- 정보 보존에 따라 ISP에 발생하는 비용은 정부가 지급한다.
- 위반 사례에 대한 통지를 의무화한다.
- ISP가 통신 컨텐츠를 저장하지 않도록 관련 기관 내에 독립적인 감사기능을 부여하여야 한다.
- 옴부즈맨과 정보 및 보안 합동위원회의 감사관이 기관의 통신 데이터 접근을 감독한다.

위원회의 보고서가 발표된 후 법무부는, "정부는 현재 데이터 보존 의무화를 추진할 계획이 없으며 관련 부처와 기관의 권고를 종합해 결론을 내릴 것"이라는 성명서를 발표했다. 하지만 2013년 연방선거 이후로 의무화 계획이 연기될 것이라는 추측만이 있다.[452]

452) Hutchinson J 2013. Dreyfus delays data retention after committee indecision. http://www.afr.com/p/technology/dreyfus_delays_data_retention_after_FuIjuqFrH5NvYp7Rv77xpK

8. 호주의 망 중립성과 컨텐츠 관련 경쟁

2010년 경쟁 및 소비자 보호법(Competition and Consumer Act 2010)은 경쟁과 공정거래를 촉진하며 호주 보호자 보호를 명시하고 있다. 이 법은 부속서 XIPB에 통신사의 경쟁에 관한 구체적인 조항을 포함하고 있다. 이 법에 따라 호주 경쟁 및 소비자 위원회는 운영자에게 반경쟁 행위에 대해 경고장을 발부하고 위반행위가 계속될 경우 벌금을 부과할 수 있는 권한을 갖고 있다. 당해법은 반경쟁 행위에 관한 것이지만 망 중립성에 대한 명백한 규정은 포함하고 있지 않다.

하지만 Taylor는 인터넷 서비스 제공자의 묶음 또는 무제한 데이터 제공이 시장의 경쟁을 약화시키는 것으로 판단될 경우 경쟁 및 소비자 보호법은 잠재적으로 망 중립성(특히, 이용자의 데이터 권한에 포함되지 않는 '무료' 컨텐츠 관련)에 적용할 수 있다고 주장하고 있다.

예를 들면, 텔스트라의 가입자에 대한 스포츠 생중계 무제한 접속 제공이 프리미엄 서비스에 제한되어 있고 텔스트라의 비가입자에 대한 차별의 방법으로 사용된다면 이에 대해 이법을 적용할 수 있다.[453]

2011년 설립된 통합심사위원회(Convergence Review Committee)는 호주의 미디어와 커뮤니케이션 규제 내용을 점검하는 역할을 해 왔다. 위원회는 네트워크 관리 실무가 경쟁을 제한하고 혁신을 위협하고 있다고 우려했다. 위원회는 호주 경쟁 및 소비자 위원회의 권한이 망 중립성, 프리미엄 컨텐츠 접속, 컨텐츠와 통신 서비스 묶음 또는 무제한 서비스 제공과 같은 컨텐츠와 관련한 문제를 해결하기에는 너무 협소하다고 밝혔다. 위원회는 "경쟁을 저해하는 독점판매권 및 묶음 서비스, 망 중립성 문제 등 발전하는 컨텐츠 관련 문제를 해결하기에는 위원회의 권한이 너무 협소하다"고 설명했다.[454]

위원회는 호주 통신미디어청을 대신할 새로운 통신규제당국을 설립할 것을 권고했다. 특히 컨텐츠 관련 경쟁에 대해서는 관련 산업에게 명확한 가이드라

453) Taylor C 2012. 'Content is king': using the Competition and Consumer Act to regulate 'net neutrality' and access to content in Australia. http://www.ibanet.org/Article/Detail.aspx?ArticleUid=8560d015-62b7-4dc3-8dcf-fa3e883fcd68

454) Parliament of Australia Joint Standing Committee on Treaties 2012, p.29.

인을 제공하는 규칙을 제정하는 동시에 새로운 쟁점에 대응할 수 있는 권한을 갖는 새로운 통신규제당국의 신설을 권고했다. 권고안의 내용을 살펴보면 다음과 같다.

새로운 통신규제당국에게 컨텐츠 경쟁과 관련해 문제점이 파악되면 시장 조사 지시 및 조사 수행권한을 비롯해 컨텐츠 시장에서 공정하고 효과적인 경쟁을 촉진할 수 있도록 유연한 규칙제정 권한을 부여하여야 한다. 이러한 권한은 호주 경쟁 및 소비자 위원회의 시장의 반경쟁행위를 시정할 수 있는 권한을 보충하는 것이어야 한다. 또한 이러한 권한은 공개조사를 실시한 이후에만 행사할 수 있어야 한다.[455] 하지만 위원회의 권고에 대한 정부의 반응은 이러한 권고사항을 고려하지 않은 것으로 보인다.[456]

455) lbid, Parliament of Australia Joint Standing Committee on Treaties 2012, p.28.

456) Conroy S 2013. Convergence Review and Finkelstein Inquiry. http://www.minister.dbcde.gov.au/conroy/media/speeches/2013_-_minister_speeches/005
Convergence Review Committee 2012. Convergence Review Final Report. Canberra: Commonwealth of Australia. http://www.dbcde.gov.au/__data/assets/pdf_file/0007/147733/Convergence_Review_Final_Report.pdf

9. 요약 및 정리 – 망 중립성 및 통신비밀 관련 입법 내용

다음의 표는 호주의 망 중립성 및 통신비밀에 관련 입법내용으로 본 보고서에서 전술한 사항을 요약하였다.

표 4 호주의 망 중립성 및 통신비밀에 관한 입법 주용 내용

입법	관련 조항	요약	운영부처
통신법(Telecommunications Act 1997)	s.313	ISP는 감청 영장, 저장된 통신기록 영장 또는 국내 및 해외 통신기록 보존 통지 준수	브로드밴드통신경제개발부
통신감청 및 접근법(Telecommunications (Interception and Access) Act 1979		통신감청 영장 저장된 통신기록 접근 영장 국내 및 해외 통신기록 보존 통지 통신데이터 접근	법무부
감시장치법(Surveillance Devices Act 2004)		데이터 감시장치 사용 영장	법무부
사생활보호법(Privacy Act 1998)	부칙 3	조직은 개인정보를 수집하여서는 안 된다. 단 개인정보가 이러한 조직의 하나 또는 그 이상의 기능 또는 역할을 수행하는데 있어 반드시 필요한 경우는 제외한다.	법무부
방송서비스법(Broadcasting Services Act 1992)	부칙 5, 부칙 7	불법 및 유해 컨텐츠 규제	브로드밴드통신경제개발부
경쟁 및 소비자 보호법(Competition and Consumer Law Act 2010)	별첨 XIB	경쟁 및 공정무역 촉진 및 소비자 보호	브로드밴드통신경제개발부 호주 인프라 및 교통부 호주 혁신산업과학연구부 재무부 산업, 혁신, 기후변화, 과학, 연구, 고등교육부

제4장

트래픽 관리의 정당화 가능성과 한계

전 현 욱

04

트래픽 관리의 정당화 가능성과 한계

제3장에서는 국외의 망 중립성 정책 관련 논의들을 포괄적으로 검토해 보았다. 망 중립성 원칙을 둘러싼 각국의 논의들로부터 이른바 망 관리의 수단으로서 선별적 접속 차단이 침해하는 개인의 권리에 대한 우려와 규범적 논증을 확인할 수 있었다. 또한 동시에 망 관리를 통해 우리가 얻을 수 있는 것이 무엇이며, 특히 인터넷 접속 서비스 제공자가 얻고자 하는 것이 어떠한 것인지를 볼 수 있었다. 이러한 논의들은 직간접적으로 망 중립성 제한행위의 정당화 가능성에 대한 논거가 된다.

이하에서는 통신비밀보호법상 불법감청 구성요건에 해당하는 행위가 망 관리를 위해서 현실적으로 어디까지 정당화될 수 있는지를 형사정책적 관점에서 검토하고, 이를 바탕으로 합리적인 트래픽 관리의 기준과 정당한 망 중립성 정책의 규범적 근거를 제시하고자 한다. 이를 위해 우선 통신비밀보호법 제2조 제7호가 정의하고 있는 감청의 개념 중 "동의"에서부터 정당화 가능성에 관한 논의를 시작하고자 한다.

제1절 동의를 통한 불법 조각 가능성

통신비밀보호법 제2조 제7호는 "동의"의 부존재를 감청의 개념표지로 명시하고 있다. 그러므로 피감청자가 통신제한조치에 동의하는 경우 통신의 내용을 지득 또는 채록하거나 전기통신의 송·수신을 방해해도 통신비밀보호법상 감청죄의 불법은 성립하지 않는다. 본래 감청 또는 통신제한조치는 너무나 당연하게도 피감청자의 의지에 반할 것을 전제로 하는 행위이다. 그러므로 법률에 동의의 부재를 요건으로 명시하였는지 여부와 상관없이, 동의는 당연히 감청행위의 불법을 조각한다고 할 것이다.

통신비밀보호법의 구조상 감청 동의는 일단 구성요건 해당성 배제사유인 것으로 보인다. 그러나 그 요건을 구체화하기 위해 감청 동의가 형법이론적으로 구성요건 해당성을 배제하는 양해에 해당하는지, 아니면 위법성을 조각하는 피해자의 승낙에 해당하는지를 분명히 할 필요가 있다. 양자를 구별하는 형법이론에 따르면 양해와 피해자의 승낙은 요건과 효력에 있어서 다소 차이가 있다고 볼 수 있기 때문이다. 또한 양해에 해당하는 것으로 본다 하더라도 개념의 일반적인 실질이 명확하지 않은 양해의 요건을 구체화하기 위해서는, 법률의 규정에 근거하고 있으며 학계와 실무에서 이미 오랜 시간동안 그 요건과 한계가 명확해진 피해자의 승낙과 비교하여 검토하는 것이 보다 용이한 방법이 될 것으로 보인다.

이러한 검토를 토대로 현재의 통신시장에서 인터넷 서비스 제공자와 일반 가입자의 현실적 관계를 고려할 때 관행적으로 이루어지고 있는 약관을 통한 동의가 불법을 조각할 수 있는 적법한 동의방법이 될 수 있을 것인지에 대해서도 살펴본다. 이를 위해 구체적으로 논의의 대상이 되는 진지한 법익처분에 대한 자기결정[457]의 요건을 검토한다. 가입자는 DPI 등 선별적 인터넷 접속 차단에 이용되는 기술의 작동 원리를 정확하기 모르기 때문에, 이로 인해 침해될 수 있는 자신의 권리의 실질에 관하여 제대로 인지하지 못하는 경우가 대부분이다. 뿐만 아니라 기술의 실제 활용은 통신 서비스 제공자가 전적으로 장악하고 있는 통신

457) 김성규, 피해자의 승낙에 관한 법리로서의 자기결정권, 비교형사법연구 제8권 제1호, 2006, 25쪽.

망에서 이루어지며, 가입자는 그 내용을 전혀 알 수 없다. 따라서 인터넷 이용자에게 요구되는 인식의 정도 및 동의할 내용에 관한 인터넷 서비스 제공자의 설명의무 여부에 대하여 상세하게 논하고자 한다.

1. 동의의 형법적 의미 - 양해와 승낙의 구별

통신비밀보호법상 통신제한조치는 논리적으로 피제한자의 의사에 반할 것을 필수적인 요건으로 하고 있으므로, 동의가 있으면 처음부터 불법감청의 구성요건에 해당하지 않는 행위가 된다. 따라서 감청 동의는 해석상 위법성 조각사유라기 보다는 구성요건 해당성을 배제하는 것으로 볼 수 있을 것이다. 이러한 관점에서 정보이용동의의 경우 위법성 조각사유인 피해자의 승낙보다 훨씬 완화된 요건으로도 구성요건 배제의 효력을 인정할 수 있다는 견해가 있다.[458] 하지만 양해의 요건에 대해서는 이를 인정하는 학자들간에도 다소 견해의 차이가 있으며, 따라서 양해에 해당한다는 이유만으로 감청 동의에 대하여 완화된 요건기준을 요구하는 것이 정당한 것인지에 대해서는 보다 상세한 논의가 필요할 것으로 생각된다. 피감청자의 동의는 통신의 비밀에 대한 법적 보호를 스스로 포기하는 것이라는 점에서 형법 제24조가 규정하고 있는 피해자의 승낙과 유사성을 인정할 수 있다. 그러므로 이 보고서에서는 형법 총론의 규정에 근거한 피해자의 승낙과 이론을 통해 인정되는 양해와 관련하여 현재 형법학계에서 논의되고 있는 이론들을 살펴본다.

이를 위해서 우선 피해자의 승낙과 양해에 관련된 기본이론을 간략하게 정리하고, 학계에서 논의되는 사항을 감청에 대한 동의에 적용하여 이를 법문의 규율 형태를 고려하여 양해로 볼 것인지 아니면 체계적 해석상 특히 피해자의 승낙으로 보아야 할 것인지를 검토한다. 무엇보다도 승낙과 양해를 구별하는 견해에 따르면 통신 서비스 약관 해당 사안에 동의를 하는 것이 승낙인지, 양해인지

458) 개인정보보호법상 정보이용동의에 관하여 요건이 완화된 양해의 법리가 적용되어야 한다는 견해로 전응준, 개인정보보호법률상 형사처벌규정의 적정성에 관한 연구, 정보법학, 제17권 제2호, 226쪽. 그러나 이 논문은 양해의 개념을 이해하는데 있어 이 보고서와 다른 견해를 가지고 있다.

에 따라 그 유효요건을 다르게 볼 수도 있으므로, 양자의 구분은 동의의 요건을 판단함에 있어 실질적인 차이로 연결될 가능성이 있다. 또한 감청 동의를 양해로 보는 처음의 판단을 유지하는 경우라 하더라도 피해자의 승낙과의 비교는 양해 요건을 구체화하는데 도움이 될 것이다. 양해와 승낙을 구별하지 않는 견해 또는 양자를 구별하더라도 각각의 구성요건별로 구체적인 경우를 따져보아야 한다는 견해에 따르면 결국 피감청자의 적절한 법익처분이 있었는지 여부가 유효한 동의 여부를 판단하는 기준이 될 것이다.

가. 형법 제24조의 해석론

피해자의 승낙은 피해자가 가해자에게 자기법익에 대한 침해를 허락하는 경우 그 가해행위의 형법상 불법을 배제시키는 제도로, 형법 제24조에 규정되어 있다.[459] 제24조는 "처분할 수 있는 자의 승낙에 의하여 그 법익을 훼손한 행위는 법률에 특별한 규정이 없는 한 벌하지 아니한다"고 규정하여 처분권자의 승낙이 법익침해의 불법을 조각함을 명백히 하고 있다. 이 조항의 해석에 있어 피해자의 승낙을 다섯 가지 위법성 조각사유 중 하나로 이해하는 것이 통설적 입장이다. 다만 피해자의 승낙을 법익의 포기로 보아 구성요건 해당성이 배제된다고 보는 입장도 있다. 구성요건 배제사유설에 따르면 피해자의 승낙은 법익을 적법하게 처분할 수 있는 권한을 가진 자가 법익의 보호를 애당초 포기한 경우, 행위자의 행위가 형법적으로 의미 있는 것인지가 문제가 되며, 이는 결국 결과반가치 및 행위반가치가 없는 행위로 보아야 하기 때문에 국가 형벌권이 관여할 필요 자체가 사라진다고 한다.[460]

그러나 우리 형법은 피해자의 승낙에 관한 규정이 없는 독일 형법과는 달리 피해자의 승낙에 대한 명시적인 규정을 갖고 있으므로 위와 같은 해석의 여지는 없을 것으로 보인다. 우리 형법상 피해자의 승낙은 위법성 조각사유인 정당행위(제20조), 정당방위(제21조), 긴급피난(제22조), 자구행위(제23조)에 바로 연이어 규정되어 있으므로 체계상 위법성 조각사유로 보는 것이 타당하다. 승낙이 구성

459) 상세한 이론적 해설은 배종대, 형법총론, 제11판, 2013, 78/1 이하 참조.
460) 김일수/서보학, 새로쓴 형법총론, 제11판, 박영사, 2006, 252쪽.

요건 해당성 배제사유라면 구성요건 배제사유설의 논리처럼 국가 형벌권이 관여할 필요가 없으므로, 법률에 명시할 필요도 없을 것으로 생각한다.[461] 판례는 형법 제24조를 위법성 조각사유로 해석한다.[462]

나. 양해와 승낙의 구별

1) 양해 개념의 인정 필요성에 대한 견해 대립

그러나 통설과 판례에 따라 형법 제24조를 위법성 조각사유로 보는 견해를 취한다 하더라도, 현실적으로 피해자가 법익침해에 대하여 동의하는 경우 애초에 구성요건에 해당한다고 할 수가 없는 경우가 있다는 사실을 부정해야 하는 것은 아니다. 오히려 대부분의 학자들은 적극적으로 이러한 경우를 인정한다. 그러므로 결국 피침해자의 동의는 구성요건 해당성을 배제하는 경우와 위법성을 조각하는 경우로 나뉘게 된다. 피해자의 의사에 반할 것이 당연히 전제되어있는 구성요건, 예컨대 절도죄나 강간죄의 경우, 피해자의 동의는 당연히 구성요건 해당성을 배제하는 것으로 해석된다. 이때 형법학계에서는 특히 구성요건 해당성을 배제하는 동의를 양해라는 용어로 부르기도 한다. 정리하자면, 위법성 조각사유로서 피해자의 승낙과 구성요건 해당성 배제사유로서 양해를 구분하는 것이 현재 우리나라 형법학계의 다수설이라고 할 수 있다.[463] 그러나 양해에 관하여,

---

461) 구성요건 배제사유설과 위법성 조각으로 해석하는 통설의 논리에 대한 정리는 권오걸, 피해자의 승낙과 양해, 법학논고 제20집, 2004, 5-6쪽 참조.

462) 산부인과 전문의 수련과정 2년차인 의사가 자신의 시진, 촉진결과 등을 과신한 나머지 초음파검사 등 피해자의 병증이 자궁외 임신인지, 자궁근종인지를 판별하기 위한 정밀한 진단방법을 실시하지 아니한 채 피해자의 병명을 자궁근종으로 오진하고 이에 근거하여 의학에 대한 전문지식이 없는 피해자에게 자궁적출술의 불가피성만을 강조하였을 뿐 위와 같은 진단상의 과오가 없었으면 당연히 설명 받았을 자궁외 임신에 관한 내용을 설명 받지 못한 피해자로부터 수술승낙을 받았다면 위 승낙은 부정확 또는 불충분한 설명을 근거로 이루어진 것으로서 수술의 위법성을 조각할 유효한 승낙이라고 볼 수 없다.(대법원 1993. 7. 27. 92도2345); 피고인이 계원들로 하여금 공소외 (갑)대신 피고인을 계주로 믿게 하여 계금을 지급하고 불입금을 지급받아 위계를 사용하여 공소외 (갑)의 계운영업무를 방해하였다고 하여도 피고인에 대하여 다액의 채무를 부담하고 있던 공소외 (갑)으로서는 채권확보를 위한 피고인의 요구를 거절할 수 없었기 때문에 피고인이 계주의 업무를 대행하는데 대하여 이를 승인 내지 묵인한 사실이 인정된다면 피고인의 소위는 이른바 위 공소외 (갑)의 승낙이 있었던 것으로서 위법성이 조각되어 업무방해죄가 성립되지 않는다.(대법원 1983. 2. 8. 82도2486)

애초에 형법적 고려의 대상조차 되지 않은 행위에 대하여 구성요건 해당성을 가설적으로 설정해놓고 다시 이를 제거하기 위하여 양해라는 개념을 인정하는 것에 전혀 실익이 없다는 이유로 이를 부정하는 견해도 있다.[464]

그러나 양해의 개념을 부정하는 견해도, 피해자의 승낙, 즉 법익 침해에 대한 동의 있는 경우 구성요건 해당성 자체가 배재되는 경우가 없다는 의미는 아니다. 다만 이러한 현상에 주목하여 별도의 용어를 만들고 이론적으로 검토하는 데에 아무런 실익이 없다는 뜻이다. 양해를 인정하는 다수설에 따르더라도 양해가 성립하기 위한 요건은 구성요건의 실질에 따라 달라질 수밖에 없기 때문에[465] 양해라는 개념은 객관적인 실질이 없으며, 구성요건 해석을 위한 논증의 수단이 될 수도 없다. 게다가 처벌되지 않는다는 점에서 피해자의 승낙과 실제 그 법적 효과면에서 차이가 없기 때문에, 법률에도 없는 용어를 일부러 도입할 필요가 없다는 지적인 것이다.

학설에 따르면, 양자의 법 효과적 차이는 오상 피해자의 승낙, 즉 피해자의 승낙이 없었음에도 불구하고 있었던 경우로 착오한 행위에 대하여 위법성 조각사유의 객관적 전제사실에 관한 착오에 대하여 엄격책임설을 취하는 견해를 따라 고의범을 인정하는 경우에만 실질적인 의미가 있다. 양해가 없었음에도 불구하고 있었던 것으로 착오하는 경우라면 사실의 착오로 보아 고의가 없으므로 주의의무 위반이 있으면 과실범이 성립하는 것으로 보는 것이 논리적이기 때문이다.[466] 그러나 이러한 분석은 지나치게 교과서적일뿐만 아니라, 최소한 이 보고서의 목표인 통신비밀보호법상 감청을 정당화시킬 수 있는 동의의 요건을 구체화하는데 아무런 도움도 주지 않는다.

---

463) 구별설이 다수설이라는 점에대한 정리는 손동권, 양해·승낙의 구분에 따른 구체적 법 효과 차이의 문제, 형사법연구 제23권 제3호, 2011, 89-90쪽.

464) 배종대, 형법총론, 제11판, 홍문사, 2013, 80/1-4.

465) 사기죄의 양해는 착오가 없어야 하지만 절도죄의 경우는 그렇지 않다. 배종대, 형법총론, 제11판, 홍문사, 2013, 80/3.

466) 손동권, 양해·승낙의 구분에 따른 구체적 법 효과 차이의 문제, 형사법연구 제23권 제3호, 2011, 100-101쪽.

2) 양해와 피해자의 승낙의 요건 차이

그러나 양해와 승낙의 성질상 차이에 따라 생기는 차이점에 대한 논의는 이 보고서의 논의를 위하여 다소 의미가 있다. 양해를 순수한 사실적 성격을 가진 것으로 보는 견해에 따르면 양해는 엄격한 요건이 필요한 피해자의 승낙과는 달리 단순한 내적 동의로 족하며, 피해자에게 사실적, 자연적으로 양해의 의사가 있기만 하면 외부로 표시될 필요도 없고, 판단능력이나 행위능력이 없어도 무방하며, 기망이나 강요, 폭행이나 협박에 의한 하자있는 의사표시라 하더라도 유효하게 구성요건 해당성을 배제시킬 수 있다고 한다.[467] 이렇게 보면 양해와 승낙의 유효요건이 현저하게 달라지게 된다.[468] 피해자의 승낙은 형법 제24조에서 규정하고 있는 것처럼 "처분할 수 있는 자", 즉 승낙능력이 있는 자가 자유의사를 가지고 승낙한 경우에만 효력이 있기 때문이다.[469]

하지만 상술한 바와 같이, 우리나라의 다수설은 각각의 구성요건의 특성과 체계적 구조에 따라 양해의 유효요건을 개별적으로 판단하는 것이 합리적이라고 한다. 이를 예를 들어 좀 더 풀어 설명하면 다음과 같다. 기망에 의하여 재물을 가져가는 것을 "양해"한 경우 사기죄가 성립하므로, 절도죄의 구성요건 해당성은 하자있는 양해 의사로도 배제될 수 있지만, 처분행위를 인정할 수 없는 경우, 예컨대 금은방에서 잠시 착용해보겠다고 가져간 금목걸이나, 가짜 경찰에게 적법한 강제수사인줄 알고 건내 준 물건의 경우, 책략절도가 성립하는 것으로 보아야 하므로 하자있는 양해가 구성요건 해당성을 배제한다고 할 수 없다.[470] 그러므로 양해를 순수한 사실적 성격을 가진 것으로 보는 견해를 전적으로 지지하기는 어렵다고 판단된다. 그런데 이렇게 보면 결국 피해자의 승낙과 양해의 유효요건에 대한 근본적인 차이점을 이야기할 수 없게 될 뿐만 아니라 설사 통신비밀보호법상 감청에 대한 양해가 있는 경우라 하더라도, 실제 구성요건 해당성을

467) 독일의 유력설이라고 한다. 손동권, 양해·승낙의 구분에 따른 구체적 법 효과 차이의 문제, 형사법연구 제23권 제3호, 2011, 103-109쪽.

468) 이정원, 법익주체의 동의로서 승낙과 양해, 법학논총 제16권 제2호, 2009, 3쪽.

469) 김혁돈, 추정적 의사의 확정과 절차적 정당화, 비교형사법연구 제10권 제1호, 2008, 1쪽.

470) 손동권, 양해·승낙의 구분에 따른 구체적 법 효과 차이의 문제, 형사법연구 제23권 제3호, 2011, 108쪽.

배제할 수 있는 상황인지를 구체적으로 검토해 보아야 한다.

다. 소 결

그러므로 감청에 대한 동의가 양해인지 피해자의 승낙인지에 대한 논의는, 위법성 조각사유의 객관적 전제사실에관한 착오에 대하여 엄격책임설을 취하는 경우에 동의가 없었음에도 불구하고 있었던 것으로 착오하고 감청한 사건을 어떻게 처리하여야 할지를 논하는 경우나, 또는 양해를 순수한 사실적 성격을 가진 것으로 보고 자연적, 사실적으로 양해의 의사가 존재하기만 하면 구성요건 해당성을 배제시킬 수 있다는 소수설을 취하는 경우에만 의미가 있다고 할 것이다. 그러나 상술한 바와 같이 전자는 감청에 대한 동의의 유효 요건을 검토하는데 아무런 의미가 없으며, 후자는 이론적으로 지지하기 어렵다.

특히 후자에 따르면 감청에 대한 내적 동의가 외부로 표시되지 않은 경우는 물론 착오나 기망, 폭행이나 협박에 의하여 감청에 동의한 경우에도 불법이 조각되어야 하는데, 만약 이를 인정한다면 우리 통신비밀보호법이 엄격하게 정하고 있는 법원에 의한 통신제한조치 허가절차가 악의적인 의도를 가진 자에 의하여 손쉽게 우회될 수 있을 것이다. 그러나 제2장에서 살펴본 바와 같이 통신의 비밀과 자유는 민주주의의 근간을 이루는 중대한 기본권으로, 원칙적으로는 법원이 발부한 허가장이 있는 경우에만 예외적으로 제한될 수 있다. 따라서 법이론적으로 감청 동의가 양해에 해당하는 것이라 하더라도, 감청 동의가 통신의 비밀과 자유를 보호하는 구성요건의 해당성을 배제하기 위해서는 법원의 허가장 발부에 준하는 것으로 평가할 수 있을 만큼 엄격한 요건을 갖추어야 한다.

결국 감청에 대한 동의를 양해로 보아야 하는지 아니면 피해자의 승낙으로 보아야 하는지 만으로는 불법을 배제하기 위해 필요한 요건을 구체화하여 제시할 수 없으며, 통신비밀보호법상 감청 구성요건의 구조와 보호법익의 의의, 침해하는 자와 침해당하는 자의 사실적 관계 등을 종합적으로 검토하여 실제 감청의 불법이 배제되기 위해서 필요한 법익 처분의 내용을 확정해야 한다. 일반적으로는 양해의 성립요건이 피해자의 승낙의 성립요건에 비하여 완화된 것으로 평가되므로 가장 엄격한 양해의 성립요건을 바로 피해자의 승낙이 성립하기 위한 요

건과 같은 것으로 보아도 큰 무리가 없을 것으로 생각된다. 그러므로 이하에서는 피해자의 승낙의 성립요건을 중심으로 감청 동의의 요건을 구체화해보겠다.

2. 피해자의 승낙의 요건과의 비교를 통한 감청 동의의 요건 구체화

가. 피해자의 승낙의 요건 개관

피해자의 승낙의 요건은 ① 승낙주체, ② 처분할 수 있는 법익, ③ 승낙, ④ 주관적 정당화요소로 구분할 수 있다. 간략하게 살펴보면, ① 피해자의 승낙은 법익에 대한 적법한 처분권한을 가진 자가 법익침해에 동의하는 것으로, 적법한 처분 권한이 있다면 승낙의 대상이 되는 법익은 자기의 법익으로 한정되지 않는다. ② 그러나 처분할 수 있는 법익은 당연히 개인적 법익으로 제한된다. 다만 개인적 법익이라 하더라도 생명, 신체에 대한 처분은 다시 제한된다. ③ 승낙은 승낙능력, 즉 침해되는 법익에 대한 이성적 판단능력이 있는 자가 자유의지를 가지고, 그리고 상대방이 인식할 수 있는 방법으로 법익 침해 전에 해야 한다. 이 점은 감청 동의의 요건을 구체화하는데 의미가 있으므로 단락을 나눠 상술한다. 끝으로 위법성 조각사유로서 행위자에게 ④ 주관적 정당화요소를 요구한다. 즉, 침해행위자는 승낙의 존재를 인식하여야 하는 것이다. 그렇지 않은 경우 위법성은 그대로 유지된다.[471]

나. 승낙능력

승낙은 법익이 침해되는 것에 대하여 동의하는 것이고, 따라서 이 동의는 법익 침해에 대한 인식과, 결과에 대한 이성적 판단 능력을 전제로 하는 것이다.[472] 다만 민법상 의사능력이나 행위능력과는 구별되는 것으로, 원칙적으로는

471) 배종대, 형법총론 제11판, 홍문사, 2013, 81/2-15.

472) 이용식, 피해자의 승낙에 관한 소고, 동산 손해목박사화갑기념논문집, 1993, 181면; 최석윤, 피해자의 승낙과 양형, 피해자학연구 제5호, 1997, 212면

일정한 연령[473]이나 사법상의 행위능력 요건과 관계없이 사물에 대한 "자연적 통찰능력"[474]을 의미하는 것으로 보아야 한다. 그러나 통찰이라는 것은 승낙자가 처한 상황, 대상의 수준이나 난이도, 또는 주어진 정보에 따라 달라질 수밖에 없으므로, 보편적으로 적용될 수 있는 능력의 기준을 제시할 수는 없고 다만 승낙의 대상이 된 법익의 종류와 승낙하려는 자가 실제로 처한 상황에 따라 승낙능력의 유무를 판단하여야 할 것이다.[475]

그러므로 일반인이 상식적인 수준에서 충분히 알기 어려운 전문적인 지식이 필요한 경우 승낙이 유효하기 위해서는 상대방 또는 전문가의 설명이 필요하게 된다. 가장 대표적인 경우로 수술 동의에 대한 의사의 설명의무를 생각해 볼 수 있다. 만약 의료인이 설명의무를 이행하지 않으면 상대적 약자인 환자의 승낙이 있다 하더라도 불법이 조각되지 않는다.[476] 승낙이 유효하기 위해서는 자유의지에 기반한 것이어야 한다. 하자있는 의사표시는 위법성을 조각할 수 없다.

다. 감청 동의의 요건

지금까지 검토해 본 피해자의 승낙의 요건에 비추어 감청 동의가 불법을 조각하기 위한 요건을 구체화해 보면 다음과 같다.

1) 동의 주체와 대상

① 감청 동의는 자신의 통신에 대해서만 할 수 있는 것이 원칙이다. 타인의 통신의 비밀 또는 통신의 자유를 처분할 수 있는 경우는 생각하기 어렵다. 다만 미성년자 등 판단능력이 부족한 사람의 통신에 대해서 법정대리인이 동의하는

473) "사실에 관한 판단문제이기 때문에 일정한 연령을 기준으로 하는 것은 아니지만 형법이 개별적으로 승낙할 수 있는 연령을 규정하는 경우도 있다. 예컨대 미성년자간음죄(제305조)에서는 13세 미만, 아동혹사죄(제274조)에서는 16세 미만인 사람은 해당 침해행위에 대한 승낙능력이 없다." 배종대 형법총론 제11판, 홍문사, 2013, 81/6에서 인용.

474) 배종대, 형법총론, 제11판, 홍문사, 2013, 81/6.

475) 정진연, 연명치료중단에 관한 형법적 고찰, 법학연구 제36편, 2009, 279면

476) 대판 1993. 7. 27. 92도2345.

경우처럼 보호가 필요한 사람의 이익을 위해 대리권을 행사하는 자가 감청에 대하여 동의하는 경우를 생각해 볼 수 있다. 그러나 법원의 허가장을 통해서만 제한될 수 있는 통신의 비밀과 자유에 대한 높은 보호필요성을 생각한다면, 설사 미성년자라 하더라도 법정대리인의 동의를 무제한적으로 허용해서는 안 될 것이며, 그 감청이 명확하게 피감청자에게 이익이 되는 경우에 한정하여 동의를 인정할 수 있을 것으로 생각된다. 이 외에도 미리 감청에 대한 동의를 구체적으로 위임받은 제3자가 대신 동의하는 경우도 생각해 볼 수 있다. 그러나 이는 위임을 하는 순간 표현된 본인의 감청 동의 의사를 전달하는 것에 불과한 것으로 보아야 한다.

② 동의의 대상은 처분할 수 있는 법익이어야 한다. 통신의 비밀과 자유는 이미 우리 통신비밀보호법이 동의를 감청의 요건으로 함으로써 명시적으로 처분할 수 있는 법익임을 선언하였다.

③ 통신에 참여하는 모든 당사자의 동의가 있어야 한다. 이 때 각 당사자는 모두 동의로 인해 포기되는 통신의 비밀과 자유의 가치에 대한 정확한 인식, 그리고 동의가 초래할 결과에 대한 자연적 통찰 능력을 가진 자가 자유의지를 가지고, 상대방이 인식할 수 있도록 명시적으로, 감청의 실행에 착수하기 전에 해야 한다. 사후적인 동의는 구성요건 해당성을 배제하지 못하며 다만 양형상 고려요소가 될 뿐이다.

2) 쌍방 동의 원칙

통신은 원칙적으로 2인 이상의 당사자간의 의사소통을 의미하므로, 참여자 일방의 동의는 감청을 정당화할 수 없다.[477] 상술한 바와 같이 타인의 통신의 비밀과 자유에 대한 권리는 설사 당해 통신의 상대방이라 하더라도 이를 임의로 처분할 수 없는 것이기 때문이다. 그러므로 동의가 감청의 구성요건 해당성을

477) 오길영, 감청의 상업화와 그 위법성, 민주법학, 제43호, 2010, 454쪽, 특히 각주 93.

배제하려면 통신에 참여하는 모든 당사자의 동의가 있어야 한다. 우리 대법원도 통화자 일방의 동의만으로는 제3자가 타인간의 전화통화를 녹음하는 것을 정당화할 수 없다고 확인한 바 있다.[478] 그러므로 인터넷에서 참여자 일방이 원치 않는 정보의 수신을 차단을 적극적으로 요청하는 경우라 하더라도, 그 차단은 발신자의 입장에서는 통신의 비밀과 자유를 제한하는 송·수신 방해가 되기 때문에, 원칙적인 관점에서 오로지 수신자가 동의했다는 이유만으로는 망 관리자가 정보의 전달을 방해하는 행위가 모두 정당화되기 어려울 것으로 생각된다.

따라서 이 경우 추가적인 정당화 사유(예컨대 명백한 불법정보에 대한 차단)가 요구되는 것으로 보아야 한다. 다만 이미 수신한 정보를 보지 않는 것은 수신자의 자유이다. 그러므로 만약 인터넷 이용자가 원치 않는 광고를 차단하기를 원한다면, 그 차단의 방법은 망 관리자에 의한 패킷 분석과 수신방해, 즉 감청을 수단으로 하는 것이어서는 안 되고, 이용자의 컴퓨터에 추가적인 어플리케이션을 설치하는 방법을 택하는 것이 망 중립성 및 통신비밀보호법의 취지에 부합하는 합법적인 솔루션이 될 것이다.

3) 인터넷 사업자의 설명 의무

또한 동의하는 사람은 감청 동의를 통해 침해될 비밀과 자유의 구체적인 범위와 이로 인한 결과에 대하여 실제로 내용을 파악하고 의미를 통찰할 수 있어야 한다. 그러나 대부분의 가입자들은 전문적인 통신기술의 원리에 대하여 잘 알지 못하며, 따라서 망 중립성을 제한하기 위해 가입자의 동의를 받고자 하는 통신사는 이를 위해 사용되는 기술과 침해되는 권리의 범위를 가입자에게 명확하게 설명해야 하는 의무를 갖는다. 이때의 설명은 통신기술의 작동원리에 대해서 전혀 알지 못하는 비전문가라 하더라도 충분히 그 규범적 의미를 이해할 수 있는 정도여야 하며, 실제 피감청자가 설명을 통해 내용을 이해한 경우에만 동의가 유효한 것으로 보아야 한다. 그러므로 mVoIP을 차단하고자 하는 이동통신사는 가입자에게 mVoIP을 차단하기 위해서 가입자의 모든 인터넷 사용내역이 자동화

478) 대판 2002. 10. 8. 2002도123. 이 판례에 대한 평석은 하태훈, 통화자일방의 동의를 받은 제3자의 전화녹음과 통신비밀보호법 위반, 안암법학, 제17호, 2003, 75쪽 이하 참조.

된 정보처리장치에 의해 실시간 분석되고 패턴별로 분류된다는 점을 명확하게 고지해야 한다.

이에 관하여 전기통신사업법 시행령 부칙 제42조 제1항에 근거하여 금지행위의 유형을 상세하게 규정하고 있는 별표 4의 5. 나. 4)는 이용자의 계약 체결 또는 해지와 관련하여 "전기통신서비스의 이용에 중요한 사항을 고지하지 않거나 거짓으로 고지하는 행위"를 이용자의 이익을 해치는 행위의 유형으로 명시하고 있다. 통신의 비밀과 자유에 대한 제한은 당연히 전기통신서비스의 이용에 중요한 사항이며, 이를 고지하지 않거나 거짓으로 고지하는 행위는 전기통신사업법상의 규정(제51조 사실조사, 제52조 금지행위에 대한 조치, 제53조 금지행위 등에 대한 과징금의 부과)에 따라 다양한 행정처분이 가능하다. 이 경우 과징금의 상한은 매출액의 100분의 3이다. 수익이 아니라 매출을 기준으로 하고 있다는 점, 그리고 우리나라 통신기업의 매출액이 수조에 이른다는 점을 고려하면 매우 강력한 처분이 가능한 것이다. 또한 같은 법 제99조에 의하여 3억원 이하의 벌금으로 처벌되는 형사불법이 된다. 이미 전기통신사업법은 감청 동의에 대하여 계약 체결당시에 구체적으로 설명할 것을 강제하고 있는 것이다.

4) 실질적인 동의 거절 가능성

또한 감청 동의가 효력을 갖기 위해서는 실질적인 동의 거절 가능성이 있어야 한다. 거절할 수 없는 행위를 하는 것은 결코 자유의지의 실현이라고 할 수 없기 때문이다. 그런데 현재 관행상 이루어지고 있는 약관에 의한 동의는, 약관을 계약내용으로 편입하는 것을 거부하면 서비스 이용 계약 체결 자체가 거부당하는 경우가 대부분이다. 즉, 감청에 대한 동의를 이를 거부하면 통신서비스에 가입할 수 없는 구조로 되어있는 것이다. 이는 자유의지를 가진 유효한 동의라고 할 수 없다. 따라서 단순 반복적인 대량계약의 편의를 위해서 감청 동의에 관한 내용을 약관으로 만들 필요가 있다 하더라도 원칙적으로 이는 계약 체결 여부를 좌우하는 약관과는 구별되는 별도의 약관이어야 한다. 이러한 의미에서 이동통신사가 요금제를 다양하게 만들어 특정 요금제에서 mVoIP을 허용하는 경우에도 mVoIP 허용 요금제가 mVoIP을 금지하는 요금제보다 불합리하게 비싸다면 이는

실질적으로 동의 거절의 자유가 박탈된 것이기 때문에 이를 유효한 동의로 볼 수 없다.

5) 약관 동의 문제

이에 관하여 현행 전기통신사업법 제50조 제1항 제5호[479]는 "약관과 다르게 전기통신서비스를 제공하거나 전기통신이용자의 이익을 현저히 해치는 방식"으로 서비스를 제공하는 행위를 금지하고 있다. 그러므로 이 조항의 해석상 같은 법 제29조 제1항 및 제2항에 의해 신고하거나 인가받은 적법한 약관에 따르는 경우에도 전기통신이용자의 이익을 현저하게 해치는 것을 금지하는 것이다. 즉 개인 간의 계약의 내용인 약관보다 전기통신사업법의 규정을 우선하겠다는 강행규정으로 볼 수밖에 없다. 따라서 상술한 바와 같이 요건을 지키지 않은 동의를 강요하는 내용의 약관은 강행규정에 위반되므로 당연히 그 효력을 부정해야 한다.

④ 주관적 정당화요소는 필요 없다. 위법성 조각사유가 아니므로 동의가 있었다는 점에 대한 인식이 필수적인 것은 아니다. 그러나 감청행위자가 피감청자의 동의의 존재를 몰랐다면 사실상 그 불법은 불능미수에 준하는 상황이 된다고 할 수 있다.

479) 제50조(금지행위) ① 전기통신사업자는 공정한 경쟁 또는 이용자의 이익을 해치거나 해칠 우려가 있는 다음 각 호의 어느 하나에 해당하는 행위(이하 "금지행위"라 한다)를 하거나 다른 전기통신사업자 또는 제3자로 하여금 금지행위를 하도록 하여서는 아니 된다. (중략) 5. 이용약관(제28조 제1항 및 제2항에 따라 신고하거나 인가받은 이용약관만을 말한다)과 다르게 전기통신서비스를 제공하거나 전기통신이용자의 이익을 현저히 해치는 방식으로 전기통신서비스를 제공하는 행위.

3. 소 결 – 선별적 송·수신 방해행위에 대한 이용자 동의가 불법을 조각하기 위한 요건

이상의 논의를 정리하면 선별적 송·수신 방해행위에 대한 이용자 동의가 불법을 조각하기 위해 특히 고려해야 하는 주요 요건은 다음과 같다.

① 원칙적으로 자신의 통신에 대한 동의만이 가능하다. 타인을 위한 감청 동의는 그 감청이 명백하게 피감청자에게 이익이 되는 경우에만 예외적으로 허용될 수 있다.

② 당해 통신에 참여하는 모든 당사자가 동의해야 한다. 그러므로 수신자의 수신 거부는 기술적으로 망 차원이 아니라 수신자의 단말기 차원에서 실현되어야 한다.

③ 망 중립성을 제한하고자 하는 통신사는 이용되는 기술의 작동원리 및 통신의 비밀과 자유에 대한 침해 범위를 비전문가인 이용자가 이해할 수 있을 정도로 상세하게 설명해야 한다. 충실한 설명이 없다면 법이 정하고 있는 고지의무를 위반하는 것이 된다.

④ 동의를 거부할 수 있어야 한다. 거부 가능성은 형식적인 것이어서는 안 되며 거부하더라도 동등한 서비스를 이용할 수 있어야 한다. 그렇지 않은 약관은 강행규정 위반으로 무효이다.

제2절 정당행위로서 합리적 트래픽 관리

1. 정당한 업무로서 망 관리

지금까지 동의가 망 중립성 침해 행위의 구성요건 해당성을 배제하기 위한 요건을 살펴보았다. 이하에서는 동의가 없는 경우의 이른바 "망 관리"의 정당화 가능성을 검토해 본다. 우리 형법은 피해자의 승낙 이외에도 정당행위(제20조), 정당방위(제21조), 긴급피난(제22조), 자구행위(제23조)의 위법성 조각사유를 두고 있다. 이 중 자구행위는 불법감청에 관하여 적용될 가능성이 없으며, 정당방위나 긴급피난은 예외적으로 긴급한 법익침해가 예상되는 경우 적용될 가능성이 있으나, 이러한 경우라면 일반적인 형법이론에 따라 판단하면 될 것이다. 다만 상시적인 트래픽 관리의 경우 침해(위난)의 현재성 요건을 충족하기 어려우므로 정당방위와 긴급피난의 법리를 적용할 수는 없을 것으로 생각된다.

물론 계속위난에 대한 대응이라는 관점에서 모든 인터넷 이용자에 대한 긴급 통신제한조치는 방어적 긴급피난[480]으로, 인터넷을 불법적으로 이용하는 자에 대한 긴급 통신제한조치는 예방적 정당방위[481]로 볼 여지가 없는 것은 아니다. 그러나 이러한 경우는 역시 예외적인 경우가 될 것이며, 인터넷 보안이나 통신망의 기능에 대한 계속위난이 상시적으로 존재하는 "망 관리"의 영역에서 위난에 대한 대처는 더 이상 예외적이고 긴급한 조치라고 할 수 없으며, 오히려 망 관리자의 일상적인 업무가 되는 것으로 보는 것이 타당하다. 따라서 이 글에서는 정당행위, 특히 업무로 인한 정당행위의 관점에서 합리적 트래픽 관리의 기준을 검토해 보겠다.

물론 업무로 인한 정당행위에 있어서 특정행위가 업무에 해당한다는 점만으로 위법성이 조각되는 것은 결코 아니며 업무는 그 자체로 "정당한" 것이어야 한다.[482] 따라서 업무행위가 법령을 준수해야 하는 것임은 물론 타인의 권리와 이

480) 방어적 긴급피난에 관해서는 윤용규, 긴급피난 규정의 이해와 입법론적 검토, 형사법연구, 제22호, 2004, 149쪽 이하 참조.

481) 예방적 정당방위에 관해서는 원형식, 소위 "예방적 정당방위"에 관한 연구, 형사법연구, 제16호, 2001, 84쪽 이하 참조.

익을 부당하게 침해하는 것이어서도 안 된다. 그러나 변호사의 변론행위나 의사의 치료행위와 같이 업무의 정당한 범위에 관하여 보편적이고 객관적인 사회적 합의가 아직 마련되지 않은 경우라면, 구체적인 경우에 대한 판단이 필요하게 된다. 이러한 경우에 대한 판단기준에 관하여 우리 대법원은 "어느 행위가 정당행위에 해당한다고 인정할 수 있기 위해서는 그 행위의 동기나 목적의 정당성, 행위의 수단이나 방법의 상당성, 보호법익과 침해법익과의 법익균형성, 긴급성, 그 행위 외에 다른 수단이나 방법이 없다는 보충성 등의 요건이 갖추어져야 한다"[483]고 판시한 바 있다. 그러므로 위법성을 조각시키기 위한 합리적인 망 관리는 정당성, 상당성, 균형성, 긴급성, 보충성의 요건을 갖춘 경우에만 정당행위로써 감청의 불법을 조각할 수 있을 것이다. 이하에서는 이러한 점을 고려하여 정당행위로서 합리적인 망 관리의 구체적인 기준을 제시해 보고자 한다.

2. 관련 법률이 선언하고 있는 정당성의 내용

법령에 의한 행위는 정당행위가 된다. 그러나 우리나라의 망 중립성 관련 법률은 트래픽 관리에 관하여 할 수 있는 행위유형을 구체적으로 규정하여 제시하고 있는 것이 아니라, 해서는 안 되는 금지와 의무를 정하고 있다.[484] 그러므로 법령에 의한 정당행위는 성립할 수 없다. 다만 금지와 의무를 정하고 있는 법령을 위반하는 행위는 정당한 업무가 될 수 없다는 소극적인 판단근거로 원용될 수 있을 뿐이다.

---

482) 배종대, 형법총론, 제11판, 홍문사, 2013, 60/1.

483) 대판 1086. 10. 28. 86도1764.

484) 할 수 있는 행위는 합리적 트래픽 관리에 관한 기준(안)에서 분명하게 제시될 예정이다. 기준(안)은 올해 안 확정을 목표로 미래창조과학부에서 의견을 수렴하여 구체화하고 있다. 정당행위 성립 요건의 기준이 될 것으로 생각되는 기준(안)에 관해서는 후술한다.

가. 전기통신사업법[485] – 자의적 망 관리 금지

현행 법 체계 중에서 사업자의 망 관리를 규율하는 법률은 바로 전기통신사업법이다. 전기통신사업법은 "전기통신사업의 적절한 운영과 전기통신의 효율적 관리를 통하여 전기통신사업의 건전한 발전과 이용자의 편의를 도모함으로써 공공복리의 증진에 이바지함을 목적으로"하는 법으로 전기통신사업자의 업무에 관하여 상세한 규정을 두고 있다. 인터넷은 바로 전기통신망이며 인터넷 접속 서비스 제공자는 바로 전기통신사업자가 되기 때문에, 이 법은 정당한 업무의 내용과 기준에 대한 원칙을 담고 있는 법률이라고 할 수 있을 것이다. 현행 전기통신사업법상 망 중립성과 직접적으로 관련되는 주요 조항은 다음과 같다.

제3조(역무의 제공 의무 등) ① 전기통신사업자는 정당한 사유 없이 전기통신역무의 제공을 거부하여서는 아니 된다. ② 전기통신사업자는 그 업무를 처리할 때 공평하고 신속하며 정확하게 하여야 한다. ③ 전기통신역무의 요금은 전기통신사업이 원활하게 발전할 수 있고 이용자가 편리하고 다양한 전기통신역무를 공평하고 저렴하게 제공받을 수 있도록 합리적으로 결정되어야 한다.

제28조(이용약관의 신고 등) ③ 제2항 본문의 경우 미래창조과학부장관은 이용약관이 다음 각 호의 기준에 맞으면 이용약관을 인가하여야 한다. (중략) 3. 다른 전기통신사업자 또는 이용자의 전기통신회선설비 이용형태를 부당하게 제한하지 아니할 것 4. 특정인을 부당하게 차별하여 취급하지 아니할 것 (후략)

제50조(금지행위) ① 전기통신사업자는 공정한 경쟁 또는 이용자의 이익을 해치거나 해칠 우려가 있는 다음 각 호의 어느 하나에 해당하는 행위(이하 "금지행위"라 한다)를 하거나 다른 전기통신사업자 또는 제3자로 하여금 금지행위를 하도록 하여서는 아니 된다. 1. 설비등의 제공 · 공동활용 · 공동이용 · 상호접속 · 공동사용 · 도매제공 또는 정보의 제공 등에 관하여 불합리하거나 차별적인 조건 또는 제한을 부당하게 부과하는 행위 (중략) 5. 이용약관(제28조제1항 및 제2항에 따라 신고하거나 인가받은 이용약관만을 말한다)과 다르게 전기통신서비스를 제공하거나 전기통신이용자의 이익을 현저히 해치는 방식으로 전기통신서비스를 제공하는 행위 (후략)

이 법 제3조 제1항은 "전기통신사업자는 정당한 사유 없이 전기통신역무의 제공을 거부하여서는 아니된다"고 규정하고 있다. 여기서 전기통신역무란 "전기통신설비를 이용하여 타인의 통신을 매개하거나 전기통신설비를 타인의 통신용으로 제공하는 것"[486]을 말하며, 따라서 사업자가 관리하는 통신망에서 가입자의 인터넷 이용을 위한 디지털 데이터의 송 · 수신을 매개하는 것을 거부하기 위해

485) 망 중립성과 전기통신사업법에 관하여 상세한 분석은 김보라미, 박건철, 이봉규, 이동통신사에 의한 mVoIP 서비스 차단의 법적 문제, 정보법학, 제16권 제1호, 2012, 11쪽 이하 참조.

486) 전기통신사업법 제2조 제6호.

서는 정당한 이유가 있어야 한다. 그러므로 망 중립성과 관련하여서도 선별적으로 송·수신을 차단하기 위해서는 언제나 "정당한 사유"가 있어야 한다는 선언적 의미를 갖는다. 그러나 이 조항은 정당한 사유의 내용과 기준을 상세하게 제시하고 있지는 않다.

같은 조 제2항은 "전기통신사업자는 그 업무를 처리할 때 공평하고 신속하며 정확하게 하여야 한다"고 선언하고 있다. 즉 전기통신사업자의 통신 중계업무는 언제나 공평해야 한다. 그러나 "공평"은 모든 것을 동일하게 취급하라는 의미는 아니며, 차별이 합리적인 한 정당한 업무로 허용하는 것으로 보인다. 따라서 패킷을 차별하기 위해서는 당연히 그 차별에 합리적인 이유가 있어야 한다. 나아가 제3조 제3항 또한 이용자에게 공평하게 전기통신업무를 제공할 것을 규정하고 있다. 그러므로 사업자는 통신망 이용자를 요금으로 차별해서는 안 된다.

미래창조과학부장관 또는 방송통신위원회는 전기통신사업자가 제3조를 위반하는 경우 제92조제1항 제1호에 의해 시정을 명할 수 있으며, 이를 이행하지 않으면 제104조 제4항 제17호에 의해 1천만원 이하의 과태료가 부과된다. 또한 제3조 제1항을 위반하여 정당한 사유 없이 전기통신역무의 제공을 거부한 자는 제95조에 제1호에 의해 3년 이하의 징역 또는 1억5천만원 이하의 벌금으로 처벌된다.

같은 법 제28조는 기간통신사업자의 전기통신서비스 이용약관에 관한 규제를 담고 있다. 같은 조 제3항은 약관의 인가기준을 제시하고 있는데, 약관을 통해서 다른 전기통신사업자와 이용자의 전기통신회선설비 이용을 부당하게 제한하지 않아야하며(제3호), 특정인을 부당하게 차별하지 않아야 한다(제4호). 제28조를 위반하는 행위도 역시 제92조 제1항 1호의 시정명령과 제104조 제4항 제17호의 과태료 처분을 받을 수 있다.

제50조 제1항은 전기통신사업자의 금지행위를 열거하고 있다. 전기통신사업자는 공정한 경쟁 또는 이용자의 이익을 해치거나 해칠 우려가 있는 행위를 하여서는 안 되며, 특히 통신망 이용에 있어서 불합리하거나 차별적인 조건 또는 제한을 부당하게 부과해서는 안 되며(제1호), 제28조에 의해 신고 또는 인가된 이용약관에 따르는 것이라 하더라도 "전기통신이용자의 이익을 현저히 해치는 방식"으로 전기통신서비스를 제공해서는 안 된다.(제5호) 제50조 제1항을 위반하는 경우 제52조에 의해 방송통신위원회는 금지행위의 중지 등 시정명령을 내릴

수 있고, 제53조에 의해 매출액의 100분의 3 이하에 해당하는 금액을 과징금으로 부과할 수 있다. 특히 제50조 제1항 제1호의 위반에 대해서는 제99조에 의해 3억원 이하의 벌금으로 처벌되기도 한다.

여기서 설명하고 있는 전기통신사업법상의 규정들은 비록 구체적인 기준을 제시하고 있는 것은 아니지만, 정당성과 합리성, 공평성에 대한 원칙을 선언하고 있으며, 전기통신사업법은 이러한 원칙을 훼손하는 사업자에게 시정명령, 과징금, 과태료, 그리고 형사처벌을 부과하는 방법으로 원칙의 준수를 강제하고 있다. 따라서 전기통신사업법은 인터넷 관리자의 "자의적" 망 관리를 금지하고 있는 것으로 해석된다.

나. 독점규제 및 공정거래에 관한 법률

> **제3조의2(시장지배적지위의 남용금지)** ① 시장지배적사업자는 다음 각호의 1에 해당하는 행위(이하 "남용행위"라 한다)를 하여서는 아니된다. 1. 상품의 가격이나 용역의 대가(이하 "가격"이라 한다)를 부당하게 결정·유지 또는 변경하는 행위 2. 상품의 판매 또는 용역의 제공을 부당하게 조절하는 행위 3. 다른 사업자의 사업활동을 부당하게 방해하는 행위 4. 새로운 경쟁사업자의 참가를 부당하게 방해하는 행위 5. 부당하게 경쟁사업자를 배제하기 위하여 거래하거나 소비자의 이익을 현저히 저해할 우려가 있는 행위

현재 우리나라의 통신시장은 SKT, KT, LG U+ 세 회사에 의하여 사실상 지배되고 있다. 사실상 전국적인 통신망을 설치하는 비용의 부담으로 인하여 통신사업자의 사업자의 신규진입은 구조적으로 어려울 수밖에 없다는 점과, 특히 통신망 재판매 사업도 활성화되지 않은 우리 통신시장의 구조를 고려하면, 우리나라의 주요 통신사업자가 시장지배적 사업자에 해당한다는 점에는 별다른 논증 없이도 동의할 수 있을 것으로 생각된다.[487] 특히 통신서비스 시장에서 한정된 자원인 통신망에 대한 통제권을 갖는 자가 시장 지배적 지위를 갖게 되는 것은 당연한 일이다.

따라서 망 관리 권한을 가진 시장지배적 통신사업자의 망 중립성 저해행위, 즉 인터넷 서비스 제공자의 이윤을 극대화하기 위하여 mVoIP 등 경쟁 서비스의

487) 통신시장의 시장지배적 사업자에 관해서는 홍명수, 통신산업에서의 시장지배적 사업자 규제에 관한 연구 : 전기통신사업법상 문제를 중심으로, 명지대학교 석사학위논문, 107쪽 이하 참조.

접속을 차단하는 선별적 인터넷 접속 차단 행위는 용역 제공의 부당 조절 행위, 경쟁사업자 배제 행위 및 소비자 이익 저해 행위에 해당한다. 이는 독점규제 및 공정거래에 관한 법률 제3조의2를 위반한 것으로[488] 같은 법 제66조에 의하여 3년 이하의 징역 또는 2억원 이하의 벌금으로 처벌될 수 있다. 그러므로 현재 우리나라의 통신시장 구조에서 독점규제 및 공정거래에 관한 법률은 망 관리의 "공정성"에 대한 법원(法源)이 된다.

3. 망 중립성 및 인터넷 트래픽 관리에 관한 가이드라인

살펴본 바와 같이 트래픽 관리를 위법성을 조각하기 위해 법률이 제시하고 있는 원칙은 정당성, 합리성, 공평성과 같은 추상적 선언에 그치고 있으며, 금지와 의무의 형태로 규정되어 있다. 구체적으로 어떠한 행위가 정당한 것인지, 합리적이고 공평한 것인지에 관한 기준을 법률이 직접 열거하고 있지는 않은 것이다. 그래서 당시 방송통신위원회는 허용되는 트래픽 관리의 범위를 보다 명확하게 제시하기 위하여 2011년 5월부터 관련 업계, 전문가, 소비자 단체 등이 참여하는 망 중립성 포럼을 구성하여 각계의 의견을 수렴하였으며, 2011년 12월 26일 가이드라인을 제정하였다. 그러므로 이 합리적 트래픽 관리에 관한 가이드라인은 차벌적 송·수신 방해행위의 위법성을 조각시키기 위한 요건의 가이드라인이기도 하다.

이 가이드라인은 망 중립성 및 트래픽 관리에 관한 기본원칙을 정함으로써 개방적이고 공정한 인터넷 환경을 조성하기 위한 것으로, 2010년 제정된 미국 FCC의 오픈 인터넷 규칙의 영향을 받은 것으로 평가되며, 2012년 1월 1일 시행되었다. 가이드라인의 전문은 다음과 같다.

---

488) 상세한 분석은 김보라미, 박건철, 이봉규, 이동통신사에 의한 mVoIP 서비스 차단의 법적 문제, 정보법학, 제16권 제1호, 2012, 14쪽 이하 참조.

망 중립성 및 인터넷 트래픽 관리에 관한 가이드라인

2011년 12월 26일 제정, 2012년 1월 1일 시행

Ⅰ. 목 적

1. 이 가이드라인은 망 중립성 및 인터넷 트래픽 관리에 관한 기본원칙을 정함으로써, 개방적이고 공정한 인터넷 이용 환경을 조성하고 ICT(Information and Communication Technology, 이하 'ICT'라 한다) 생태계의 건전하고 지속가능한 발전을 도모함을 목적으로 한다.

Ⅱ. 기본원칙

이용자의 권리

2. 인터넷 이용자는 합법적인 컨텐츠, 애플리케이션, 서비스 및 망에 위해가 되지 않는 기기 또는 장치를 자유롭게 이용할 권리를 가지며, 관련 사업자로부터 인터넷 트래픽 관리에 관한 정보를 제공받을 권리를 갖는다.
   ※ 인터넷 이용자는 '최종이용자(end user)'를 말한다.

인터넷 트래픽 관리의 투명성

3. 인터넷접속서비스제공사업자는 인터넷 트래픽 관리의 목적, 범위, 조건, 절차 및 방법 등을 명시한 트래픽 관리방침을 공개하고, 트래픽 관리에 필요한 조치를 하는 경우 그 사실과 영향 등을 해당 이용자에게 고지하여야 한다(다만, 해당 이용자에게 고지하기 어려운 부득이한 사유가 있는 경우에는 공지로 갈음할 수 있다). 방송통신위원회는 필요한 경우 공개 및 고지 또는 공지 대상 정보의 범위 및 방식 등을 별도로 정할 수 있다.
   ※ 인터넷접속서비스제공사업자는 전기통신사업법의 규정에 따라 유무선 인터넷접속서비스를 제공하는 전기통신사업자를 말한다.

차단 금지

4. 인터넷접속서비스제공사업자는 합법적인 컨텐츠, 애플리케이션, 서비스 또는 망에 위해가 되지 않는 기기 또는 장치를 차단해서는 안된다. 다만, 합리적인 트래픽 관리의 필요성이 인정되는 경우에는 그러하지 아니하다.

불합리한 차별 금지

5. 인터넷접속서비스제공사업자는 컨텐츠·애플리케이션·서비스의 유형 또는 제공자 등에 따라 합법적인 트래픽을 불합리하게 차별해서는 안된다. 다만, 합리적인 트래픽 관리의 필요성이 인정되는 경우에는 그러하지 아니하다.

합리적인 트래픽 관리

6. 합리적인 트래픽 관리의 필요성이 인정되는 경우는 아래의 경우를 포함하며, 이에 한하지 않는다. 그 밖에 합리적인 트래픽 관리의 범위, 조건, 절차, 방법 및 트래픽 관리의 합리성 여부에 대한 판단 기준 등은 방송통신위원회가 별도로 정한다. 이 경우 해당 망의 유형(유무선 등)과 기술 특성에 따라 다르게 정할 수 있다.
   ① 망의 보안성 및 안정성 확보를 위해 필요한 경우
   ② 일시적 과부하 등에 따른 망 혼잡으로부터 다수 이용자의 이익을 보호하기 위해 필요한 경우
   ③ 국가기관의 법령에 따른 요청이 있거나 타 법의 집행을 위해 필요한 경우 등

Ⅲ. 관리형 서비스

7. 인터넷접속서비스제공사업자는 최선형인터넷의 품질이 적정 수준이하로 저하되지 않는 범위 내에서

관리형서비스(managed service)를 제공할 수 있다. 관리형서비스의 제공이 최선형인터넷(best effort Internet)의 품질과 시장에 미치는 영향 등에 대해서는 방송통신위원회가 별도로 모니터링한다.

※ 관리형서비스(managed service)는 인터넷접속서비스제공사업자가 일반적으로 통용되는 최선형인터넷의 제공 방식과 다른 트래픽 관리기술 등을 통해 전송 대역폭 등 트래픽 전송 품질을 보장하는 서비스를 말한다.

Ⅳ. 상호 협력

8. 인터넷접속서비스제공사업자와 컨텐츠·애플리케이션·서비스 제공자 등은 ICT 생태계의 건전하고 지속가능한 발전을 위하여 서로 협력하여야 하며, 특히 컨텐츠·애플리케이션·서비스의 제공 및 망의 안정적 운용 등을 위해 필요한 경우 정보를 제공하는 등 신의성실의 원칙에 따라 협조하여야 한다. 또한, 망 중립성 및 인터넷 트래픽 관리에 관한 시장 자율적 기준 마련 등을 위해 필요한 경우 협의체를 구성할 수 있다.

Ⅴ. 정책자문기구의 구성·운영

9. 방송통신위원회는 인터넷 트래픽 관리의 투명성 제고, 합리적인 트래픽 관리의 범위, 조건, 절차, 방법 및 트래픽 관리의 합리성 여부에 대한 판단 기준의 마련 등 이 가이드라인의 시행에 필요한 조치, mVoIP 등 새로운 서비스 확산에 대한 정책방향의 논의, ICT 생태계의 변화에 따른 새로운 시장질서의 모색 등을 위해 이해관계자·전문가 등이 참여하는 별도의 정책자문기구를 구성·운영한다. 그 구성 및 운영 등과 관련하여 필요한 사항은 방송통신위원회가 별도로 정한다.

1) 이용자(end user)의 권리

이 가이드라인은 다섯 가지의 기본 원칙을 선언하고 있다. 이 기본 원칙은 가장 먼저 이용자(end user)의 권리를 확인하는 것으로 시작한다. 이용자는 합법적이고 망에 위해가 되지 않는 한 컨텐츠나 장치를 자유롭게 이용할 권리를 가질 뿐만 아니라 트래픽 관리정보를 제공받을 권리를 갖는다. 합법적이고 위해가 되지 않는 행위를 할 자유는 국민으로써 당연히 향유할 수 있는 권리이며, 가이드라인의 선언을 통해 창설되는 것이 아니다. 통신망에서도 이는 당연히 인정된다 할 것이며, 따라서 이는 통신사업자들이 이용자의 당연한 권리를 보장하지 않았던 관행을 역설적으로 보여주는 문언이라고 할 수 있다.

또한 망 관리에 대한 정보를 제공받을 권리는 망 관리를 정당화하기 위한 필수적인 전제조건이다. 이는 이용자의 선택의 자유를 보장하기 위한 것일 뿐만 아니라, 사후적 통제가능성을 확보함으로써 사업자의 망 관리 권한의 남용을 통제하기 위한 절차적 보장이다. 또한 가이드라인은 이용자의 개념을 최종이용자로 정의함으로써 단대단 원칙을 기본 원칙으로 선언하고 있다.

2) 투명성

가이드라인이 선언하고 있는 두 번째 기본 원칙은 바로 트래픽 관리의 투명성이다. 이용자의 권리측면에서 이미 한번 선언한 투명성을 다시 사업자의 의무 차원에서 상세하게 규정하고 있다. 인터넷 사업자는 트래픽 관리방침을 구체적으로 공개하고 실재 조치를 하는 경우 해당 이용자에게 이를 고지해야 한다. 이 가이드라인은 구체적인 트래픽 관리의 기준을 제시하기에 앞서 트래픽 관리의 투명성을 먼저 선언함으로써 그 중요성을 강조하고 있다.

합리적인 트래픽 관리 기준이 치밀하게 제시되어도 그 준수 여부를 확인할 수 없다면 아무 의미가 없을 것이다. 통신망은 사업자의 사실적 지배 아래 있으므로 트래픽 관리의 방법이나 실시 여부에 대해서 이용자는 사업자가 알려주기 전에는 알 수 있는 방법이 사실상 없기 때문에 사업자에게 관련 정보의 공개를 강제하지 않으면 이용자는 자신의 통신의 비밀과 자유가 침해되고 있는 경우에도 이를 알기 어렵다.

3) 사업자의 의무 - 차단 및 차별 금지

세 번째와 네 번째 기본 원칙은 각각 차단 금지와 차별 금지이다. 사업자는 합법적인 트래픽을 불합리하게 차단하거나 차별해서는 안 된다. 이 또한 첫 번째 원칙, 즉 인터넷 이용자의 인터넷 이용 권리에 상응하는 사업자의 의무규정이라고 할 수 있다. 특히 차별 금지 원칙은 전기통신사업법 제3조, 제28조, 제50조에서 반복적으로 선언하고 있는 원칙을 반복하고 있는 것이며, 구체적인 내용을 더하는 바는 없다. 결국 불합리한 차별 여부는 개별적인 경우를 구체적으로 따져 봐야 판단할 수 있을 것이다. 가이드라인은 “합리적인 트래픽 관리의 필요성이 인정되는 경우”에는 합법적인 트래픽이라 하더라도 차별, 또는 차단할 수 있도록 하는 단서조항을 통해, 트래픽 관리의 필요성과 인터넷 이용의 자유를 조화시킬 수 있도록 하고 있다.

다만 차별 금지 원칙은 차단 금지 원칙에 비하여 기기 또는 장치에 대한 내용이 빠져있어, 기기 또는 장치는 차별해도 되는 것으로 잘못 해석될 우려가 있다. 그러나 일단 차단되지 않고 인터넷에 연결된 기기 또는 장치를 이용하는 행위는

당연히 트래픽을 발생시키는 행위이며, 트래픽에 대한 차별은 금지되므로 논리적으로 기기 또는 장치에 대한 불합리한 차별도 금지된다. 더 나아가 차단 금지 원칙은 차단의 합리성 여부를 따지지 않고 모든 유형의 차단을 금지한다. 그러나 아직까지는 트래픽 관리의 합리성이 무엇인지, 구체적으로 허용되는 행위가 무엇이고 금지되는 행위가 무엇인지 그 내용에 대해서는 구체적으로 알 수 없다.

4) 합리적 트래픽 관리

마지막으로 다섯 번째 기본 원칙에서 비로소 합리적 트래픽 관리의 기준을 확인할 수 있다. 가이드라인은 망의 보안성 및 안정성 확보, 망 혼잡으로부터 다수이용자의 이익 보호, 법령의 집행을 위해서 필요한 경우 등 세 가지 유형의 트래픽 관리를 합리적 트래픽 관리의 유형으로 보아 열거하고 있다. 다섯 번째 기본원칙에서 열거하고 있는 세 가지 유형은 트래픽 관리가 합리성을 가질 수 있는 가장 기본적인 경우이다. 보안, 혼잡 완화, 법집행은 모두 공공의 이익을 위한 것으로 비례성 원칙을 준수하는 범위 내에서 통신의 비밀과 자유를 제한하는 근거가 될 수 있다. 그러나 이 세 가지 유형은 예시적이며, 그 밖의 기준에 관해서는 다시 별도로 정하도록 하였다. 또한 명시적으로 유무선망의 합리적 트래픽 관리의 기준을 달리 정할 수 있도록 하고 있다.

그러나 가이드라인은 지나치게 추상적인 원칙만을 나열하고 있으며, 여전히 구체적인 트래픽 관리의 방법을 제시하지는 않는다. 그래서 P2P를 선별하여 차별적으로 차단할 수 있는지, 또는 통신사의 경제적 이익을 위해 (또는 망 유지, 관리, 보수비용의 충당을 위해) 음성 통화수익을 확보할 목적으로 mVoIP을 골라내 차단하는 것이 합리적인 트래픽 관리에 포함되는지 여부에 대해서는 분명한 기준을 확인할 수 없다.[489] 따라서 관련 당사자들은 각자의 이해관계에 따라 서로 다른 해석을 하게 되고 이해관계의 첨예한 대립으로 인해 여전히 합의를 도출하지 못하고 있다.

489) 그러나 이 가이드라인에 열거되지 않은 또 다른 트래픽 관리의 필요성이 합리적인 트래픽 관리에 포함되기 위해서는 체계적인 해석상 최소한 열거된 세 가지의 합리적인 트래픽 관리 유형의 실질과 유사한 것이어야 한다. 이렇게 제한 해석한다면 합리성의 실질을 보다 구체화할 수 있다.

4. 합리적 트래픽 관리의 기준 구체화

1) 2012년 통신망의 합리적 관리 및 이용에 관한 기준(안)

방송통신위원회는 이후 논의를 계속하여 망 중립성 및 인터넷 트래픽 관리에 관한 가이드라인의 후속조치로 2012년 7월 13일 "통신망의 합리적 관리 및 이용에 관한 기준(안)"을 발표한다. 이 기준(안)은 트래픽 관리의 합리성 판단 기준에 대하여 별도로 정하기로 한 가이드라인을 구체화하기 위한 것으로, 트래픽 관리의 기본 원칙을 선언하고 합리적 트래픽 관리로 인정되는 경우를 세분하여 설명하고 있으며, 구체적인 예시를 통해 그 의도하는 바를 분명하게 하고 있다.

그러나 해당 가이드라인은 이동통신사가 스스로 설정한 요금제에 따라 mVoIP을 차단하는 현재의 관행을 합리적 트래픽 관리로 인정하여 허용하는 예시를 포함하였으며, P2P나 헤비유저, VOD 서비스에 대한 개별적이고 특화된 데이터 이용 제한도 가능하게 하는 등, 사실상 통신사의 손을 들어준 것으로 평가되었다.[490] 이에 따라 증권사들은 통신사의 수익 증대를 예상하고 일제히 통신사 주식의 적극 매수를 권고하기도 하였다[491]

당시 KT는 이러한 흐름 속에서 유선 인터넷에도 DPI(Deep Packet Inspection)을 통한 망 관리를 시작한다고 발표하기도 하였으며 이미 이동통신망에 대해서는 KT와 SKT는 DPI 솔루션을 도입했고 LG U+는 도입을 준비 중인 것으로 알려졌다.[492] 이미 KT는 유튜브를 차단하고 있다는 의심을 받고 있었으나 공식적으로는 부인하고 있는 상황이었다.[493] 그러나 추후 언론보도를 통해 드러난 사실에 따르면 KT는 2012년 5월 관련 시스템을 유선 통신망에 설치 완료하였으며, 이를 통해 변칙적으로 운용되는 P2P 서비스도 차단할 계획이었다고 한다.[494] 삼성전자 등 제조사와 카카오톡 및 다음(DAUM) 등 컨텐츠 서비스 제공자들은 일

490) 연합뉴스, 2012년 7월 13일자, "방통위 "이통사, mVoIP 차단할 수 있다"(종합)" 참조.
491) 미디어오늘, 2012년 7월 16일자, ""보이스톡은 물론, 스마트TV, 티빙, 푹 다 차단할 수 있다" - 방통위 트래픽 관리안에 통신사들 신났다… 증권사들 일제히 매수추천 보고서" 참조.
492) 전자신문, 2012년 7월 16일자, "KT, DPI 망 관리 시작한다" 참조.
493) 이데일리, 2012년 7월 3일자, "서비스 느려졌는데, 통신사 "이상없다"..사용자만 답답" 참조.
494) 전자신문, 2012년 9월 26일자, "변칙 P2P, 차단해? 말아? KT의 '딜레마'" 참조.

제히 이에 반대 의견을 내었으며, 거센 반발에 직면한 방송통신위원회는 기준(안) 발표 공개토론회 이후 내용을 수정하여 11월에 다시 검토하였으나, 결국 추가 의견을 수렴하여 추후에 다시 논의하기로 결정하였다.

2) 2013년 통신망의 합리적 관리·이용과 트래픽 관리의 투명성에 관한 기준(안)

2013년 10월 10일 방송통신위원회에서 통신규제 기능을 이어받은 미래창조과학부는 2012년의 기준(안)을 대폭 수정하여 "통신망의 합리적 관리·이용과 트래픽 관리의 투명성에 관한 기준(안)"을 발표하였다. 개정안의 내용은 다음과 같다.

통신망의 합리적 관리이용과 트래픽 관리의 투명성에 관한 기준(안)

Ⅰ. 목적

1. 이 기준은 『망 중립성 및 인터넷 트래픽 관리에 관한 가이드라인』('11.12.26. 제정, '12.1.1. 시행)에 근거하여 합리적인 트래픽 관리 및 트래픽 관리의 투명성에 관한 세부사항을 정함으로써, 인터넷접속서비스제공사업자의 투명하고 합리적인 트래픽 관리를 유도하고 망 자원의 합리적이고 효율적인 이용환경을 조성하여 ICT 생태계의 건전하고 지속가능한 발전을 도모함을 목적으로 한다.

Ⅱ. 적용 대상

2. 이 기준은 일반적인 인터넷접속서비스에 적용되며, 관리형서비스에 대하여는 적용되지 아니한다.
   ※ 관리형서비스(managed service)는 인터넷접속서비스제공사업자가 일반적으로 통용되는 인터넷의 제공 방식과 달리 트래픽 전송 품질을 보장하는 서비스를 말한다.

Ⅲ. 트래픽 관리의 기본 원칙

3. 인터넷접속서비스제공사업자는 트래픽 증가에 대응함에 있어서 지속적인 망 고도화를 통해 이를 해결하도록 노력하여야 한다.

   인터넷접속서비스제공사업자는 원칙적으로 합법적인 컨텐츠, 애플리케이션, 서비스(이하 '컨텐츠 등'이라 한다) 또는 망에 위해가 되지 않는 기기 또는 장치를 차단하거나 컨텐츠 등의 유형 또는 제공자 등에 따라 합법적인 트래픽을 불합리하게 차별해서는 안된다.

   인터넷접속서비스제공사업자는 이 기준이 정하는 바에 따라 합리적인 범위 내에서 제한적으로 트래픽 관리를 시행할 수 있으나, 이 경우 해당 트래픽 관리의 목적에 부합하고, 트래픽 관리가 이용자에게 미치는 영향이 최소화될 수 있는 방안을 강구하여야 한다.

   인터넷접속서비스제공사업자는 트래픽 관리에 있어 유무선 등 망의 유형이나 구조, 서비스 제공방식, 주파수 자원의 제약 등 기술적 특성을 고려할 수 있다.

   인터넷접속서비스제공사업자는 서비스의 품질, 용량 등에 비례하여 요금 수준을 다르게 하거나 요금 수준에 따른 제공 서비스의 용량을 초과하는 트래픽을 관리하는 경우 이용자의 실질적 선택권 보장 등 이용자의 이익과 공정한 경쟁을 해쳐서는 안 된다. 이와 관련하여서는 관련 법령 및 요금제도에 따른다.

Ⅳ. 합리적 트래픽 관리

트래픽 관리의 합리성 판단 기준

4. 미래창조과학부는 인터넷접속서비스제공사업자의 트래픽 관리의 합리성 여부를 판단하는 경우 다음의 사항을 고려하여야 한다.

① (투명성) 인터넷접속서비스제공사업자가 트래픽 관리에 관한 정보를 사전에 충분히 공개하였는지 여부와, 구체적인 트래픽 관리 조치를 시행하는 경우 트래픽 관리로부터 직접적인 영향을 받는 이용자 또는 그 밖의 자에게 트래픽 관리에 관한 정보를 사전에 또는 부득이한 경우 사후에 충분히 고지하였는지 여부

② (비례성) 인터넷접속서비스제공사업자의 트래픽 관리 행위가 트래픽 관리의 목적·동기와 부합하는지 여부 및 당해 트래픽 관리의 영향을 최소화하는 방법을 강구하였는지 여부
※ 혼잡을 유발하는 컨텐츠가 특정될 수 있는 경우, 혼잡관리를 위해 당해 컨텐츠가 아닌 다른 컨텐츠를 제한하거나, 기기의 망에 대한 접근을 차단하는 행위는 합리적인 트래픽 관리로 보기 어려움
※ 혼잡관리를 위해 요구되는 최소한의 트래픽 관리의 수준을 넘어 필요이상으로 전송속도를 저하시키거나 트래픽을 전면 차단하는 행위는 합리적인 트래픽 관리로 보기 어려움

③ (비차별성) 유사한 형태의 컨텐츠 등, 기기 또는 장치에 대하여 불합리하게 차별하여 취급하지 않았는지 여부
※ 트래픽 관리의 필요성에 비추어 동일한 트래픽 관리가 적용되어야 할 것으로 보이는 유사한 서비스 A와 B에 대해, A서비스는 제한하고 B서비스는 허용하는 것은 합리적인 트래픽 관리로 보기 어려움

④ (기술적 특성) 유무선 망의 유형 및 구조, 서비스 제공방식, 주파수 자원의 제약 등 기술적 특성

합리적 트래픽 관리의 유형

5. 인터넷접속서비스제공사업자의 트래픽 관리가 합리적인 것으로 인정될 수 있는 경우는 다음과 같다. 다만, 향후 기술의 발전과 새로운 서비스의 등장, 인터넷 이용형태의 변화 등에 의해 나타날 수 있는 트래픽 관리행위에 대해서는 미래창조과학부가 사안별로 그 합리성 여부를 판단할 수 있다.
① DDoS, 악성코드, 해킹 또는 이와 유사한 수준의 사이버 공격 및 통신장애에 대응하기 위한 트래픽 관리 등 망의 보안성 및 안정성 확보를 위해 필요한 경우

〈예시 1〉 DDoS 공격 시 미래창조과학부 및 한국인터넷진흥원의 요청에 따라 DDoS 공격의 원인이 되는 좀비 PC를 망에서 차단하는 경우

〈예시 2〉 망에 위해를 주는 악성코드, 바이러스 등에 대응하기 위한 경우

〈예시 3〉 망의 장애 상황 또는 장애가 명백하게 예상되는 상황에서 그 원인이 되는 트래픽을 긴급히 제한할 필요성이 있는 경우
* 〈예시3〉의 상황에서 무선망의 경우 미래창조과학부의 인가를 받는 등 공신력 있는 표준화기구가 Keep Alive 신호 등에 따른 이동통신 장애에 대비하여 마련한 표준을 준수하지 않은 애플리케이션을 우선 제한 가능

② 일시적 과부하 등에 따른 망 혼잡으로부터 다수 이용자의 이익을 보호하고, 전체 이용자의 공평한 인터넷 이용환경을 보장하기 위하여, 불가피하게 제한적으로 트래픽 관리를 시행하는 경우

〈예시 4〉 유선인터넷에서 과도한 트래픽이 발생해 트래픽의 전송지연이나 패킷 손실, 새로운 접속 연결 수용 곤란 등으로 통신망의 품질 수준 저하 또는 망 장애 등이 일어나거나 발생 가능성이 객관적으로 명백한 때, 트래픽을 과도하게 유발하는 소수의 초대량이용자(heavy user)들에 한해 일시적으로 전송속도를 일정 속도이하로 제한하는 경우

〈예시 5〉 무선인터넷에서 특정지역 내에서의 일시적인 호 폭주 등 망 혼잡이 발생하였거나, 망 운영 상황, 트래픽 추세 변화, 자체 관리 기준 등에 근거하여 망 혼잡 발생 가능성이 객관적으로 명백한 때, 동영상서비스(VOD 등) 등 대용량 서비스의 사용을 일시적으로 제한하는 경우

※ 〈예시4〉와 〈예시5〉의 트래픽 관리를 시행하는 경우에도, 인터넷 검색, 이메일 등 대용량의 트래픽을 유발하지 않는 서비스는 이용할 수 있도록 하여야 함

③ 관련 법령의 집행을 위해 필요하거나 법령이나 이용약관 등에 근거한 이용자의 요청이 있는 경우

6. 인터넷접속서비스제공사업자는 미래창조과학부의 요청이 있는 경우 당해 트래픽 관리 행위의 합리성을 입증할 수 있는 객관적인 자료를 제출하여야 한다.

Ⅴ. 트래픽 관리정보의 투명한 공개

공개 대상 정보

7. 인터넷접속서비스제공사업자는 이용자의 선택권 보장을 위해, 트래픽 관리의 범위와 트래픽 관리가 적용되기 위한 조건, 절차, 방법 및 이에 따른 영향 등 자신의 트래픽 관리에 관한 정보를 이용자에게 공개하여야 하며, 제공서비스의 종류 또는 상품에 따라 차이가 있는 경우에는 이를 구분하여 표시하여야 한다.

인터넷접속서비스제공사업자는 이용자에게 실질적인 트래픽 관리정보가 제공될 수 있도록, 공개되는 정보의 내용을 지속적으로 현행화하여야 한다.

공개 방법

8. 미래창조과학부는 인터넷접속서비스제공사업자에 대하여 이용자가 이해하기 쉽고, 타 인터넷접속서비스제공사업자와 비교할 수 있도록 트래픽 관리정보 공개에 관한 공통양식(별지 참조)을 정하여 공개할 것을 권고할 수 있으며, 인터넷접속서비스제공사업자는 공통양식에 따르거나 또는 자율적으로 양식을 정하여 사용할 수 있다. 다만, 인터넷접속서비스제공사업자가 자율적 양식을 사용하는 경우에도 공통양식에 명시된 사항에 관한 정보는 반드시 포함하여야 한다.

Ⅵ. 이용자 보호

이용자에 대한 고지

9. 인터넷접속서비스제공사업자는 트래픽 관리정보에 관한 사항을 이용약관에 규정하는 외에도 인터넷 홈페이지 등 이용자의 접근이 용이한 방식을 통해 안내하여야 한다.

10. 인터넷접속서비스제공사업자가 트래픽 관리에 필요한 조치를 하는 경우에는 그 사실을 해당 이용자에게 전자우편(e-mail), 단문메시지 서비스(SMS) 등을 통하여 고지하여야 하며, 개별적인 고지가 어려운 경우에는 인터넷접속서비스제공사업자의 인터넷 홈페이지 등 다양한 수단을 통해 해당 사실을 이용자에게 널리 알리기 위하여 노력하여야 한다.

11. 인터넷접속서비스제공사업자는 개별 이용자의 자기 통제권 보장과 합리적 인터넷 이용을 위해 기술적으로 가능한 범위 내에서 이용자가 자신의 트래픽 사용현황을 확인할 수 있도록 하여야 한다.

민원처리기구의 운영

12. 인터넷접속서비스제공사업자는 트래픽 관리와 관련된 문의, 트래픽 관리에 대한 사실확인 및 이의제기 등 이용자의 민원사항을 처리할 수 있는 전담기구를 설치운영하여야 한다.

Ⅶ. 통신망 자원의 조화로운 이용을 위한 노력

13. 통신망을 이용하는 컨텐츠 등의 제공사업자와 기기 및 장비 제조사는 인터넷접속서비스제공사업자가 합리적 트래픽 관리의 필요성에 따라 트래픽에 관한 정보를 요청하는 경우 특별한 사유가 없는 한 이를 제공하여야 하며, 신규서비스 등을 개발하는 경우 망에 대한 부하를 최소화하는 기술을 적용하는 등 망의 공평하고 효율적인 관리와 활용을 위하여 노력하여야 한다.

14. 인터넷접속서비스제공사업자는 통신망을 기반으로 하는 컨텐츠 등의 제공사업자 또는 기기 및 장비 제조사가 신규서비스 개발 등을 위해 필요한 망의 관리에 관한 정보를 요청하는 경우 특별한 사유가 없는 한 이를 제공하여야 한다.

15. 인터넷접속서비스제공사업자, 컨텐츠 등의 제공사업자와 기기 및 장비 제조사는 정보의 제공 등에 대해 사업자간 협의가 이루어지지 않는 경우 미래창조과학부에 조정을 요청하거나 또는 전기통신사업법 제45조에 따라 방송통신위원회에 재정을 신청할 수 있다.

Ⅷ. 관련 법령의 준수

16. 인터넷접속서비스제공사업자가 이 기준에 따라 트래픽 관리를 시행하고자 하는 경우에는 전기통신사업 관련 법령이 정하는 바에 따라 이용약관을 개정한 후 시행하여야 한다. 다만, 기존 이용약관에 포함되어 있거나, 컨텐츠제공사업자와 인터넷접속서비스제공사업자간 협의를 통하여 정하는 사항 등 내용상 이용약관에 포함되는 사항이 아닌 경우는 제외한다.

17. 인터넷접속서비스제공사업자는 트래픽 관리를 시행함에 있어 전기통신사업법, 통신비밀보호법, 정보통신망 이용촉진 및 정보보호 등에 관한 법률 등 관련 법령을 준수하여야 하며, 미래창조과학부 등 관련 중앙행정기관의 장은 인터넷접속서비스제공사업자가 이를 위반하는 경우 관련 법령에 따라 필요한 조치를 취한다.

Ⅸ. 후속 조치

18. 인터넷접속서비스제공사업자는 미래창조과학부가 이 기준을 확정한 날로부터 6개월 이내에 트래픽 관리정보를 자사의 인터넷 홈페이지 등에 공개하여야 한다.

2013년의 통신망의 합리적 관리·이용과 트래픽 관리의 투명성에 관한 기준(안)은 그간의 논의를 통해 세 번째로 등장한 트래픽 관리 기준안으로, 2012년 처음 제시되었던 기준(안)에 비하여 개선된 모습을 보여주고 있다. 이 말은 처음 제시되었던 트래픽 관리안이 지나치게 망 중립성을 저해할 여지가 많았다는 점을 반증하는 것이기도 하다. 특히 2013년 기준(안)은 mVoIP 차단에 원용될 수 있는 예시규정이 삭제되었다는 점을 주목할 만하다. P2P 전송 제한을 합리적인 트래픽 관리로 인정하던 규정도 삭제되었다. 초 다량 이용자 트래픽 제한에 관

한 규정은 “망 혼잡시” 트래픽 관리의 예시로 변경되어 유지되었다. 기술표준을 미준수하는 서비스에 대한 제한도 “망 장애시” 트래픽 관리의 예시로 변경되어 유지되었다. 이 외에도 방송통신위원회를 미래창조과학부로 변경하여 정부조직 개편을 반영하였다.

그러나 새로운 기준(안)도 여전히 다양한 이해관계의 조정을 통한 합의를 유도하기 위한 목적으로 불명확하고 모호한 규정들을 유지하고 있는 것으로 보인다. 특히 이동통신사업자측은 기준(안) 3.이 여전히 mVoIP을 차별할 수 있는 것처럼 해석될 여지가 있는 것으로 주장하고 있어[495] 컨텐츠 사업자, 서비스 사업자, 시민단체의 입장과 충돌하고 있다. 이에 관하여 망 중립성 정책을 담당하고 있는 미래창조과학부 통신정책과장은 2013년 10월 10일 정보통신정책연구원에서 열린 “통신망의 합리적 트래픽 관리기준 마련을 위한 토론회”에서 mVoIP 차단 허용 여부에 관하여 “망 운영자 입장에서는 투자비용에 대한 생각이 분명히 있다”며 이 문제는 “옳고 그름의 문제가 아닌 자원배분, 감독과 관리의 시기 등을 염두에 두고 결정해야 할 일”이라고 하였다.[496] 망 중립성 원칙을 담당하고 있는 미래창조과학부는 여전히 이 문제를 이익형량의 관점에서 접근하고 있는 것으로 보인다.

그러나 지금까지 이 보고서를 통해 논증한 바와 같이 망 중립성 원칙은 통신의 자유와 비밀에 대한 침해라는 불법을 어떻게 정당화시킬 수 있을 것인가에 관한 문제로, 합리적 트래픽 관리기준은 바로 불법과 합법을 가르는 기준이 되어야 한다. 2011년 가이드라인의 제정을 준비하기 시작하면서부터 지난 3년간 우리나라에서 합리적 트래픽 관리의 기준을 마련하기 위한 논의가 진행되는 과정을 통해, 망 중립성 원칙을 비용부담이나 이익형량의 관점에서 당사자 간의 의견조율을 통해 구체화하려는 노력은 매우 비효율적일 수밖에 없고, 문제해결에 도움이 되지 않을 뿐만 아니라 오히려 이를 악화시키기까지 한다는 점을 경험을 통해 알 수 있었다. 보편적으로 승인된 객관적인 가치기준에 의지하지 않

495) 연합뉴스, 2013년 10월 3일자, “통신사업자에 요금제별 트래픽 관리 사실상 허용”(종합); 파이낸셜뉴스 2013년 10월 10일자 “트래픽 관리 기준안 나왔지만 mVoIP 여전히 ‘논란’” 참조.

496) ZDnet Korea 2013년 10월 11일자, “끝나지 않은 m-VoIP 논란, 무엇이 문제인가” 참조.

고서는 주장의 합리성을 논증하고 설득할 방법이 없기 때문에, 단지 치열한 이익다툼만이 남게 되고, 따라서 서로 다른 이해관계를 합리적으로 조율하는 것이 매우 어렵기 때문이다.

[참고자료] 망 중립성 모델 프레임워크

올해 10월 발리에서 열린 제8차 인터넷 거버넌스 포럼(IGF)에서는 "망 중립성 동적 연합(Net Neutrality Dynamic Coalition)"가 결성되었다. 인터넷 거버넌스 포럼이란 2006년 설립된 UN 산하의 국제포럼으로 정부기관 뿐만 아니라 다양한 이해당사자가 모여 인터넷 현안에 관하여 논의하는 공개포럼으로 특정한 주제에 관하여 이해관계자들이 "동적 연합"을 결성하기도 한다. 올해에는 대회 개최 전부터 망 중립성을 주제로 동적 연합이 결성되어 서로 소통하면서 국제적으로 적용가능한 망 중립성 모델 프레임워크를 인권친화적으로 만들어보자는 논의가 전개되었다. 점차 망 중립성이 인권차원의 문제라는 점이 국제적인 지지를 얻고 있는 것이다. 즉, 중립적 플랫폼을 잃게 된다는 것은, 인터넷 이용자들의 기본권, 표현의 자유, 정보접근권 등에 영향을 줄 수밖에 없다는 측면이 인터넷 거버넌스 포럼을 기회로 모델 프레임워크를 만들게 된 가장 큰 이유였다.

이 논의를 통해서 이 모델 프레임워크에서는 기존의 최종 이용자를 제8조 제i항에서 인터넷 이용자로 규정하고 인권적인 요소들을 다수 포함하였으며, 합리적인 수준의 트래픽 관리 규정 또한 필요 최소한도로 제한해야 함을 명시하였다. 이는 바로 망 중립성을 "옳고 그름"의 문제로 바라보고 만든 원칙이라고 할 수 있을 것이다. 따라서 감청의 위법성을 조각할 수 있는 합리적 트래픽 관리의 내용과 한계를 제시하는데 있어 중요한 참고자료가 될 것으로 생각하여 이를 번역하여 첨부하였다.[497]

497) 전문은 망 중립성 동적 연합 홈페이지 (http://networkneutrality.info/sources.html) 참조.

망 중립성 모델 프레임워크(MODEL FRAMEWORK ON NETWORK NEUTRALITY)

1) 망 중립성 원칙이라 함은 특정 컨텐츠, 서비스, 애플리케이션 또는 단말기 등에 기초해 인터넷 트래픽 전송을 차별하지 않고 인터넷 사용자의 선택의 자유를 제한하지 않기 위해 발신인, 수신인, 컨텐츠 내용에 관계없이 인터넷 트래픽을 차별, 제한 또는 개입 없이 동등하게 취급하는 것을 말한다.

2) 망 중립성 원칙에 따라 인터넷 서비스 제공자는 인터넷 트래픽 전송을 차별, 제한하거나 전송에 개입하여서는 안 된다. 단, 다음의 목적을 위해 개입이 적합하다고 판단된 경우에 한해서만 엄격하고 제한적으로 인터넷 트래픽을 관리할 수 있다.
   a) 법 이행 및 법원 명령,
   b) 네트워크, 서비스, 인터넷 사용자의 단말기의 완전성 및 보안 유지
   c) 사전에 광고 차단 조치에 동의한 인터넷 사용자에게 직접 마케팅을 목적으로 한 원치 않는 통신의 전송 방지
   d) 가입자의 명시적인 차단 요청 준수. 단, 인터넷 서비스 제공자 또는 인터넷 서비스 제공자의 제휴회사가 가입자에게 차단 요청을 독려하지 않았고 가입자가 자유의사에 따라 차단을 요청한 경우
   e) 애플리케이션을 차별하지 않는 방법으로 일시적 또는 예외적으로 발생하는 트래픽 폭주로 인한 트래픽 혼잡 완화. 단, 전술한 방법으로 문제가 해결되지 않을 경우에는 애플리케이션 특정 트래픽 속도 제한 조치를 취할 수 있음

3) 망 중립성 원칙은 신호 전송에 사용되는 기본적인 기술에 관계없이 모든 인터넷 액세스 서비스와 인터넷 서비스 제공자가 제공하는 인터넷 전송 서비스에 적용한다.

4) 망 중립성 원칙은 특별서비스(specialized service)에는 적용하지 않는다. 인터넷 서비스 제공자는 인터넷 액세스 서비스와는 별도로 특별서비스를 제공할 수 있다. 단, 이러한 서비스 제공이 인터넷 액세스 서비스, 서비스 품질, 서비스 이용성 및 성능을 저해하여서는 안 된다. 이러한 특별서비스는 차별 없이 제공되어야 하며 인터넷 이용자는 자유의지에 따라 이러한 서비스의 이용을 선택할 수 있어야 한다.

5) 인터넷 액세스 서비스 가입자는 개방형 및 전세계 단일 식별 인터넷 주소를 이용할 권리가 있다.

6) 인터넷 트래픽을 감시 또는 분석할 수 있는 어떠한 기술도 프라이버시 및 개인정보보호법을 준수하여야 한다. 이러한 기술은 헤드 정보 검사 목적으로만 사용할 수 있다. 국가개인정보보호 당국은 프라이버시 및 개인정보보호 의무 준수 평가를 위해 통신 컨텐츠를 분석 또는 검사할 수 있는 기술의 사용을 검토하여야 한다.

7) 인터넷 서비스 제공자는 제공자의 트래픽 관리 실태 및 회사의 정책 시행 특히, 인터넷 액세스 서비스 및 특별 서비스 제공 여부와 관련해 투명하고 쉽게 이해할 수 있는 정보를 제공하여야 한다. 인터넷 액세스 서비스와 특별 서비스가 네트워크 용량을 공유해서 사용할 경우 네트워크 용량에 관한 기준도 함께 적용하고 이를 명확히 명시하여야 한다.

8) 규제당국이 수행하여할 주요 업무는 다음과 같다. 관계당국이 업무를 시의 적절하게 그리고 효율적으로 수행할 수 있도록 필요한 재원을 제공하여야 한다.
   a) 인터넷 트래픽 관리 실태 및 인터넷 서비스 제공자의 정책 시행에 대해 정기적으로 감사를 시행하고 감사 결과에 대해 정기적으로 보고서를 작성하여야 하며, 망 중립성 보장을 위하여 인터넷 트래픽 관리 및 인터넷 서비스 제공자의 정책이 사용자의 기본권에 잠재적으로 미칠 수 있는 영향을 평가하고, 적합한 서비스 품질 제공 및 인터넷에 사용에 필요한 충분한 네트워크 용량을 할당하도록 하여야 한다. 이에 대한 결과보고서는 투명하게 작성되어야 하며 대중에게 공개하여야 한다.
   b) 망 중립성과 관련해 사용자의 불만이 접수되면 이를 적합한 조치를 통해 투명하고 공개적으로 그리고 효율적으로 처리하여야 한다. 모든 인터넷 사용자는 관련기관에 망 중립성 위반에 대해 신고할 수 있다.
   c) 불만이 접수되면 합리적인 시간 내에 처리하고 네트워크 망중립 원칙 위반에 대해 필요한 조치를 취하여야 한다.

5. 정당행위의 관점에서 구체화한 합리적 트래픽 관리 기준

가. 정당행위의 요건

결국 합리적 트래픽 관리의 기준은 이익형량의 관점이 아니라 "옳고 그름"의 문제로 바라볼 때 분명히 확인할 수 있다. 이해관계의 조화 관점을 떠나지 않는 한 추상적인 원칙을 선언하고 있는 현재의 가이드라인보다 구체적인 기준을 도출하기 위한 논의를 전개할 때마다 해석에 관하여 분쟁이 발생할 수밖에 없다. 그러므로 규범적 측면에서는 망 중립성 원칙의 문제를 이용자의 권리에 대한 침해와 그 정당화 문제로 접근해야 한다. 망 유지·관리비용의 문제는 경제적 측면에서 고민해야 할 문제이다. 비록 사회에서 규범적 문제와 경제적 문제가 서로 밀접하게 영향을 주고받으며, 그래서 양자가 완전히 분리될 수는 없다 하더라도, 지금의 망 중립성 논란처럼 경제적 측면이 규범적 측면을 완전히 지배하는 것을 바람직하다고 할 수도 없다는 점은 명백하다. 지금까지 정리된 옳고 그름에 대한 판단을 토대로 새로운 것으로 보이는 현상에 대해 무엇이 옳고 무엇이 그르다는 것을 말 할 수 있어야 한다.

그런데 가장 강력한 기본권 제한인 형벌을 수단으로 투입하는 것이 정당한가를 판단하기 위해서 형법이 이용하는 기준은 바로 비례성 원칙이다. 비례성 원칙이란, 가장 단순화해서 다음과 같이 말할 수 있다. 희생되는 수단보다 더 큰 목적을 달성할 수 있는 경우 그 수단의 희생은 정당화된다. 이러한 관점을 통해서 규범원칙을 판단함에 있어 경제적 문제가 "간접적으로" 고려될 수 있다. 하지만 주의해야 할 점이 있다. 지금 여기서 논의하는, "정당행위의 성립 여부"를 확인하기 위해서 판단해야 하는 것은 일차적으로는 처벌의 정당성이 아니라 처벌의 전제조건인 행위의 정당성이다. 즉 수단으로서 형벌과 목적으로서 법익보호의 가치를 비교하는 것이 아니라, 선별적 송·수신 방해를 통해서 달성하고자 하는 목적이 이로 인해 침해되는 통신의 비밀과 자유보다 큰 것인가를 확인해야 하는 것이다.

전술한 바와 같이 우리 판례는 정당행위의 정당성 판단 기준을 검토하기 위해 고려해야 할 요소를 구체적으로 제시하고 있다. "행위의 동기나 목적의 정당성,

행위의 수단이나 방법의 상당성, 보호법익과 침해법익과의 법익균형성, 긴급성, 그 행위 외에 다른 수단이나 방법이 없다는 보충성"이 바로 그것이다. 이 다섯 가지 요건은 대체로 비례성 원칙의 적합성, 필요성, 균형성과 유사한 것으로 보인다. 다만 법원은 주로 법률에 의한 기본권 제한의 정당성 판단 원리인 비례성이 원칙적으로 목적으로서의 법익과 수단으로서의 형벌 사이의 균형을 검토하는 것인데 반해, 처벌의 전제조건인 행위의 정당성을 검토해야 하는 정당행위의 사안에서는 행위를 통해 달성하고자 하는 바가 목적이 되고, 법익이 수단이 된다는 점에서, 용어의 혼동을 피하기 위해 이를 풀어 설명하고 있는 것으로 보인다. 그러므로 어떤 행위가 정당행위로 위법성이 조각되기 위해서는 위의 다섯 가지 요건을 종합적으로 고려해 보아야 한다.

다만 이 때, 판례가 제시하는 다섯 가지 요건 중 긴급성 요건은 다른 요건들을 보조하는 역할을 하는 것으로 보아야 할 것이다. 정당행위는 정당방위나 긴급피난과는 달리 긴급성을 필수적인 요건으로 하지 않는다. 다만 긴급성이 높은 경우라면 논리적으로 보다 강력한 수단이 상당성이나 균형성, 보충성 등을 충족할 가능성이 높아질 것이다. 즉 긴급성은 정당행위의 성립 가능성을 높이는 부수적인 역할을 수행한다. 그러나 본래부터 균형성 등을 충족하지 못하는 행위에 대하여 긴급성은 아무런 의미를 갖지 못한다. 그러므로 판례가 제시한 다섯 가지 요건들은 정당행위의 성립 여부를 판단하기 위하여 유기적으로 고려되어야 한다. 이하에서는 판례가 제시한 기준을 논의의 틀로 삼아, 다섯 가지 요건들을 종합적으로 고려하여, 현재 우리나라에서 합리적 트래픽 관리의 범위와 한계에 관하여 특히 논란이 되는 문제들에 관하여 옳고 그름의 문제에서 접근한 정당행위의 성립요건을 판단해 보도록 하겠다.

나. 기업의 이익추구를 위한 트래픽 관리 절대 금지

트래픽 관리가 오로지 기업의 이윤을 목적으로 하는 경우는 절대 정당화 될 수 없다. 목적이 정당하지 않은 경우 이미 수단과 비교할 대상이 존재하지 않는다. 통신기업의 이윤을 목적으로 두고 침해된 개인의 이익을 수단으로 비교할 수는 없기 때문이다. 사적 이익이 아무리 커도 타인의 작은 손해를 정당화 시킬

수 없다. 물론 사적 이익간의 비교형량을 통한 정당화 가능성에 관하여, 가치의 상대적 우위에 기반을 두는 정당화적 긴급피난의 경우를 생각해 볼 수는 있다. 그러나 정당화적 긴급피난은 나의 불이익과 타인의 불이익간의 비교임에 유의해야 한다. 나의 이익을 위해 타인에게 손해를 끼치는 행위를 우리는 범죄라고 한다. 그러므로 트래픽 관리는 오로지 통신의 비밀과 자유보다 본질적으로 우월한 공공의 이익을 위해서만 허용될 수 있다. 예컨대 통신망에 대한 공격을 방어하기 위한 경우, 또는 모두가 불이익을 겪을 수밖에 없는 혼잡을 해소하기 위한 경우에는 트래픽 관리가 정당화 될 수 있을 것이다.

다. 모든 트래픽에 대한 동등취급

1) 원 칙

mVoIP이나 스마트 TV 등 경쟁서비스를 이용하는 패킷을 식별하여 차별취급하기 위한 목적의 DPI도 당연히 그 위법성이 조각되지 않는다. 이러한 차별취급은 거의 대부분 그 궁극적인 목적이 기업의 이윤 극대화에 있기 때문이다. 따라서 모든 패킷은 동등취급하는 것이 원칙이고 차별은 불합리한 것으로 추정해야 한다. 그러므로 통신사의 패킷에 대한 선별적 송·수신 방해에 대한 사실상의 입증, 즉 실제 이동통신망을 통해 mVoIP을 이용하는 것이 패킷 손실로 인해 불가능한 상황이라는 점에 대한 입증만 있으면, 그 행위는 이미 통신비밀보호법상 구성요건 해당성이 확인된 것이며, 통신사가 별도로 정당화사유를 입증하지 못하는 경우 처벌되어야 한다. 상술한 바와 같이 경제적 측면은 정당화 사유가 될 수 없다. 통신사는 시장의 경쟁구조를 부당하게 왜곡하여 추가적인 이익을 취하려고 해서는 안 된다. 이러한 행위는 통신의 비밀과 자유를 침해하는 것을 수단으로 하여 다시 재산상의 손실까지 입히는 행위로 이용자의 법익에 대한 이중의 침해가 된다.

망 구축 및 유지비용은 경제적 측면에서 고려되어야 하며, 투명하게 산출된 내역을 제시하고 적정한 요금을 만들어서 정당하게 받는 이용료로 감당해야 한다. mVoIP으로 인한 음성 매출 감소는 음성통화의 품질과 편의성 경쟁, 요금인하 등으로 극복해야 할 것이며, 궁극적으로는 데이터 중심 요금제로 전환하는

것이 방법이 될 것으로 생각된다. 문자서비스는 이미 카카오톡이라는 데이터 기반 인스턴트 메신저와의 경쟁을 극복하지 못하고 대부분의 요금제에서 추가 비용 부담 없이 무제한 제공됨으로써 결국 사실상 무료화 되었음을 참고해야 한다. 이미 이동통신사의 음성통화도 VoLTE로 전환되고 있는 추세이다. VoLTE 음성통화에 대하여 데이터 통화 요금과는 다른 별도의 요금체계를 유지한다면 이는 결국 동일한 데이터 통신을 용도에 따라 구별하여 다른 요금을 부과하는 것이 된다.

망 중립성 규제가 지나치게 경쟁을 제한하는 것이라는 반박에 대하여도 다음과 같은 재반박이 가능하다. 이익은 경쟁의 원동력이며, 경쟁을 통해야 발전을 거둘 수 있다. 만약 시장구조를 왜곡시켜 추가적인 이익을 얻을 수 있도록 놔둔다면, 통신사는 경쟁의 원동력을 잃게 된다. 즉, 합리적이고 적절한 망 중립성에 대한 규제는 경쟁 촉진적인 규제가 되는 것이다.

2) 예외와 그 한계

다만 예외적으로 사적 이익을 목적으로 하지 않는 차별적 취급은 정당화 될 수 있다. 예컨대, 정보의 불법성에 대한 판단이 정당하다는 것을 전제로, 불법정보의 유통을 차단하기 위한 경우나, 또는 DDoS 공격이 막 진행되는 중 이에 대하여 대처하기 위한 경우 등을 생각해 볼 수 있을 것이다. 그러나 이 경우에는 추구하는 공익이 침해되는 통신의 비밀과 자유에 비하여 중대해야 하고(균형성), 다른 방법으로는 그 목적을 달성할 수 없어야 함이 명백해야 한다(보충성). 균형성과 보충성에 관한 판단이 명확하지 않은 경우, 그 입증은 차별취급을 하려는 망 관리자에게 있으며, 입증에 실패하면 위법성은 조각되지 않는다. in dubio pro reo의 원칙이 적용되어야 하는 상황이 아니기 때문이다.

상술한 바와 같이 여기서 검토하는 정당성에 관한 판단은 국가 형벌권에 대한 것이 아니라, 이용자의 통신의 비밀과 자유를 침해하는 행위에 관한 것이다. 본래 "증명책임", 즉 증명불분명의 위험은 검사에게 있으나, 위법성 조각사유에 대한 입증의 부담은 피고인이 진다.[498] 따라서 트래픽을 차별취급 하고자 하는 통신사는 그 행위의 균형성과 보충성을 스스로 입증하여야 하며, 입증에 실패하고

공론경쟁을 통해 논란을 불식하지 못한다면 차별취급은 정당행위로 정당화될 수 없다.

라. 필수적 전제로서 보충성 원칙

DPI 장비를 이용한 프라이버시 침해적 망 관리는, 만약 아예 감청의 구성요건에 해당하지 않아서 불가벌이 되거나 또는 보다 가벼운 침해로도 목적을 달성할 수 있는 다른 기술적 수단이 있는 경우, 절대 허용되어서는 안 된다. 그러므로 수단이 목적과의 관계에서 정당성, 상당성, 긴급성, 균형성을 모두 갖춘 경우라 하더라도 오직 다른 가벼운 수단을 찾을 수 없을 때에만 정당행위가 성립할 수 있다. 이를 다른 말로 최소침해의 원칙, 또는 필요성의 원칙이라고 한다. 다른 방법으로 목적을 달성할 수 있음이 명백한 경우에는 설사 그 목적이 아무리 중대한 이익이라 하더라도, 예컨대 사이버 보안이라 해도, 인터넷 이용자의 통신의 비밀과 자유를 침해하는 것을 결코 정당화 시킬 수 없다.

패킷의 차별적 취급도 보충성 원칙이 준수된다면 정당화 될 가능성이 생긴다. 즉 다른 요건을 모두 충족하는 것을 전제로, 통신의 내용에 따른 차별 말고는 문제 해결의 가능성이 없을 때에만 패킷의 차별 취급을 수단으로 하는 트래픽 관리가 정당화 될 수 있다. 그런데 현실적으로 이러한 경우는 많지 않을 것으로 생각된다. 예컨대 전체 이용자가 이메일이나 웹 검색 서비스 등을 원활하게 이용할 수 있도록 하기 위해서 기술적으로 VOD나 P2P 서비스만을 선별하여 차단하는 것 외에는 방법이 없을 때에만 서비스의 차별이 가능할 것이다. 그러나 이러한 문제는 소수의 다량이용자의 전체 트래픽을 차별 없이 축소하는 것만으로도 망 혼잡으로 인한 다른 이용자의 불편은 사라질 것이다. 어떤 서비스를 우선 이용할 것인지는 이용자의 선택의 자유인 것이다. 이때에도 통신사는 계약조건을 통해 최저 보장속도를 설정하고 준수하여야 한다.

게다가 망 혼잡에 대해서는 언제나 망 시설투자나 통신기술 개발이 언제나 다른 수단으로 제기된다. 따라서 망 혼잡을 해결하기 위한 차별적 송·수신 방해

498) 배종대/이상돈/정승환/이주원, 신형사소송법, 제5판, 홍문사, 2013, 51/30.

행위의 보충성은 원칙적으로 약화되어있는 상태라고 하겠다. 물론 문제가 된 시점에서 시설투자나 기술개발에 지나치게 과다한 비용이 소요되어 객관적으로 불가능한 상황이라면 요금을 올리거나, 아니면 이용자에게 제공하는 최저 보장 속도를 낮추어야 할 것이며, 또는 이용자에게 사실을 상세하게 알리고 특정 서비스가 제한될 수 있다는 점에 대하여 선택권이 보장된 실질적인 동의를 받아 구성요건 해당성을 배제해야 할 것이다. 이때 이용자의 선택권은 모든 패킷에 대한 차별 없이 상대적으로 낮은 최저 보장속도로 운영되는 서비스와, 특정 서비스는 금지되지만 이메일이나 웹서핑 등 통상의 인터넷 서비스는 상대적으로 높은 최저 보장속도로 운영되는 서비스를 선택하게 함으로써 실질적으로 보장될 수 있다.

마. 투명성의 절차적 보장

그러나 실질적으로 망 관리가 어떠한 방법으로 이루어지는지에 관해서 이용자는 알 수 있는 방법이 없다. 다만 경험적으로, 또는 통계적으로 대규모의 조사를 통해서 특정한 패킷의 송·수신이 차별당하고 있는 사실을 추정할 수 있을 뿐이다. 망 관리 실무는 전적으로 통신사가 장악하고 있는 통신설비 위에서 이루어지기 때문이다. 그러므로 상술한 원칙들이 준수되는지 여부를 객관적으로 검증하는 것은 통신사의 협조 없이는 불가능하다. 그러나 이해당사자인 통신사가 자발적으로 이에 협조할 가능성은 거의 없으므로, 제도를 통해 투명성을 절차적으로 보장해야 할 것이다. 2010년 미국 FCC가 오픈 인터넷 규칙을 만들면서 “투명성”을 망 중립성 원칙의 핵심적인 원칙으로 포함시킨 것은 바로 이러한 이유이다.

같은 맥락에서 우리 통신비밀보호법은 이미 투명성 보장에 관한 절차적 규정을 가지고 있다. 내용은 다음과 같다.

통신비밀보호법

제2조(정의) 이 법에서 사용하는 용어의 정의는 다음과 같다. (중략) 7. “감청”이라 함은 전기통신에 대하여 당사자의 동의없이 전자장치 · 기계장치 등을 사용하여 통신의 음향 · 문언 · 부호 · 영상을 청취 · 공독하여 그 내용을 지득 또는 채록하거나 전기통신의 송 · 수신을 방해하는 것을 말한다. 8. "감청설비"라 함은 대화 또는 전기통신의 감청에 사용될 수 있는 전자장치 · 기계장치 기타 설비를 말한다. 다만, 전기통신 기기 · 기구 또는 그 부품으로서 일반적으로 사용되는 것 및 청각교정을 위한 보청기 또는 이와 유사한 용도로 일반적으로 사용되는 것중에서, 대통령령이 정하는 것은 제외한다. (후략)

제10조(감청설비에 대한 인가기관과 인가절차) ① 감청설비를 제조 · 수입 · 판매 · 배포 · 소지 · 사용하거나 이를 위한 광고를 하고자 하는 자는 미래창조과학부장관의 인가를 받아야 한다. 다만, 국가기관의 경우에는 그러하지 아니하다. ② 삭제 ③ 미래창조과학부장관은 제1항의 인가를 하는 경우에는 인가신청자, 인가연월일, 인가된 감청설비의 종류와 수량 등 필요한 사항을 대장에 기재하여 비치하여야 한다. ④ 제1항의 인가를 받아 감청설비를 제조 · 수입 · 판매 · 배포 · 소지 또는 사용하는 자는 인가연월일, 인가된 감청설비의 종류와 수량, 비치장소 등 필요한 사항을 대장에 기재하여 비치하여야 한다. 다만, 지방자치단체의 비품으로서 그 직무수행에 제공되는 감청설비는 해당 기관의 비품대장에 기재한다. ⑤ 제1항의 인가에 관하여 기타 필요한 사항은 대통령령으로 정한다.

통신비밀보호법 시행령

제3조(감청설비 제외대상) 법 제2조제8호 단서에 따라 감청설비에서 제외되는 것은 감청목적으로 제조된 기기 · 기구가 아닌 것으로서 다음 각 호의 어느 하나에 해당하는 것을 말한다. 1.「전기통신사업법」 제2조제4호에 따른 사업용전기통신설비 (후략)

패킷의 선별적 송·수신 차단을 위해 패턴을 분석하는 DPI 장비는 바로 제2조 제8호가 정의하고 있는 감청설비에 해당한다. 감청에 “사용될 수 있는” 설비이기 때문이다. DPI 장비가 사용자의 의도에 따라 인터넷 사용 내용을 구체적으로 복원하여 확인하거나 인터넷 전화의 도청을 위해서도 사용될 수 있음은 앞에서 설명하였다. 따라서 DPI 장비를 이용하기 위해 도입하려는 자는 제10조에 의해 미래창조과학부장관의 인가를 받아야 하며, 미래창조과학부장관과 DPI 장비를 사용하는자는 인가사항을 대장에 기재하여 비치하여야 한다. 그러나 현재 우리나라에서 대부분의 통신사가 DPI 장비를 도입하여 활용하고 있음에도 불구하고, 인가나 대장 비치는 이루어지지 않고 있는 것으로 확인된다. 통신비밀보호법 시행령 제3조가 사업용전기통신설비를 감청설비에서 제외하고 있기 때문이다. 사업용전기통신설비란 “전기통신사업에 제공하기 위한 전기통신설비”를 말하는 것으로 통신회사가 이용하는 DPI 장비는 여기에 해당한다.

그러나 이러한 규범구조는 음성통신을 전제하고 있는 것으로 보인다. 음성통

신인 경우 극히 예외적인 경우를 제외하고는 사업자에게 감청의 유인이 없다. 타인간의 통신을 몰래 듣는다 해도 이는 범죄에 해당할 뿐이며, 기업의 이윤을 높여주지 않기 때문이다. 그래서 통신사가 이용하는 전기통신설비에 대하여 투명성을 강요하는 것은 그 목적에 비해 비용이 과다하였고, 그래서 시행령 제3조는 이를 감청설비에서 제외하고 있는 것이다. 그러나 데이터 통신의 경우, 통신사는 선택적 송·수신 차단을 통해 경쟁서비스를 차별하고, 망 유지비용을 축소하여 막대한 경제적 이익을 취할 수 있다. 따라서 비록 사업용전기통신설비라 하더라도 DPI 장비에 대해서는 별도의 규정을 마련하여 투명성을 강화하는 것이 바람직할 것으로 보인다. DPI 장비 자체를 등록하도록 하고, 모든 사용 내역을 디지털 로그파일의 형태로 기록에 남기도록 한다면, 그리 부담스럽지 않은 비용으로 망 중립성 원칙의 핵심 세부원칙인 투명성을 강력하게 절차적으로 보장할 수 있을 것이다. 더 나아가 우선 DPI 장비를 도입할 때 내용을 사람이 인지할 수 있을 정도로 복원해 내는 해당하는 기능에 대한 삭제 역시 절차적으로 보장되어야 한다. 정보처리기기의 기능은 얼마든지 소프트웨어적으로 추가가 가능하므로, 장비의 구체적인 사용 내역이나 업데이트 여부 등도 모두 기록에 남도록 해야 할 것이다.

제5장

요약 및 정책제언

전 현 욱

05

요약 및 정책제언

1. 요 약

CIA와 미국 국가안보국(NSA)에서 일했던 미국의 컴퓨터 전문가인 스노든(Snowden)에 의해 미국과 그 동맹국의 정보기관들이 프리즘(PRISM)이라는 비밀 정보수집 프로젝트를 통해 전세계의 통화기록과 인터넷 사용정보를 무차별적으로 감청해왔다는 사실이 폭로된 이후, 인터넷 시대의 프라이버시에 관한 국제사회의 움직임이 가속화되고 있다. 지난 11월 1일에는 브라질과 독일이 함께 "디지털 시대의 프라이비권(The Right to Privacy in the Digital Age)"에 대한 결의안 초안을 UN 총회에 제출하였고, 최근 이 결의안은 총회 산하 제3위원회를 만장일치로 통과하여 12월 UN 총회에 상정될 예정이다. 2010년 미국 FCC가 오픈 인터넷 규칙을 통해 망 중립성 원칙을 선언한 것도 디지털 정보의 감청에 대한 취약성으로 인해 프라이버시에 대한 우려가 확장되고 있기 때문이다.

프라이버시는 민주사회를 구성하는 기본원리로, 시민의 기본권이며 형법상 법익으로 매우 강력한 보호를 필요로 한다. 프라이버시에 대한 새로운 침해 우려는 형사정책적 관점에서 적극적으로 검토되어야 하고, 관련 정책은 법익보호의 관점에서 합리적으로 구체화되어야 한다. 이 보고서는 바로 이러한 시대적 변화에 특히 형사정책이 민감해야 한다는 점을 강조하기 위하여 기획되었다. 그리고 지금까지의 논의를 통해 현행 법률과 법치국가적 형법이론의 범위 내에서 비교적 합리적으로 망 중립성과 프라이버시의 문제를 다룰 수 있음을 논증하였다.

제2장에서는 왜 망 중립성의 문제를 형사정책적 시각에서 검토해야 하는가를

설명하였다. 이를 논증하기 위하여 먼저 통신비밀보호법상 불법감청 구성요건의 적용범위를 분석하였다. 이어 망 중립성 침해행위의 본질이 패턴분석을 통한 통신의 비밀 침해와, 선택적 송·수신 차단을 통한 통신의 자유 침해에 있음을 확인하고, 국내의 사례와 이를 둘러싼 논의의 전개과정을 살펴본 후, 이를 토대로 인터넷 이용자의 관점에서 법익 보호의 필요성을 논증하였다. 또한 필요한 범위 내에서 DPI 기술의 작동원리를 살펴보고, DPI 기술의 사용을 통해 침해되는 이익과 달성될 수 있는 목적을 검토하였다. 결국 디지털 통신은 자동화된 정보처리로 인해 기존의 음성 통신과는 근본적으로 다른 특징이 있으며, 따라서 망 중립성을 침해하는 행위, 즉 DPI와 같은 장비를 이용하여 모든 패킷의 패턴을 실시간으로 감시하고 이에 기반하여 선별적으로 송·수신을 차단하는 행위는 개인의 통신의 비밀과 자유를 침해하는 행위가 된다. 또한 현행 통신비밀보호법 제2조의 감청에 대한 정의가 이러한 행위를 포섭할 수 있도록 되어있어 법률의 제·개정 없이도 형법적 법익보호를 실현할 수 있음을 확인하였다. 그러므로 데이터 통신의 선택적 송·수신 차단행위는 별도의 정당화사유가 없는 한 통신비밀보호법상 감청의 불법에 해당하는 것으로 보아야 한다. 그러나 아직 관련된 논의가 충분히 성숙되지 않았으며, 규범의 인식이 정보기술의 발전으로 인한 현실의 변화속도를 미처 따르지 못하고 있어, 여전히 망 중립성의 문제는 이해관계의 충돌 내지는 비용의 분담 문제로 인식되고 있다. 그러나 규범의 인식부재로 인해 객관적 가치규범을 확인할 수 없는 영역에서는 이익의 크기를 비교할 척도를 발견할 수 없기 때문에, 이해관계의 조화라는 관점에서 망 중립성의 정책의 내용을 구체화하는 것은 사실상 불가능하다. 망 중립성 정책, 즉 합리적 트래픽 관리의 범위는 개인적 이익에 대한 침해라는 측면에서 바라봐야 비로소 내용이 명확해지며, 구성요건 해당행위의 불법 조각을 위한 요건을 검토하는 것을 통해서 구체화될 수 있다.

제3장에서는 뜻하지 않게 주어진 국제공동연구의 기회를 활용하여, 미국 FCC의 오픈 인터넷 규칙을 비롯하여, 캐나다, 영국(EU), 호주의 망 중립성 정책 관련 논의 현황을 살펴보았다. 인터넷은 국경을 초월한 정보통신 수단으로 이에 관한 국가정책은 당연히 국제적인 관점에서 검토되어야 한다. 그러나 우리나라뿐만 아니라 세계적으로 망 중립성에 대한 정책은 아직 수립 과정 중에 있으며,

따라서 통신비밀보호 또는 프라이버시 보호와 망 관리에 관한 각국의 분쟁 현황과 규제기관의 정책동향은, 국가마다 그 접근의 방향에 있어서 서로 조금씩 다른 모습으로 나타나고 있다. 망 중립성에 관한 주요원칙 대체로 동일하나 각 국가의 규제 관점 및 가치기준에 따라 그 문제를 제기하는 방법에서부터 망 중립성 원칙의 세부적인 내용이나 강도, 법제화 방법에서 크고 작은 차이를 보이고 있다. 따라서 각각의 합리성을 비교분석하는 것은 망 중립성과 프라이버시의 가치를 확인하고, 합리적 트래픽 관리의 허실에 관한 다양한 관점과 이를 바탕으로 하는 논증의 타당성을 구체적으로 확인할 수 있는 기회가 되며, 따라서 우리나라의 정책방향 설정에 있어서 좋은 참고자료가 된다.

제4장에서는 지금까지의 논의를 토대로 통신비밀보호법상 불법감청 구성요건에 해당하는 행위의 불법을 조각하기 위한 요건을 크게 “동의”와 “정당행위”의 관점에서 구체적으로 살펴보았다. 통신비밀보호법상 감청 동의는 형법이론상 이른바 “양해”에 해당하며, 구성요건 해당성을 배제하는 것으로 보아야 한다. 다만 통신의 비밀과 자유는 원칙적으로 법원이 발부한 허가장을 통해서만 제한될 수 있는 것으로 동의가 허가장을 우회하는 수단이 되어서는 안 되며, 따라서 설령 양해에 해당한다 하더라도 그 요건은 형법 제24조에서 규정하고 있는 피해자의 승낙에 준하여 엄격하게 검토되어야 한다. 또한 “합리적 트래픽 관리”가 업무로 인한 정당행위가 되기 위한 요건을 살펴보았다. 이를 위해 2011년 제정된 우리나라의 당시 방송통신위원회의 망 중립성 및 인터넷 트래픽 관리에 관한 가이드라인과 2013년 10월 만들어져 현재 논의되고 있는 통신망의 합리적 관리·이용과 트래픽 관리의 투명성에 관한 기준(안)의 내용을 검토하였다. 끝으로 이러한 논의를 토대로 형법이론적 관점에서 정당행위가 되기 위한 합리적 트래픽 관리의 범위와 한계를 제시하였다. 현행법과 법치국가적 형법이론의 검토를 통해 도출된 망 중립성 정책은 항목을 바꿔 상술한다.

2. 정책제언 – 망 중립성 정책의 기본 원칙

가. 구성요건 해당성을 배제하기 위한 동의의 요건

① 원칙적으로 자신의 통신에 대한 동의만이 가능하다. 타인을 위한 감청 동의는 그 감청이 명백하게 피감청자에게 이익이 되는 경우에만 예외적으로 허용될 수 있다.

② 당해 통신에 참여하는 모든 당사자가 동의해야 한다. 그러므로 수신자의 수신 거부는 기술적으로 망 차원이 아니라 수신자의 단말기 차원에서 실현되어야 한다.

③ 망 중립성을 제한하고자 하는 통신사는 이용되는 기술의 작동원리 및 통신의 비밀과 자유에 대한 침해 범위를 비전문가인 이용자가 이해할 수 있을 정도로 상세하게 설명해야 한다. 충실한 설명이 없다면 법이 정하고 있는 고지의무를 위반하는 것이 된다.

④ 동의를 거부할 수 있어야 한다. 거부 가능성은 형식적인 것이어서는 안 되며 거부하더라도 동등한 서비스를 이용할 수 있어야 한다. 그렇지 않은 약관은 강행규정 위반으로 무효이다.

나. 정당행위가 되기 위한 합리적 트래픽 관리의 범위와 한계

① 사적 이익, 즉 기업의 이윤 극대화를 위한 추구를 위한 트래픽 관리는 절대 허용되어서는 안 된다. mVoIP이나 스마트 TV에 대한 송·수신 차단은 균형성 원칙을 충족할 수 없다.

② 모든 트래픽은 동등하게 취급되어야 한다. 사적 이익을 위한 차별적 취급은 통신의 비밀과 자유는 물론 재산까지 침해하는 이중의 법익침해가 된다. 다만 예외적으로 중대한 공익을 위한 차별적 취급은 정당화될 수 있다. 이 경우 입증책임은 통신사에게 있다.

③ 보다 가벼운 침해로도 목적을 달성할 수 있는 다른 수단이 있는 경우 절대 허용되어서는 안 된다.

④ 투명성은 절차적으로 보장되어야 한다. 망 관리는 전적으로 통신사가 장악

하고 있는 통신설비 위해서 이루어지기 때문에, 이를 사후적으로라도 검증할 수 있도록 적절한 정보 제공을 절차적으로 보장하는 것이 중요하다

참고문헌

[국내문헌]

단행본

국회정치관계법심의특별위원장, 통신비밀보호법안(대안), 1993. 12.

김일수/서보학, 새로쓴 형법총론, 제11판, 박영사, 2006.

미래창조과학부 주최, 정보통신정책연구원 주관 “통신망의 합리적 트래픽 관리 기준 마련을 위한 토론회”(2013. 10. 10) 자료집

박상천 의원 외 93인, 통신비밀보호법안, 1993. 5.

배종대, 형법총론, 제11판, 홍문사, 2013.

배종대/이상돈/정승환/이주원, 신형사소송법, 제5판, 홍문사, 2013.

이상돈, 법학입문, 법문사, 2009.

이상돈/홍성수, 법사회학, 박영사, 2000.

한국방송통신전파진흥원, 글로벌 모바일 망 중립성 현황과 전망, 2012.

.

연구논문

강유리, “인터넷 트래픽 관리와 DPI” 방송통신정책 제 25권 8호 통권 553호, 2013.

권오걸, 피해자의 승낙과 양해, 법학논고 제20집, 2004.

김보라미/박건철/이봉규, 이동통신사에 의한 mVoIP 서비스 차단의 법적 문제, 정보법학, 제16권 제1호, 2012.

김성규, 피해자의 승낙에 관한 법리로서의 자기결정권, 비교형사법연구 제8권 제1호, 2006.

김성환, 망 중립성의 개념과 쟁점의 이해, 정보통신포럼 2007, 법원사, 2008.

김천수, 망 중립성에 대한 공법적 고찰, 한국외국어대학교 박사학위논문, 2012.
김혁돈, 추정적 의사의 확정과 절차적 정당화, 비교형사법연구 제10권 제1호, 2008.
김형준, 현행 통신비밀보호법의 문제점과 개선방안 - 통신제한조치와 대화감청을 중심으로 -, 형사법연구, 제24호, 2005.
박희영, DPI 기술의 운영과 ISP의 형사책임, Internet and Information Security, 제2권 제1호, 2011.
배종대, 보안처분과 비례성원칙, 배종대/김일수 편, 법치국가와 형법, 세창출판사, 1998.
손동권, 양해·승낙의 구분에 따른 구체적 법 효과 차이의 문제, 형사법연구 제23권 제3호, 2011.
오길영, 감청의 상업화와 그 위법성, 민주법학, 제43호, 2010.
오길영, 인터넷 감청과 DPI, 민주법학, 제41호, 2009.

원형식, 소위 "예방적 정당방위"에 관한 연구, 형사법연구, 제16호, 2001.
윤용규, 긴급피난 규정의 이해와 입법론적 검토, 형사법연구, 제22호, 2004.
이용식, 피해자의 승낙에 관한 소고, 동산 손해목박사화갑기념논문집, 1993.
이정원, 법익주체의 동의로서 승낙과 양해, 법학논총 제16권 제2호, 2009.
임규철, 망 중립성, 비교법연구 제11권 제2호, 2011.
임영덕, 미국 미디어 규제와 망 중립성에 대한 고찰, 미국헌법연구, 제21권 제3호, 2010.
장윤정, m-VoIP 서비스에서의 망 중립성에 대한 법적 검토, Ewha Law Review 제2권 제2호, 2012.
전응준, 개인정보보호법률상 형사처벌규정의 적정성에 관한 연구, 정보법학, 제17권 제2호, 2013.
전현욱, 개인정보 보호에 관한 형법정책, 고려대학교 박사학위논문, 2010.
전현욱, 지적재산권과 형법정책, 경원법학 제3권 제2호, 2010.
전현욱, 해킹의 형법적 규율 방안, 고려대학교 석사학위논문, 2000.
정석균, IT Network 정책방향에 대한 연구 : 망 중립성과 효율성을 중심으로,

디지털정책연구 제10권 제1호, 2012.
정영철, 인터넷접속서비스와 망 중립성 - 사업자권한과 국가권련간 균형을 중심으로, 정보법학, 제14권 제2호, 2010.
정진연, 연명치료중단에 관한 형법적 고찰, 법학연구 제36편, 2009.
차진아, 사이버범죄에 대한 실효적 대응과 헌법상 통신의 비밀 보장, 공법학연구, 제14권 제1호, 2013.
최승재, 경쟁법의 관점에서 본 망 중립성에 대한 연구, 언론과 법 제10권 제2호, 2011.
최석윤, 피해자의 승낙과 양형, 피해자학연구 제5호, 1997.
하태훈, 통화자일방의 동의를 받은 제3자의 전화녹음과 통신비밀보호법 위반, 안암법학, 제17호, 2003.
홍명수, 통신산업에서의 시장지배적 사업자 규제에 관한 연구 : 전기통신사업법상 문제를 중심으로, 명지대학교 석사학위논문, 2009.
황주연, 유럽에서의 망 중립성 논의 경향, 정보통신정책 제23권 6호, 2011.

〈국외문헌〉

Vaile, David/Watt, Renee, Inspecting the Despicable, Assessing the Unacceptable: Prohibited Packets and the Great Firewall of Canberra, UNSW Law Research, 2009.
Attorney-General's Department, Surveillance Devices Act 2004 Report for the Year ending 30 June 2012, 2013.
BEREC Report on differentiation practices and related competition issues in the scope of net neutrality, Document number: BoR (12) 132, 2012.
Bowden, Caspar, The US National Security Agency (NSA) surveillance programmes (PRISM) and Foreign Intelligence Surveillance Act (FISA) activities and their impact on EU citizens' fundamental rights, European Parliament Civil Liberties Committee, 2013.
Broadband Industry Technical Advisory Group, By-laws of Broadband Industry Technical Advisory Group S, 2012.

Broadband Initiatives Program, Broadband Technology Opportunities Program Notice, 74 Fed. Reg. 33104, 33110.11, 2009.

Brown, Ian, Lawful Interception Capability Requirements, Computers and Law, 2013.

Canadian Association of Internet Providers, Re: Part VII Application by the Canadian Association of Internet Providers Requesting Certain Orders Directing Bell Canada to Cease and Desist from "Throttling" its Wholesale ADSL Access Services, 2008.

Chirico, Filomena/Haar, Ilse Van der/Larouche, Pierre, Network Neutrality in the EU', TILEC Discussion Paper, 2007.

Conroy, Stephen, Media release: Child abuse material blocked online, removing need for legislation, 2012.

Conroy, Stephen, Convergence Review and Finkelstein Inquiry, 2013.

Convergence Review Committee, Convergence Review Final Report, 2012.

Cooper, Alissa, How Regulation and Competition Influence Discrimination in Broadband Traffic Management: A Comparative Study of Net Neutrality in the United States and the United Kingdom, Thesis submitted for the degree of DPhil, University of Oxford, 2013.

CRTC, Telecom Decision CRTC 2005-28: Regulatory framework for voice communication services using Internet Protocol, 2005.

CRTC, Telecom Decision CRTC 2008-108: The Canadian Association of Internet Providers' application regarding Bell Canada's traffic shaping of its wholesale Gateway Access Service, 2008.

CRTC, Telecom Decision CRTC 2011-44, Ottawa, 25 January 2011: Usage-based billing for Gateway Access Services and third-party Internet access services, File number: 8661-C12-201015975, 2011.

CRTC, Telecom Information Bulletin CRTC 2011-609: Internet traffic management practices – Guidelines for responding to complaints and enforcing framework compliance by Internet service providers, 2011.

CRTC, Telecom Public Notice CRTC 2008-19 - Notice of consultation and hearing: Review of the Internet traffic management practices of Internet service providers, 2008.

CRTC, Telecom Regulatory Policy CRTC 2009-657: Review of the Internet traffic management practices of Internet service providers, 2009.

CRTC, The conversation in CRTC, Transcript of Proceeding: Review of the Internet traffic management practices of Internet service providers, vol 1, 2009.

David, Paul A, The Evolving Accidental Information Super-Highway, Oxford Review of Economic Policy, 2001.

Department of Broadband, Communications and the Digital Economy Consultation paper: Mandatory internet service provider (ISP) filtering: Measures to increase accountability and transparency for Refused Classification, 2009.

Department of Justice Office of Public Affairs, Justice Department Charges Leaders of Megaupload with Widespread Online Copyright Infringement, 2012.

Department of Justice, Comments on Network Neutrality in Federal Communications Commission Proceeding, 2007.

European Commission, Consultation on the Commission's comprehensive approach on personal data protection in the European Union, 2012.

European Commission, Declaration on Net Neutrality, appended to Directive 2009/140/EC, O J L 337/37, 2009.

European Data Protection Supervisor, Opinion on net neutrality, traffic management and the protection of privacy and personal data, 2011.

European Parliament, Final Report on the Existence of a Global System for the Interception of Private and Commercial Communications (ECHELON Interception System), Temporary Committee on the ECHELON Interception System, 2001.

FCC, In AT&T Inc and BellSouth Corp Application for Transfer of Control, 22 FCC Rcd 5562, 2007.

FCC, Internet Policy Statement 05-151, 2005.

FCC, Madison River Communications, LLC, Order, DA 05-543, 20 FCC Rcd 4295, 2005.

FCC, Memorandum Opinion and Order, 23 FCC Rcd 13028 ('ComcastOrder'), 2008.

FCC, NOTICE OF PROPOSED RULEMAKING- Before the Federal Communications Commission Washington, D.C. 20554, 2009.

FCC, Report and Order Preserving the Open Internet, 25 FCC Rcd 17905, 2010.

FCC, Report on a Rural Broadband Strategy, 2009.

Federal Communications Commission, Appropriate Framework for Broadband Access to the Internet over Wireline Facilities, Policy Statement, 2005.

Frieden, Rob, Rationales for and Against Regulatory Involvement in Resolving Internet Interconnection Disputes, 14 Yale J.L. & Tech 266, 2012.

Goldberg Mark, Canada Leads World With Net Neutrality Regulatory Framework, CircleID, 2009.

Gould Carol, The Information Web, Ethical and Social Implications of Computer Networking, Boulder, 1989.

Green Party of Canada, Vision Green, Green Party of Canada, 2007.

Haddadi, Hamed/Fay, Damien/Uhlig, Steve/Moore, Andrew W/Mortier, Richard/AJamakovic, lmerima, Analysis of the Internet's structural evolution, Technical Report UCAM-CL-TR-756, University of Cambridge, Computer Laboratory, 2009.

Hahn, Robert/Wallsten Scott, The Economics of Net Neutrality, AEI Brookings Joint Center for Regulatory Studies, 2006.

Hardy, Keiran, Operation Titstorm: Hactivism or cyber-terrorism? UNSW Law Journal, 2012.

House of Commons Debates, 39th Parl, 1st Sess, No141, 2007.

House of Commons Debates, 40th Parl, 2nd Sess, Vol 144 No 078, 2009.

Industry Canada, Does the Minister intend to allow telecommunications companies to determine the content that its customers can and cannot access by imposing special rates, undermining net neutrality?, Question Period Card in Telecommunications Policy Branch, Network Neutrality – Questions and Answers, 2006.

Kang, Jerry, Information Privacy In Cyberspace Transactions, Stanford Law Review, 1998.

Koops, Bert-Jaap/Sluijs, Jasper P, Network Neutrality and Privacy According to Art. 8 ECHR, European Journal of Law and Technology, 2012.

La Rue, Frank, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Human Rights Council seventeen session, 2011.

Lardinois, Frederic, Facebook And FTC Settle Privacy Charges — No Fine, But 20 Years Of Privacy Audits, Tech Crunch, 2012.

Lemley, Mark A./Lessig, Lawrence, The End of the end-to-end: preserving the architecture of the nternet in the broadband era, UC Berkeley Public Law Research Paper, 2010.

Lessig, Lawrence, Code and other Laws of Cyberspace, 김정오 역, 코드 - 사이버공간의 법이론, 나남출판, 2002.

MacKinnon, Rebecca, The network is aware: Social science research on deep packet inspection, 2013.

Make Your Voice, 2008 Election Campaign Kit, Canadian Library Association, 2008.

Marsden, Christopher T, Net Neutrality: Towards a Co-regulatory Solution, Bloomsbury Academic, London, 2010.

Marsden, Christopher T, Regulating Intermediary Liability and Network Neutrality, Chapter 15, pp701-750 in 'Telecommunications Law and Regulation, Oxford, 4th edition, 2012.

Matthews, Bruce, International Training Program 2011: The Australian Internet Security Initiative, Australian Communications and Media Authority, 2012.

Musiani, Francesca/Löblich, Maria, Net Neutrality from a Public Sphere Perspective, The Value of Network Neutrality for the Internet of Tomorrow, 2013.

OECD, OECD Broadband statistics. 2a Households with broadband access 2000-10. 2011.

OECD, OECD Broadband statistics. 2d Business use of broadband, 2003-2010 or latest available year, 2011.

OECD, Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data, 2013.

OECD, Working Party on Telecommunication and Information Services Policies - Internet Traffic Prioritisation: An Overview (DSTI/ICCP/TISP(2006)4/FINAL), 2007.

Parsons, Christopher, Deep Packet Inspection in Perspective: Tracing its Lineage and Surveillance Potentials, New Transparency Project, 2008.

Rauhofer, Judith/Bowden Caspar, Protecting Their Own: Fundamental Rights Implications for EU Data Sovereignty in the Cloud, Edinburgh School of Law Research, 2013.

Richelson, Jeffrey T/Ball, Desmond, The Ties That Bind: Intelligence Cooperation Between the UKUSA Countries. Allen & Unwin., 1985.

Scott, Marcus/Pieter, Nooren/Cave, Jonathan, Carter Kenneth R, Network Neutrality:Challenges and responses in the EU and in the U.S, European Parliament, 2011.

Sluijs, Jasper P/Schuett, Florian/Bastian, Henze, Transparency regulation in broadband markets: Lessons from experimental research, 35 Telecommunications Policy 592.602 for an experimental analysis of transparency regulation in broadband, 2011.

Souter, David, Human Rights and the Internet : a review of perception in human rightos rganisations, APC, 2012.

Telecommunications Policy Review Panel, Final Report, 2006.

Telstra, Trialling new network management techniques - Myth buster, 2013.

Telus Communications Inc, Submission to the Departments Industry Canada and Canadian Heritage: Response to Consultation on Digital Copyright Issues, 2001.

Varadarajan V. Chari, Internet filtering-Issues and challenges, Security & Privacy, IEEE, 8(4), 2010.

Wu, Tim, Network Neutrality, Broadband Discrimination, Journal of Telecommunications and High Technology Law, Vol. 2, 2003.

〈언론보도〉

Agence France-Presse, 2013년 10월 9일자, "Brazil to host Internet governance summit next year"

Ars Technica, 2007년 11월 5일자, "BitTorrent blocking goes north: Canadian ISP admits to throttling P2P" by Ryan Paul

Ars Technica, 2008년 11월 20일자, "Canadian regulators allow P2P throttling" by Nate Anderson

Ars Technica, 2008년 4월 23일자, "Vuze says some ISPs abuse TCP resets; data not that clearcut" by Iljitsch van Beijnum

BBC, 2013sus 6월 13일자, "Phone hacking: Arrests by investigation"

Bell Canada, 2008년 11월 20일, "Bell welcomes CRTC decision allowing wholesale Internet network management"

Canadian Association of Internet Providers, 2009년 5월 21일자, "Application to Review and Vary Telecom Decision CRTC 2008-108"

CBC, 2006년 11월 2일자, "Battle over 'net neutrality' arrives in Canada"

CBC, 2008년 10월 17일자, "CRTC delays ruling on Bell's throttling"

CBC, 2008년 11월 20일, "We're not endorsing internet throttling: CRTC"

CBC, 008년 11월 20일자, "CRTC allows Bell to continue internet throttling"

CBC, 2008년 3월 25일자, "Bell crimps P2P file-sharing during peak hours"

CBC, 2008년 4월 21일자, "David Bazan et al, Audio-CD: Rock The Net: Musicians For Network Neutrality"

CBC, 2008년 4월 21일자, "NDP calls for net neutrality"

CBC, 2008년 4월 22일자, "Cogeco ranks poorly in internet interference report"

CBC, 2008년 5월 26일자, "Internet protesters to descend on Ottawa"

CBC, 2008년 5월 27일자, "NDP to introduce 'net neutrality' private member's bill"

CBC, 2009년 11월 23일자, "Re: Review of the Internet traffic management practices of Internet service providers, Telecom Public Notice CRTC 2008-19"

CBC, 2011년 8월 30일, "Rogers asked to probe possible game throttling"

DSL Reports, 2008년 3월 24일자, "Bell Canada Throttles Wholesalers, Doesn't Bother To Tell Them" by Karl Bode

Forbes, 2011년 10월 2일자 "Net Neutrality Star Tim Wu Joins Federal Trade Commission as Senior Policy Advisor"

Green Party, 2007년 4월 5일자, "Green Party alarmed by recklessness of Bernier's rush to deregulation"

itnews, 2010년 1월 1일자, "Analysis: The murky world of deep packet inspection"

Liberal Party Newsroom, 2009년 6월 19일자 "Liberals speak out in support of net neutrality"

Market News, 2009년 9월 6일자, "Bell Silently Closes Online Video Store" by Christine Persaud

National Post, 2006년 3월 23일자, "Review panel takes step in right direction"

National Union of Public and General Employees, 2007년 8월 3일자, "NUPGE seeks action on Internet access and net neutrality"

National Union of Public and General Employees, 2008년 2월 20일자, “Consultations and legislation needed to protect net neutrality”

National Union of Public and General Employees, 2008년 3월 28일자, "NUPGE asks CRTC to investigate Internet ‘traffic shaping’”

National Union of Public and General Employees, 2008년 4월 28일자, “NUPGE asks federal Liberals to join net neutrality campaign”

NBC News, 2007년 10월 19일 “BitTorrent, Comcast (CMCSA) Shake Hands, Downloaders Still Screwed”

New America Foundation, 2007년 2월 15일자, “Wireless Net Neutrality: Cellular Carterfone and Consumer Choice in Mobile Broadband” by Tim Wu

Office of the Privacy Commissioner of Canada, 2008년 11월 21일자, “CRTC begins dialogue on traffic shaping”

Open Media, 2011년 10월 27일자, “It’s Official: Gamers have Caught Rogers Violating Internet Openness Rules”

Open Media, 2011년 8월 4일자, “Canadian Gamers Fed Up With CRTC on Net Neutrality issues”

Slyck News, 2006년 9월 9일자, “CBC Reporting on Today’s Entertainment Trends”

Telephony Online, 2009년 1월 23일자, “Comcast’s Congestion Catch22”.

The New York Times, 2005년 8월 1일 “Telus cuts subscriber access to pro-union website”

The New York Times, 2005년 8월 1일자 “A Canadian Telecom’s Labor Dispute Leads to Blocked Web Sites and Questions of Censorship”

The New York Times, 2012년 1월 4일자, “Internet access in not a human right”

The Province, 2011년 9월 16일자, “CRTC tells Rogers to stop throttling online games”

The Toronto Star, 2007년 10월 8일자 “Canadians deserve better ISP transparency” by Michael Geist

The Toronto Star, 2008년 11월 20일자, “Bell can squeeze downloads, CRTC rules”

The Tyee, 2008년 4월 9일자, “‘Throttling’ Net Traffic” by Tom Barrett

TorrentFreak, 2008년 4월 18일자, “First Results from Vuze Network Monitoring Tool”

TorrentFreak, 2010년 12월 13일자, “Rogers’ BitTorrent Throttling Experiment Goes Horribly Wrong”

Xconomy, 2008년 3월 24일자 “How Network Non-Neutrality Affects Real Businesses”

뉴시스, 2012년 5월 4일자, “방통위 “KT 삼성 스마트TV 접속 차단 위법이나 경고””

디지털 데일리, 2012년 2월 10일자 “삼성전자, KT 스마트TV 접속차단에 가처분 신청으로 맞불”

미디어오늘, 2012년 7월 16일자, ““보이스톡은 물론, 스마트TV, 티빙, 푹 다 차단할 수 있다” - 방통위 트래픽 관리안에 통신사들 신났다… 증권사들 일제히 매수추천 보고서”

아시아경제, 2009년 4월 7일자, “이통사 vs 인터넷 업계 ‘공짜 전화’격돌”

아시아경제, 2012년 2월 9일자 “김효실 KT 상무 “법률검토 마쳤다.””

아시아경제, 2012년 2월 9일자 “삼성·LG “KT, 스마트TV 차단 부당””

연합뉴스, 2012년 2월 9일자 “KT “스마트TV 연결 인터넷망 즉시 차단”(1보)”

연합뉴스, 2012년 7월 13일자, “방통위 “이통사, mVoIP 차단할 수 있다”(종합)”

이데일리, 2012년 7월 3일자, “서비스 느려졌는데, 통신사 “이상없다”. 사용자만 답답”

이투데이, 2013년 4월 9일자, “이통사, 인터넷 무료통화 확대…보이스톡 품질불량은 그대로?”

전자신문, 2012년 7월 16일자, “KT, DPI 망 관리 시작한다”

전자신문, 2012년 9월 17일자, “모바일 인터넷전화(mVoIP) 허용 논란”

전자신문, 2012년 9월 26일자, “변칙 P2P, 차단해? 말아? KT의 ‘딜레마’”

전자신문, 2013년 7월 17일자 “공정위, 이통사 mVoIP 차단 관련 무혐의 결론”

파이낸셜, 2012년 2월 16일자, “OIA “KT, 삼성 스마트TV 접속 차단 망 중립성 위반””

한겨레, 2013년 6월 26일자, “망 과부하 초래 사업자에 추가비용 받아야”

〈판례〉

Dowling v United States, 473 US 207, 222 (1985).

Ford v. Attorney General (Quebec), [1988] 2 SCR 712.

대법원 1086. 10. 28. 86도1764.

대법원 1983. 2. 8. 82도2486.

대법원 1993. 7. 27. 92도2345.

헌법재판소 2005.5.26. 선고, 99헌마513.

〈기타〉

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce').

Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive).

Directive 2002/58/EC on Privacy and Electronic Communications: Article 5(1)

Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) (Text with EEA relevance).

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data:

Article 2(h).

Directive 98/48/EC of the European Parliament and of the Council.

Abstract

Criminal Policy on Net Neutrality and Communication Confidentiality

Chun, Hyun-Wook

The Protection of Communications Secrets Act clarifies the definition of 'tapping'[499] and regulates protection of secretes of communications and conversation.[500] Under the Act, any person who intercepts transmission and reception of electronic communications of others shall be punished by imprisonment with prison labor for not more than 10 years or by suspension of qualification for not mare than 5 years[501]. In reality, Internet Services Providers (ISPs) in Korea inspect and classify communications of subscribers in

499) Article 2 Definition
(7) the term "tapping" means acquiring or recording the contents of telecommunications by listening to or openly reading the sounds, words, symbols or images of the communications through electronic and mechanical devices without the consent of the party concerned or intercepting transmission and reception of electronic communication

500) Article 3 Protection of Secretes of Communications and Conversation
(1) No person shall censor any mail, wiretap any telecommunications, provide the communication confirmation data, record, or listen to conversations between others that are not made public without following the provisions under this Act, the Criminal Procedure Act or the Military Court act

501) Article 16 Penal Provisions
(1) Any person falling under any of the following subparagraphs shall be punished by imprisonment with prison labor for not more than 10 years or by suspension of qualification for not more than 5 years; 1. A person who has censored any mail, wiretapped any telecommunications or recorded or eavesdropped on any conversations between other individuals in violation of the provisions of Article 3

real time before blocking or throttling traffic that passes over their network by using interception technologies such as Deep Packet Inspection (DPI) for the purpose of maximizing their profits. Their practices practically violate Net Neutrality. Net neutrality is the principle that ISPs should treat all data on the Internet equally. Logically, it is possible for ISPs to control traffic of certain packets or contents only after they inspect all contents accessed via their network in real time. In other words, "inspection" is prerequisite for traffic management. "Inspection" and "Interception" are key elements of trapping specified in the Protection of Communications Secrets Act. In this regard, any practice violating net neutrality constituting tapping falls under an illegal practice without justifiable reasons specified in laws. Unfortunately a illegal tapping under the Protection of Communications Secretes Act, especially with regard to violation of principles of net neutrality, has not yet drawn much attention in criminal law field.

On the other hand, net neutrality issues appear to be subject to passing costs from either an ISP to a third party ISP or an ISP to end-users within the framework of the civil law and the administrative law. Until now, the Korea Broadcasting and Communication Commission and the Fair Trade Commission considered violation of net neutrality as a temporary or microscopic issue of comparing profits and losses. Most of their decisions issues were in favor of ISPs as network discrimination is not widely viewed as tapping within the big picture of criminal law and normative standards and normative standards of net neutrality has not yet firmly established and advances in information and communication technologies much outpace the laws and policies that govern it. Absent of legal framework to govern net neutrality could to increase in conflict of interest between service providers or between them and consumers but no justifiable solution to deal with it has not been founded. That is the reason why arguments of ISPs, who control network and have the upper hand against consumers and other els, is bought. Simply put, imprecise principles of net

neutrality seems to give indulgence to large network providers, for unreasonable discrimination of traffic, rather than protect the weak, consumers and others else.

In modern society, free and equal access to the Internet is an essential prerequisite to ensure freedom of expression and to provide people with grounds where they freely and openly exchange ideas and opinions. As we already experienced that lack of adequate norms and legal framework could lead to what we see now with the advent of IT technologies. We already achieved consensus on the fact that freedom of communication must be protected. Against this backdrop, it is left to address strictly violation of net neutrality that must be included in the elements of tapping. From the beginning, legislators of the Act use technical terms such as "electronic communication", "interception of transmission and reception" to incorporate future development in technologies within the scope of not undermining clarity of them. Challenges we face might be stemmed from differences from interpreting the act and applying it to real cases as the key way of communication is changing from voice-based to data-based. We could understand those challenges and find appropriate solutions on traditional principles of the criminal law. In this regard, net neutrality issues should be discussed from the viewpoint of criminal justice to protection of legal interests and then we could know where future policy directions would head for.

Internet-based data communication and voice-based one is different technically as the former is processed via an automatic dapa processing system. That is the reason that prevention measures are needed to prevent the internet from using for illegal purposes. As communication network systems are finite resources, extra charges should be imposed on users who cause traffic congestion in proportion to the amount of data they use. However, the problem is who will bear congestion costs on the network. In other words, if ISPs are not making profits, the internet would be neither maintained nor improved. To address traffic congestion, 'reasonable traffic management' by

ISPs is required. In criminal law, reasonable traffic management is exempted from illegal practice of tapping. Therefore this specific characteristic of managing traffic should be considered in interpreting the elements of an offense under the Act. In fact, packets being conveyed on the network system is automatically analyzed and identified via Deep Packet Inspection (DPI) technologies. However, doing that constitutes tapping as data containing telecommunication informations are processed and stored as intended. Put it simple, using DPI technologies could be translated as an interception of human beings. Acquiring processed packet information does not constitute the elements of tapping under the Act. There are loopholes in acquiring users' prior consent because they must agree to follow 'Use Policy --unilaterally established-- by ISPs in order to be provided with access to a network or to the Internet and prior consent is included in the use policy. That is the reason that the current ISPs practices of using DPI technologies to manage traffic are not seen as legitimate disposition of legal benefit.

Policies on Net neutrality should consider violation of it as illegitimate tapping. To this end, exceptions should be reviewed under the Protection of Communications Secrets Act to justify certain practices and acts and exmept them from the elements of tapping. The paper presents reasons and necessities why net neutrality should be reviewed from the criminal law viewpoint. Chapter Ⅱ explains grounds behind the argument that net neutrality should be approached not from the perspective of network management but from violation of users' rights and then reviews legal aspects of network discrimination and the elements of illegal tapping under the Protection of Communications Secrets Act. Chapter Ⅲ looks at net neutrality issues at home and abroad so as to provide base information on possibilities and limits of justifiable exceptions when it comes to tapping. First, it closely loot into issues on net neutrality and communication confidentiality in Canada which puts importance on striking balance between free internet use and reasonable

network management and the United States which is known for ISP-friendly business environment. With arguments and logics of numerous parties, I could understand conditions for "reasonable traffic management" which is directly and indirectly being materialized. Then it presents discussions and efforts to deal with net neutrality issues in the United Kingdom, which is heavily influenced by legislation of the European Union. Legal developments in the country give insight into normative elements that must be considered in justifiable exceptions of illegitimate tapping, such as consumers prior consent and legal judgment on 'tapping' which undermining net neutrality. It also implies how hard to enforce the law against ISPs which practically control the network systems. Chapter 4 closely examine legal implications of 'prior consent' and 'justifiable exception' as an acceptable reason for the exemption of illegality of tapping under the Act. Prior consent in the Protection of Communications Secrets Act is equivalent to 'permission' in theories of criminal law and may be understood as providing specific exceptions to tapping. Communication confidentiality or freedom is only restricted based on warrant issued by the court. Therefore prior consent must not be interpreted as the warrant. Even if prior consent is equivalent to 'permission', the elements of an offence have to be strictly construed based upon consent of victim in Article 24 of the Criminal Law. The paper also examines conditions of 'reasonable traffic management' to constitute justifiable exceptions based on "Guidelines on New Neutrality and Traffic Management" and "Guidelines on Reasonable Traffic Management and Internet Use and Transparency in Traffic Management", both of which were established and published by the Korea Broadcasting and Communication Commission in 2011 and 2013 respectively. At last, this paper suggests directions for criminal policies to address acts and practices violating net neutrality. Then it looks to procedural and institutional measures to make parties in conflict of interests involved comply with the guidelines.

부록

The Emergence of Net Neutrality Regulation in Canada: How Canada Developed a Consensus Policy on One of the Internet's Most Contentious Issues

Michael Geist

Canada Research Chair in Internet and E-commerce Law

University of Ottawa, Faculty of Law

September 2013

1. Introduction

Network neutrality has generated an increasing amount of attention in Canada and around the world in recent years.[1] While the definition of net neutrality is open to some debate, at its core is the commitment to ensuring that Internet service providers (ISPs) treat all content and applications equally with no privileges, degrading of service or prioritization based on the content's source, ownership or destination. According to Tim Wu, the Colombia Law School professor who is often credited with coining the term,[2] network neutrality is a "design principle" that requires the public network to "treat all content, sites, and platforms equally."[3] Adopting a neutral approach, in other words, requires strict adherence to one cardinal rule: that ISPs transport data without discrimination, preference, or regard for content.

The concern over net neutrality is not new. Observers have long feared that ISPs would succumb to economic self-interest, engaging in "packet preferencing" by blocking or slowing data coming from competing sites or services.[4] ISPs frequently argue that they merely want to serve as intermediaries without regard for what traverses their networks (i.e. the end-to-end approach). Yet, as they offer competing Internet phone services, music download services, and other value-added content, there is an obvious temptation to create a home network advantage.

Several concerns are often raised in the context of net neutrality. First, there is the fear of the emergence of a "two-tier Internet". As providers build faster networks, there is reason to believe that they will seek additional compensation to place content on the "fast lane" and leave those unwilling to pay consigned to a slow lane. Such a two-tier structure can cause major issues that undermine competition. For example, larger studios' television shows and movie productions could be delivered more quickly to consumers because those studios have paid for the fast lane (or have the same owner as the ISP), while smaller studios' products and user-generated content creeps along in the slow lane. The issue of competition is closely connected to the expansion of digital economy. Many e-commerce companies and other innovators rely on network neutrality, secure in the knowledge that the network treats all companies, whether big or small, equally. This neutrality enables those with the best products and services, not the deepest pockets, to emerge as the market winners.

---

[1] See, e.g., "Battle over 'net neutrality' arrives in Canada", *CBC* (2 November 2006); "NDP calls for net neutrality", *CBC* (21 April 2008) online: CBC <http://www.cbc.ca/>; David Bazan et al, Audio-CD: *Rock The Net: Musicians For Network Neutrality* (Thirsty Ears: 2008); Canadian Liberty Association, "2008 Election Campaign Kit" at 7, online: CLA <http://www.cla.ca/ >; and "Liberals speak out in support of net neutrality", *Liberal Party Newsroom* (19 June 2009) online: Liberal Party of Canada <http://www.liberal.ca/>.

[2] See, e.g., "Net Neutrality Star Tim Wu Joins Federal Trade Commission as Senior Policy Advisor", *Forbes* (2 October 2011) online: Forbes <http://www.forbes.com/>.

[3] See Tim Wu et al, "Network Neutrality FAQ", online: Tim Wu <http://timwu.org>.

[4] See, e.g., David P Reed, Jerome H Saltzer & David D Clark, "Active Networking and End-To-End Arguments"; Mark A Lemley & Lawrence Lessig, "The End of End-to-End: Preserving the Architecture of the Internet in the Broadband Era"; and David Clark & Marjory Blumenthal, "Rethinking the Design of the Internet: The End to End Arguments vs. the Brave New World", online: The Center for Internet and Society <http://cyberlaw.stanford.edu/>.

Other issues and concerns related to network neutrality include fundamental legal rights such as the privacy of online users and freedom of speech. The notion that ISPs should be permitted to block or degrade access to some content or applications not only undermines economic competition but also violates core Charter of Rights and Freedoms values of privacy and freedom of speech. Moreover, the concern over privacy is aggravated by the lack of transparency in the so-called "traffic shaping."

The Canadian experience with net neutrality has featured a steady stream of consumer and business concerns that have ranged from incidents such as Telus blocking access to a union supporting websites during a labour dispute (and blocking more than 600 other sites in the process) to Rogers degrading the performance of certain applications such as BitTorrent.[5] These incidents are described in further detail below.

In terms of neutral access to online content, Canadian law raises some interesting questions. While not directly applicable to a private sector company, the Charter of Rights and Freedoms guarantees Canadians "freedom of thought, belief, opinion and expression." The Supreme Court of Canada ruled in *Ford v. Attorney General (Quebec)* that freedom of expression extends beyond the speaker to the listener, who also has an interest in freedom of expression.[6] ISPs may not be subject to the *Charter*, but it is reasonable to expect that all Canadian corporations should aspire to abide by its principles.

The *Telecommunications Act* is also relevant to the issue of net neutrality with two provisions repeatedly raised in regulatory proceedings.[7] First, section 27(2) forbids unjust discrimination in the provision of a telecommunication service. This section is primarily applicable to competing services, though blocked websites may well fit within the definition. Second, Section 36 of the *Act* provides that "[e]xcept where the Commission [i.e. CRTC] approves otherwise, a Canadian carrier shall not control the content or influence the meaning or purpose of telecommunications carried by it for the public."[8] This provision has been carefully parsed to consider the scope of the terms "control" and "influence the meaning."

---

[5] See Michael Geist's testimony in House of Commons, Standing Committee on Industry, Science and Technology, *Evidence*, No 047 (26 February 2007) at 1635.
[6] *Ford v. Attorney General (Quebec)*, [1988] 2 SCR 712.
[7] *Telecommunications Act*, SC 1993, c 38.
[8] Ironically, *Telus* whose blockage set a crucial precedent for net neutrality in Canada had in 2001 relied on section 36 to support the notion that there should be limited liability for ISPs since they act as intermediaries with no control or influence over the content that runs on their systems. In their submission to the government on copyright policy, they further explained that "an ISP does not initiate the transmission of information; nor does it select the recipients of the transmission, nor does it select, control, influence or modify the information contained in the transmission." [Telus Communications Inc, "Submission to the Departments Industry Canada and Canadian Heritage: Response to Consultation on Digital Copyright Issues" (14 September 2001), online: Industry Canada <http://strategis.ic.gc.ca/eic/site/crp-prda.nsf/eng/home>] In fact, because of its benefits for Internet users, network neutrality has in the past played an important role for ISPs to increase their customers and invest heavily in new infrastructure, and to fostered greater competition and innovation. In fact, research shows that "the incentive for the broadband service provider to expand under net neutrality is unambiguously higher than under the no net neutrality

With a steady stream of net neutrality complaints and until recently uncertainty about the applicability of existing laws to the issue, Canadian ISPs, content creators, and consumers were left with limited guidance on the legality of many traffic management practices. This led to a series of regulatory proceedings that ultimately fostered the development of net neutrality policies that have been lauded by many as among the best in the world.[9] This paper traces the evolution of Canadian net neutrality policy. Part two identifies the early net neutrality warning signs, that captured the attention of several digital rights groups and started the movement toward a national regulatory policy. Part three focuses on the growing demands for a net neutrality policy that unfolded from 2006-09. Part four provides a detailed look at the regulatory hearing on Internet traffic management policies, which directly addressed net neutrality. Parts five and six assess the resulting policy and challenges of enforcement that soon followed.

2. 2004-06: The Net Neutrality Warning Signs in Canada

Warning signs about the possibility of net neutrality violations in Canada date back to at least 2004. As part of the CRTC's public consultation on Internet telephony or voice-over-IP (VOIP) services in the fall of 2004, the parent company of at least one major ISP gave every indication that it did not view third party services favourably. Quebecor, which owned Videotron, a leading Quebec-based cable ISP, told the Commission that Internet-based telephony services such as Vonage contributed nothing to the development of facilities-based competition.[10]

A year later, Telus, one of the largest telecommunications companies in Canada, actively blocked access to "Voices for Change", a website supporting the Telecommunications Workers Union. The company had been embroiled in a contentious labour dispute with the union, yet its decision to unilaterally block subscriber access to the site was unprecedented. Telus argued that the site contained confidential proprietary information and that photographs on the site raised privacy and security issues for certain of its employees.[11] Nevertheless, the blockage of the site was ineffective since it remained available to anyone outside the Telus network. Moreover, those within the Telus network could access the site by using proxy services.

---

regime. This goes against the assertion of the broadband service providers that under net neutrality, they have limited incentive to expand." [Hsing K Cheng, Subhajyoti Bandyopadhyay & Hong Guo, "The Debate on Net Neutrality: A Policy Perspective" (2011) 22:1 Information Systems Research 1].

[9] See, e.g., Mark Goldberg, "Canada Leads World With Net Neutrality Regulatory Framework", *CircleID* (21 October 2009) online: CircleID <http://www.circleid.com/>.

[10] See Canadian Radio-Television and Telecommunications Commission (CRTC), *Telecom Public Notice CRTC 2004-2: Regulatory framework for voice communication services using Internet Protocol*, vol 3 (Gatineau: CRTC, 2004) at paras 4470-71.

[11] See "Telus cuts subscriber access to pro-union website", *CBC* (24 July 2005) online: CBC <http://www.cbc.ca/>; and Ian Austen, "A Canadian Telecom's Labor Dispute Leads to Blocked Web Sites and Questions of Censorship", *The New York Times* (1 August 2005) online: The New York Times < http://www.nytimes.com>.

Although Telus ultimately obtained a court order barring the site from posting content with the intent of threatening company employees, the company's unilateral blocking raised a host of challenging legal issues. Telus argued that its subscriber contract granted it the right to block content. While that might have been true for its roughly one million retail subscribers at the time, the blockage occurred at the Internet backbone level, thereby blocking access for other ISPs (and their customers) that used Telus as their wholesale provider.

The Telus actions were not alone in raising net neutrality concerns. Rogers Communications, Canada's largest cable Internet provider, quietly employed "traffic shaping" technologies, thereby reducing access to peer-to-peer services such as BitTorrent as well as the downloading of podcasts from services such as iTunes. This traffic shaping occurred despite the fact that BitTorrent was legal in Canada and was used by many open source software developers and independent artists and filmmakers. By reducing the bandwidth available for this application, Rogers impaired the ability for Canadian artists to distribute their work and hampered the development of open source software in Canada.[12]

In response to this traffic shaping, many file sharing applications began to employ encryption to make it difficult to detect the contents of data packets. This, in turn, led to a technical "cat and mouse" game, with heightened levels of encryption to circumvent ISPs' bottlenecks.[13] On the other hand, the use of encryption raised the possibility of ISPs mistaking other encrypted applications (such as emails and remote desktop applications) for encrypted file-sharing content and, thereby, slowing those applications down as well. Rogers packet shaping also raised several important consumer concerns. For instance, it was difficult to reconcile how the company could advertise a service offering specific speeds and a maximum cap on data transfers, yet secretly hamper the ability for consumers to make full use of the service for which they had paid.[14]

---

[12] Peer-to-peer traffic shaping has caused other –collateral– damages as well. According to the CEO of Glance Networks, "some Web conferencing providers have seen their services slow to a crawl in some regions of the world because of poorly executed traffic management policies." Furthermore, "[s]ince ISPs often deny they use such practices, it can be exceedingly difficult to identify the nature of the problem in an attempt to restore normal service." [Rich Baker, "How Network Non-Neutrality Affects Real Businesses" (24 March 2008), online: Xconomy <http://www.xconomy.com/>].

[13] See "Canada" under "Bad ISPs" in Vuze Wiki <http://wiki.vuze.com/>. In the U.S., *Comcast* engaged in similar traffic shaping [see Peter Svensson, "Comcast blocks some Internet traffic", *NBC News* (19 October 2007) online: NBC News <http://www.nbcnews.com>] although it eventually struck a deal with *BitTorrent* [see Dan Frommer, "BitTorrent, Comcast (CMCSA) Shake Hands, Downloaders Still Screwed", *Business Insider* (27 March 2008) online: Business Insider <http://www.businessinsider.com/>].

[14] Some described Rogers traffic shaping as only "bandwidth resource management" and, hence, not a violation of net neutrality [See for instance Mark Evans, "Rogers: It's Bandwidth Management; Not Throttling" (13 April 2007), online: Mark Evans Tech <http://www.markevanstech.com>]. This labeling seemed to be a distinction without a difference. The traffic shaping certainly made it difficult to access certain applications and content. The issue was whether the technical constraints were "reasonable." Given the impact of traffic shaping on many other encrypted data, the fact that consumers had paid for a set amount of monthly bandwidth, and the fact that the constraints rendered some applications all but unusable indicate that the technical constraints were arguably unreasonable ground to violate net neutrality.

Not to be left out of the net neutrality debate, Bell Canada, Canada's largest ISP, opened up on the traffic shaping issue by advising customers that they might engage in network management to address excessive bandwidth use. Yet, the disclosure failed to satisfy the critics. For instance, Bell's so-called unlimited data plan contract featured fine print that prohibited "multi-media streaming, voice over Internet protocol or *any other application which uses excessive network capacity*."[15] Bell also acknowledged that it engaged in traffic shaping peer-to-peer applications such as BitTorrent.[16]

Bell's arguably most controversial practice, however, was throttling Internet traffic for its wholesale services without disclosing the practice to its wholesale partners.[17] To do this, Bell began installing "deep packet inspection" (or DPI) capabilities into its network. The DPI capabilities allow ISPs to identify the type of content that runs on their networks and render it possible for them to manage the traffic based on the content. The throttling practices raised at least three crucial competition issues.

First was its effect on ISP competition, particularly in Ontario and Quebec. In fact, the CRTC had tried to address limited ISP competition in Canada by requiring companies such as Bell to provide access to third-party ISPs that "resell" Bell service with regulated wholesale prices. Wholesale level throttling lessened the ability for independent ISPs to differentiate their services and therefore to compete in the marketplace. The second competition concern was the effect on ISP services such as the secure virtual private networks (or VPNs) used by companies and video streaming employed by many broadcasters. With DPI and throttling in place, Bell would be positioned to implement premium pricing for services that business took for granted, thereby raising costs and cutting independent ISPs out of the picture. The third competition concern brought a cultural dimension to the issue. The major ISPs claimed that throttling was needed to ensure better quality of service to all customers, yet it also had a significant effect on the video marketplace as cable and satellite companies began to sell new video on demand services to consumers.[18]

Finally, a 2008 study conducted by Vuze, an online video site based on BitTorrent protocol, placed another Canadian provider, Cogeco, in the spotlight. To track ISP network management techniques, Vuze created a plug-in that allowed users to measure network interruptions. Interruptions (i.e. reset messages) might occur in the ordinary course of network activity or

[15] Michael Geist, "Canadians deserve better ISP transparency", *The Toronto Star* (8 October 2007) online: The Toronto Star <http://www.thestar.com/> ; see also "Bell crimps P2P file-sharing during peak hours", *CBC* (25 March 2008) online: CBC <http://www.cbc.ca>.
[16] See Ryan Paul, "BitTorrent blocking goes north: Canadian ISP admits to throttling P2P", *Ars Technica* (5 November 2007) online: Ars Technica <http://arstechnica.com/>.
[17] Karl Bode, "Bell Canada Throttles Wholesalers, Doesn't Bother To Tell Them", *DSL Reports* (24 March 2008) online: DSL Reports <http://www.dslreports.com/>.
[18] It must be noted that *Bell* itself acknowledged that traffic shaping may backfire due to "adverse publicity" [see *Bell Canada*, "Management's Discussion and Analysis: Risks That Could Affect Our Business and Results", online: Bell Canada <http://www.bce.ca/>].

might be the result of false messages used to hamper peer-to-peer file sharing. Based on an enormous amount of data, Vuze ranked the major ISPs. The ISP with the highest percentage of resets was U.S.-based Comcast. Surprisingly, however, Canada's Cogeco, offering service in Quebec and Ontario, ranked second. Moreover, none of the major Canadian providers fared particularly well.[19]

3. 2006-09: The Demand for Net Neutrality Regulation Mounts in Canada

Concerns about website blocking, packet preferencing or discrimination against competitive Internet telephony services, doubts about the effectiveness of ISP action against spam, and fears about ISP protection of customer private data in light of law enforcement surveillance requirements, led to increasing calls for a new national ISP accountability framework in Canada. With regard to network neutrality, it was argued that in an era where limited broadband competition and growing convergence would leave providers with economic incentives to favour their own (or affiliated content) over competing services or offerings[20], content neutrality in the provision of network services was an absolutely essential principle that should be firmly established under Canadian law backed by regulatory oversight and significant penalties for compliance failures.

In a response to the call for greater regulatory framework, the 2006 Telecommunications Policy Review Panel[21] Report called for a new legislative provision protecting net neutrality standards – or an "open access provision." The Panel's recommendations included the following:

> *"The Telecommunications Act should be amended to confirm the right of Canadian consumers to access publicly available Internet applications and content of their choice by means of all public telecommunications networks providing access to the Internet. This amendment should*
>
> *(a) authorize the CRTC to administer and enforce these consumer access rights,*

[19] The study is available online: "First Results from Vuze Network Monitoring Tool" (18 April 2008), online: TorrentFreak <http://torrentfreak.com/images/vuze-plug-in-results.pdf >. See also "Cogeco ranks poorly in internet interference report", *CBC* (22 April 2008) online: CBC <http://www.cbc.ca/>. Note that some researchers have called into question the methodology of the study and the relevance of reset data [see Iljitsch van Beijnum, "Vuze says some ISPs abuse TCP resets; data not that clearcut", *Ars Technica* (23 April 2008) online: Ars Technica <http://arstechnica.com/>].

[20] Bell announced in 2009 its plans to focus on its Bell TV Online service that provided online access to movies and television shows for its subscribers [Christine Persaud, "Bell Silently Closes Online Video Store", *Market News* (6 September 2009) online: Market News <http://www.marketnews.ca/>]. The announcement raised the concerns associated with Bell's throttling practices at the time, since subscribers would obtain unfettered access to the Bell-backed TVOnline offering but throttled access to competing content made available over the Internet via BitTorrent.

[21] The Telecommunications Policy Review Panel was established on April 11, 2005. Gerri Sinclair, Hank Intven and André Tremblay were appointed by Industry Canada to conduct a review of the country's telecommunications policy and regulatory framework. The Panel was also asked to make recommendations towards an internationally competitive telecommunications industry in Canada. While the recommendations of the Panel were generally market-oriented, the Report did identify a series of important consumer-focused concerns including network neutrality, ubiquitous broadband access, privacy, spam, and consumer protection.

> *(b) take into account any reasonable technical constraints and efficiency considerations related to providing such access, and*
>
> *(c) be subject to legal constraints on such access, such as those established in criminal, copyright and broadcasting laws."*[22]

The Panel disagreed with companies such as Telus, which had argued that there was no need for legislation to address net neutrality. The Panel concluded that "open access is of such overriding importance that its protection justifies giving the regulator the power to review cases involving blocking access to applications and content and significant, deliberate degradation of service."[23]

The Report also contained two other related recommendations, namely the retention of privacy within the *Telecommunications Act* (including the view that the Privacy Commissioner of Canada and the CRTC should have complementary roles on privacy)[24] and the call for a new national broadband strategy that would target universal broadband access in Canada by 2010.[25]

Until 2006, the CRTC seemed reluctant to tackle the net neutrality issue. In fact, the Commission was rapidly moving in the opposite direction by actively deregulating the telecommunication industry.[26] This left considerable confusion as to the state of law in Canada was when it came to violations of net neutrality, such as the Telus blockage. One particularly troubling aspect of this ambiguity was that there were no requirements for ISPs to disclose any packet preferencing or traffic shaping activities.

In 2006, the Canadian Broadcasting Corporation, Canada's public broadcaster, made a submission to the CRTC on the state of consumer entertainment. The submission raised the network neutrality concerns, though it did not use that specific term. According to CBC:

> *"The business case analysis for Internet video is complicated by the fact that suppliers of broadband connections may also have incentives to control the bandwidth available for Internet video. Canadian cable companies engage in "bandwidth shaping" which allocates different levels of transmission capacity to different services according to the operational preferences of the cable company. This type of bandwidth shaping can*

---

[22] Telecommunications Policy Review Panel, *Final Report* 2006, (Ottawa: Industry Canada, 2006) 6-18.
[23] *Ibid*.
[24] *Ibid* at 6-13.
[25] See *Ibid* at 7-17. According to documents obtained under the *Access to Information Act*, in the Spring of 2006, Industry Canada quietly conducted an informal consultation on stakeholder responses to the Report that confirmed industry support for a complete implementation of Report's recommendations. In a memorandum to the Industry Minister, officials noted that the "department solicited stakeholders' views on their top five and bottom five recommendations" and concluded that "most firms only oppose recommendations if they are implemented separately, and believe the Panel's report should be implemented as a package." [Michael Geist, "Videotron Rekindles Fear of a Two-Tier Internet" (6 November 2006), online: Michael Geist's Blog <http://www.michaelgeist.ca/>].
[26] See, e.g., "Review panel takes step in right direction", *National Post* (23 March 2006) online: National Post <http://www.nationalpost.com/>.

> *ensure efficient use of transmission capacity. It can also ensure that Internet video by third parties does not become a threat to the business of the cable company, whether it be the delivery of traditional television programming to cable subscribers, VOD or the distribution of cable company-owned Internet video services. In light of this complex mix of issues, it remains unclear whether Internet video will become a primary means of distributing video content on a commercial basis."*[27]

This statement effectively corresponded to network neutrality, indicating that Canada's national public broadcaster was opposed to a "wait and see" regulatory approach. Meanwhile, larger ISPs campaigned against net neutrality legislation. Bell Canada, for instance, maintained that net neutrality "should be determined by market forces, not regulation."[28]

Other civil society groups and experts also voiced their support for net neutrality regulation. For example, the Alternative Telecommunications Policy Forum drafted a guideline stating that "network operators shall not discriminate against content, applications, or services on broadband Internet services based on their source or ownership."[29] Yet, the public generally remained somewhat apathetic towards the issue, with the net neutrality debate crowded by "telecom lobbies."[30]

While opponents of network neutrality legislation argued that a competitive marketplace would remove the need for government intervention, the reality is that the market for broadband services in Canada is at best an oligopoly. Most Canadians have limited choice, with consumers in urban areas choosing between indistinguishable cable and telephone Internet packages, while Canadians in rural communities are often left with no broadband options at all. Moreover, Canadian consumers who do have access to broadband networks invariably face steady price increases and service limitations.

Meanwhile, the federal government seemed to be sympathetic to the market-oriented arguments by the ISPs, although publicly maintaining that it was monitoring the issue. Based on a number of government documents[31] obtained under the *Access to Information Act*, as of early 2007, the government was clearly aware of major telecom companies' intent on becoming gatekeepers for content with the prospect of levying additional content-based fees:

---

[27] See "CBC Reporting on Today's Entertainment Trends", *Slyck News* (9 September 2006) online: Slyck News <http://www.slyck.com/>.
[28] See "Battle over 'net neutrality' arrives in Canada", *CBC* (2 November 2006) online: CBC <http://www.cbc.ca/>.
[29] Andrew Clement et al, *Connecting Canadians: Investigations in Community Informatics* (Edmonton: AU Press, 2012) at 460.
[30] See Bryan Zandberg, "Canada Sleeps Through War to 'Save the Internet'", *The Tyee* (17 January 2007) online: The Tyee <http://thetyee.ca/>.
[31] See "Does the Minister intend to allow telecommunications companies to determine the content that its customers can and cannot access by imposing special rates, undermining net neutrality?" Question Period Card in Telecommunications Policy Branch, *Network Neutrality – Questions and Answers*, (Ottawa: Industry Canada, 2006).

> *"Canadian telecommunications companies, like Bell and TELUS, are increasingly determined to play a greater role in how Internet content is delivered. As the carriers of the content, they believe should be gatekeepers of the content, with the freedom to impose fees for their role."*

Yet, these documents also indicated that the Canadian government was inclined to accept the ISPs' position on the issue:

> *"Many commentators note that the net neutrality debate is both broader and more complex than it is typically framed by advocates and opponents. First, the Internet has never been truly neutral or equitable with respect to data transmission. Throughout its evolution, new applications and users' growing requirements have necessitated changes to many aspects of Internet design and operation, including the introduction of non-neutral operating procedures, such as preferential content arrangements, filtering and blocking to control network abuse, as well as 'traffic shaping' in order to ensure an acceptable service level for all subscribers, despite the bandwidth-demanding activities of some users."*[32]

In other words, by formulating "traffic shaping" in terms of "contractual arrangements" between private parties or in terms of "technical measures" to ensure a viable industry, the government had chosen a hands-off approach to network neutrality. The policy was to allow "market forces to continue to shape the evolution of the Internet infrastructure, investment and innovation to the greatest extent feasible." The discussion of net neutrality legislation, therefore, was a "premature" one according to the government.[33]

Surprisingly, Canada seemed to be an active player on net neutrality policy on the international front, however. In 2006-2007, the OECD was working on a report titled "Internet Traffic Prioritisation."[34] Having been an active participant at the OECD, Canadian officials were most likely engaged in the drafting process. The OECD report acknowledged the concerns associated with anti-competitive conduct, the prospect of hindering access to information, and the privacy implications of monitoring the content by ISPs. Moreover, it noted that robust competition can help mitigate these concerns, though Canada was not cited as a country with the competition to counterbalance anti-competitive incentives.[35]

---

[32] On February 19, 2007, then Industry Minister, Maxime Bernier, gave similar statements in his presentation before the Standing Committee on Industry, Science, and Technology. See House of Commons, Standing Committee on Industry, Science and Technology, *Evidence*, No 045 (19 February 2007) at 1625.
[33] The government seemed to justify its position by polls showing support for "telecommunication reform." [*House of Commons Debates*, 39th Parl, 1st Sess, No141 (7 February 2007) at 1455].
[34] OECD, "Working Party on Telecommunication and Information Services Policies – Internet Traffic Prioritisation: An Overview (DSTI/ICCP/TISP(2006)4/FINAL)" (6 April 2007), online: OECD <http://www.oecd.org/internet/ieconomy/38405781.pdf>.
[35] *Ibid* at 28-29.

A logical place to start with net neutrality seemed to be more transparent disclosure rules. For instance, experts such as Wu recommended disclosure of limits on bandwidth usage and any other important limitations placed on service features.[36] The disclosure was, however, only one step towards more comprehensive regulation. In March 2007, the Standing Committee on Industry, Science, and Technology tabled a very short (one paragraph) report on telecom deregulation. The Committee:

> *"recommends that the Minister of Industry withdraw the order varying Telecom Decision CRTC 2006-15 and table in Parliament a comprehensive package of policy, statutory and regulatory reforms to modernize the telecommunications services industry*."[37]

This was the Committee's opposition to the Minister's selective implementation of the 2006 Telecommunication Review Panel Report and a call for a comprehensive regulation. Determined to deregulate the telecommunication industry, the Conservative government remained "defiant."[38] It must be noted that many supporters of net neutrality in Canada did support the idea of deregulation. However, they took issue with the way the minister was pursuing the modernization of the telecommunications sector within Canada and the harms it might cause to consumers and to fair competition within VoIP, IPTV and other emerging application industries.

Meanwhile, various supporters of net neutrality made submissions to CRTC prior to its 2007 Diversity of Voices proceeding.[39] Corus, which is one of Canada's most successful media and entertainment companies, submitted that "Canadian creators and producers need to ensure that they can continue to have access to the networked bit stream on the basis of equitable rules." The company also recommended the creation of an Industry Task Force on net neutrality. The Canadian Media Guild also offered a strong endorsement of net neutrality in its submission to CRTC. The CMG urged the CRTC to "guarantee 'net neutrality' by establishing a rule prohibiting Internet service providers from controlling clients' access to websites for commercial

[36] Tim Wu, "Wireless Net Neutrality: Cellular *Carterfone* and Consumer Choice in Mobile Broadband", *New America Foundation* (15 February 2007), online: New America Foundation <http://newamerica.net/>.
[37] House of Commons, Standing Committee on Industry, Science and Technology, *Sixth Report: Deregulation of telecommunications* (March 2007).
[38] See "Tories overrule CRTC, further deregulate phone market", *Canada.com* (4 April 2007) online: Canada.com <http://o.canada.com/>. See also the Green Party of Canada's press release denouncing the Minister of Industry's accelerated deregulation of telecommunication industry despite recommendations of CRTC and the Parliamentary Committee ["Green Party alarmed by recklessness of Bernier's rush to deregulation", *Green Party* (5 April 2007) online: Green Party of Canada <http://www.greenparty.ca/>].
[39] See CRTC, *Broadcasting Public Notice CRTC 2008-4: Diversity of voices*, (Ottawa: CRTC, 2008), online: CRTC <http://www.crtc.gc.ca/>.

gain."[40] National Union of Public and General Employees, one of Canada's largest trade unions, also called on the government to take action ensure network neutrality.[41]

A Cabinet shuffle in August 2007 (including the replacements of Minister of Canadian Heritage and Minister of Industry) renewed the calls for a shift from parochial focus on telecommunication deregulation towards a more comprehensive plan to enhance Canada's digital economy competitiveness.[42] Meanwhile, Canadian public opinion seemed to shift toward support for net neutrality principles. A 2007 poll by *Leger Marketing* found that Canadians were generally unaware of net neutrality issues, yet strongly supported that ISPs "should be required to treat all content, sites and platforms equally." Two-thirds of Canadians also disagreed with the proposal that ISPs "should be allowed to impose additional fees for access to specific content on the web." The same poll showed that 76% of Canadians believed the federal government "should pass a law to confirm the right of Internet consumers to access publicly available Internet applications and content of their choice."[43] Indeed, the survey's results pointed again to the lack of transparency within the Canadian marketplace as most consumers could hardly be faulted for being unaware of net neutrality issue since ISPs did not disclose their traffic shaping practices. The strong support for the principles behind net neutrality, however, was a clear indication for the need for legislative action. In early 2008, the National Union of Public and General Employees renewed its call for net neutrality and urged the government to hold open, public consultations on the issue.[44]

On the political front, the Green Party of Canada adopted net neutrality as a part of its 2007 platform. The Vision Green document stated that

> *"The Green Party of Canada is committed to the original design principle of the internet - network neutrality: the idea that a maximally useful public information network treats all content, sites, and platforms equally, thus allowing the network to carry every form of information and support every kind of application. Green Party MPs will pass legislation granting the Internet in Canada the status of Common Carrier - prohibiting Internet*

[40] See Michael Geist, "Corus Calls For Net Neutrality Task Force" (20 July 2007), online: Michael Geist's Blog <http://www.michaelgeist.ca/>; and Mark Goldberg, "Net neutrality and the new media proceeding" (7 August 2007) online: Personal Website <http://www.mhgoldberg.com/>.
[41] See "NUPGE seeks action on Internet access and net neutrality", *National Union* (3 August 2007) online: National Union of Public and General Employees <http://nupge.ca/>.
[42] See, e.g., Michael Geist, "A blueprint for reforming the digital economy", *The Toronto Star* (20 August 2007) online: The Toronto Star < http://www.thestar.com/>.
[43] See the results of the survey in "Canadians rebuff restrictions on their Internet access", *CNW Group* (1 October 2007) online: CNW Group <http://www.newswire.ca>.
[44] See "Consultations and legislation needed to protect net neutrality", *National Union* (20 February 2008); and "NUPGE asks CRTC to investigate Internet 'traffic shaping'", *National Union* (28 March 2008) online: National Union of Public and General Employees <http://nupge.ca/>.

> *Service Providers from discriminating due to content while freeing them from liability for content transmitted through their systems."*[45]

In February 2008, the Standing Committee on Canadian Heritage released its report on the CBC and public broadcasting, in which several pages were dedicated to net neutrality. The Committee noted that:

> *"Network non-neutrality could have significant consequences for CBC/Radio-Canada since it is not in a position to respond to market changes through convergence on a sufficiently large scale…If the Internet evolves into a multi-tiered network, where content providers pay for different levels of service, the possible degradation of its content and services, or the requirement to pay additional fees for their online delivery, would put the Corporation at a significant competitive disadvantage and undermine its ability to meet its mandated goals."*[46]

In light of those concerns, the majority of the Committee[47] agreed that "non-discriminatory access by Canadians to CBC/Radio-Canada online content and services is necessary to the fulfillment of the role of our national public broadcaster in the digital age." It therefore recommended that the CRTC address the net neutrality issue as part of its New Media Project initiative.

In the following months, the NDP called on government to follow the recommendations of the 2006 Telecommunications Policy Review Panel, and to introduce net neutrality legislation.[48] In April 2008, the National Union of Public and General Employees (NUPGE) also asked then Liberal Opposition Leader, Stéphane Dion, to support its "campaign for government action" to protect the neutrality of the Internet in Canada.[49] In May 2008, and in response to a rally in support of net neutrality on Parliament Hill, NDP MP Charlie Angus announced that he planned to introduce a Private Member's bill addressing the net neutrality issue.[50] The bill, which was introduced the following day, sought to add transparency, neutral network management, and open devices to the Canadian telecom law framework:

---

[45] See Green Party of Canada, *Vision Green* (15 October 2007) at 154, online: Green Party of Canada <http://www.greenparty.ca/sites/greenparty.ca/files/VisionGreenOct15.pdf >.
[46] House of Commons, Standing Committee on Canadian Heritage, *CBC/Radio-Canada: Defining Distinctiveness in the Changing Media Landscape*, ch 2 (February 2008).
[47] Note that the Conservatives on the Committee issued a minority opinion dissenting from this aspect of the report on the grounds that it addressed the CRTC, not the CBC.
[48] "NDP calls for net neutrality", *CBC* (21 April 2008) online: CBC <http://www.cbc.ca/>.
[49] See "NUPGE asks federal Liberals to join net neutrality campaign", *National Union* (28 April 2008) online: National Union of Public and General Employees <http://nupge.ca/>.. In a reported response, a Liberal MP stated that government's deregulator approach did not "afford proper recognition to the rights of Canadian internet users". [Michael Geist, "Liberal Response to Net Neutrality" (8 May 2008), online: Michael Geist's Blog <http://www.michaelgeist.ca/>].
[50] See "Internet protesters to descend on Ottawa", *CBC* (26 May 2008) online: CBC <http://www.cbc.ca/>; and "NDP to introduce 'net neutrality' private member's bill", *CBC* (27 May 2008) online: *Ibid*.

> *"Network operators shall not engage in network management practices that favour, degrade or prioritize any content, application or service transmitted over a broadband network based on their source, ownership or destination."*[51]

The bill included several notable exceptions to this general principle, including action to provide computer security, prioritize emergency communications, offer differentiated pricing or bit caps, enable anti-spam filters, handle breaches in terms of service, and prevent violations of the law. The bill also focused on open devices and greater transparency. It provided that "network operators shall not prevent or obstruct a user from attaching any device to their network, provided the device does not physically damage the network or unreasonably degrade the use of the network by other subscribers."[52] Further, it required that "network operators shall provide and make available to each user information about the user's access to the Internet, including the speed, nature, and limitations of the user's broadband service at any given time."[53] As the 2008 federal election approached, various civil society and non-profit organizations such as Canadian Library Association and SaveourNet.ca joined a broad coalition calling for net neutrality to be considered as an election issue.[54]

The regulatory breakthrough in Canada occurred in 2008 when the Canadian Association of Internet Providers (CAIP) filed a Part VII application with the CRTC asking it to direct Bell Canada to cease and desist from throttling its wholesale Internet service.[55] The application provided some additional insights into Bell's activities, namely that its throttling practices had reduced speeds by as much as 90 percent. CAIP argued that the throttling was rendering it impossible for the independent ISPs to manage their networks and forcing them to pay for bandwidth they could not use. CAIP also raised privacy concerns with the throttling practices, maintaining that Bell had acted "unlawfully and contrary to the prohibition on carrier interference with the content of messages carried over its telecommunications network contrary to s. 36 of the [Telecommunication] Act and contrary to the Canadian telecommunications policy

---

[51] Bill C-552, *An Act to amend the Telecommunications Act (Internet Neutrality)*, 2nd Sess, 39th Parl, 2008, cl 36.1(1).
[52] *Ibid* cl 36.1(3).
[53] *Ibid* cl 36.1(4). In June 2008, Liberal MP David McGuinty introduced *the Telecommunications Clarity and Fairness Act* as a Private Member's Bill. The Bill would require the CRTC to study issues such as how to stop providers from locking devices, how to provide more accurate information on network speeds, and how to implement greater transparency of network management practices on mobile and broadband networks. It also called on the CRTC to issue a net neutrality report on "network management practices that favour, degrade or prioritize any packet transmitted over a broadband network based on source, ownership, or destination." [see Bill C-555, *An Act to provide clarity and fairness in the provision of telecommunication services in Canada*, 2nd Sess, 39th Parl, 2008].
[54] See, for instance, Canadian Liberty Association, "2008 Election Campaign Kit" at 7, online: CLA <http://www.cla.ca/news/CLA%20Election%20Kit%202008.pdf>. For a brief overview of the digital policies of various political parties in the 2008 election, see Michael Geist, "Which party is ahead on the digital scoreboard?", *The Toronto Star* (14 October 2008) online: The Toronto Star <http://www.thestar.com/>.
[55] See above for more details of *Bell*'s throttling practices.

objectives set out in paragraphs 7(a) and (i) which, inter alia, seek to protect the privacy of persons."[56]

The privacy argument focused on Bell's DPI system:

> *"In order to throttle the Internet traffic originating from/or destined for end-user customers of independent ISPs, Bell is using measures to first, open each data packet, examine the packet data and header information, and then apply certain rules to the content in question. This aspect of Bell's wholesale throttling activities give rise to concerns that Bell's actions violate the privacy of the communications of its wholesale customers (as well as that of their own end-user customers)."*[57]

Finally, CAIP also brought the broader net neutrality issue into the picture in clear and strong words:

> *"The throttling or choking of wholesale ADSL access services that has been engaged in by Bell involves the running of complex algorithms on the GAS and HSA traffic of independent ISPs. In so doing, Bell is reducing the throughput available to the end-user customers of these ISPs by as much as 90 per cent. At such speeds, mainstream content available on the Internet, such as audio or video content (e.g., the CBC's 'Next Great Prime Minister' program), would be slowed beyond recognition or meaning. In fact, Bell degrades the service to the point of, in some cases, rendering the content inaccessible or at least, highly undesirable. Bell is, therefore, clearly interfering with and, indeed, exercising control over this content by isolating it from other content, classifying it as low priority vis à vis other types of content and quarantining the content until Bell decides that it can be released to the end-user recipient in a manner determined wholly by Bell.*
>
> *Similarly, Bell is influencing the "meaning" and the intended "purpose" of this content by preventing it from being delivered in the manner and within the time frames intended by the content sender and the content recipient."*[58]

---

[56] Canadian Association of Internet Providers, "Re: Part VII Application by the Canadian Association of Internet Providers Requesting Certain Orders Directing Bell Canada to Cease and Desist from "Throttling" its Wholesale ADSL Access Services" (3 April 2008) at para 116, online: Canadian Advanced Technology Alliance <http://www.cata.ca/files/PDF/caip/CAIP-PartVII__Traffic-Shaping_Final_v2.pdf>.

[57] *Ibid* at paras 78-79;84.

[58] *Ibid* at paras 92-94. See also See Tom Barrett, "'Throttling' Net Traffic", *The Tyee* (9 April 2008) online: The Tyee <http://thetyee.ca/>. Later on, *Primus Communications* and *Wireless Nomad* filed a submission with the CRTC in support of *CAIP* in the *Bell* throttling issue. [see Primus Telecommunications Inc., "Re: Application requesting certain orders directing Bell Canada to cease and desist from "throttling" its wholesale ADSL Access Services" (15 April 2008), online: CRTC < http://www.crtc.gc.ca/public/partvii/2008/8622/c51_200805153/891007.pdf>] It is noteworthy that, in the context of imposing levies on ISP services, ISPs did resort to their role as "passive" transmitters of data in order to argue for their exemption from the *Broadcasting Act*. See Michael Geist, "Canadian ISP Alliance Forms For New Media Fight" (15 July 2008), online: Michael Geist's Blog

The CAIP filing was supported by another submission from Vaxination Informatique, which asked the CRTC to take action in response to Bell's DPI practices.[59]

Bell's response to the CAIP submission maintained that its actions were justified and that there was no need to deal with the issue on an emergency basis.[60] The response was generally silent regarding the privacy concerns with deep-packet inspection – except for stating that Bell did not retain or use the data. Moreover, Bell disclosed some data on its network usage that seemed to undermine its claim that peer-to-peer usage was causing havoc with its network. Bell claimed that the "problem" lay with 5 percent of its users that were heavy peer-to-peer users using 33 percent of available bandwidth during peak periods. Although disproportionate, this number seemed lower compared to other countries where more than half of the available bandwidth had been used by comparable percentage of heavy users.[61] In fact, in its filed response to the Bell throttling submission, CAIP maintained that:

> *"There is also uncontradicted evidence…that strongly suggests that the reasons behind Bell's decision to throttle its competitors' GAS traffic have little to do with Bell's unsubstantiated claims of "network congestion" and more to do with a desire to lessen competition in retail telecommunications markets. There are far too many "coincidences" between the timing of the initiation of Bell's throttling practices and the timing of a number of other events in order to conclude otherwise."*[62]

This new submission also included new allegations on the impact of DPI technologies and throttling on VPNs and VOIP services (in addition to peer-to-peer networks). The submission

---

<http://www.michaelgeist.ca/>. Another example of this double standard may be found in *Rogers*'s claim of being a "dumb pipe" and hence not responsible for the downloaded content while the same company had acknowledged "traffic management" based on content before [Mark Evans, "Rogers: It's Bandwidth Management; Not Throttling" (13 April 2007), online: Mark Evans Tech < http://www.markevanstech.com>; and Joanne Chianello, "Canadian content available online may be regulated", *Ottawa Citizen* (16 February 2009) online: Ottawa Citizen <http://www.ottawacitizen.com >].

[59] Vaxination Infomatique's submission is available online: CRTC <http://www.crtc.gc.ca/public/partvii/2008/8622/c51_200805153/886374.PDF>. For an example of *Bell*'s public response to these claims, see "Internet throttling defended", *Canada.com* (11 April 2008) online: Canada.com <http://o.canada.com/>. Around the same time, *L'Union des Consommateurs* and a Quebec consumer launched a class action lawsuit against *Bell Canada* over its throttling practices. The suit, which was seeking certification on behalf of all provincial subscribers, argued that the practices deliberately slowed consumer services and raised privacy issues ["Demande de recours collectif contre Bell", *CNW Group* (29 May 2008) online: CNW Group <http://www.newswire.ca>].

[60] Bell Canada's April 2008 submissions are available online: CRTC <http://www.crtc.gc.ca/public/partvii/2008/8622/c51_200805153/890988.zip>.

[61] See Michael Geist, "Does Bell Really Have a P2P Bandwidth Problem?" (17 April 2008), online: Michael Geist's Blog <http://www.michaelgeist.ca/>.

[62] See Canadian Association of Internet Providers, "Re: Part VII Application by the Canadian Association of Internet Providers Requesting Certain Orders Directing Bell Canada to Cease and Desist from "Throttling" its Wholesale ADSL Access Services" (24 April 2008) at para 9, online: CRTC <http://www.crtc.gc.ca/public/partvii/2008/8622/c51_200805153/895702.pdf>.

also included a statement from SaskTel, the leading telecom company in Saskatchewan, in which it confirmed that, unlike Bell, it did not employ "any form of traffic shaping, rate limiting, or usage caps on a per user or per application…".[63]

CAIP reiterated why throttling violated the common carrier provisions found in s. 36 of the *Telecommunications Act*:

> *" Section 36 of the Act states very clearly that a carrier "shall not control the content or influence the meaning or purpose of telecommunications carried by it for the public." Bell's traffic shaping measures clearly influence the meaning and purpose of the telecommunications that it carries for the public. Indeed, as noted by CAIP in its Application, Bell is reducing the throughput or data transfer speeds available to the end-user customers of competitors by as much as 90 per cent. At speeds such as this, mainstream content available on the Internet, such as audio or video content (e.g., the CBC's "Next Great Prime Minister" program), would be slowed beyond recognition or meaning.*
>
> *These drastically reduced speeds also make it clear that Bell is exercising control over this content by isolating the data packets that make up this content, classifying those packets as low priority vis à vis other types of content and quarantining the packets until Bell decides that they can be released to end-user recipients at a time and in a manner determined wholly by Bell.*
>
> *In a similar fashion, Bell is influencing the "meaning" and the intended "purpose" of this content by preventing it from being delivered in the manner and within the time frames intended by the content sender and the content recipient."*[64]

The privacy concerns associated with DPI were raised directly with the Privacy Commissioner of Canada in May 2008 when the Canadian Internet Policy and Public Interest Clinic (CIPPIC) filed a privacy complaint under PIPEDA over Bell's DPI practices.[65] CIPPIC identified several privacy concerns including failure to obtain consent for the collection of personal information through DPI. CIPPIC also argued that Bell violated the privacy principle of limiting collection, since the evidence indicated that Bell could "manage its network adequately without inspecting the content of user communications."[66] The complaint also referred to Bell's violation of the

[63] See *Ibid* at para 62.
[64] See *Ibid* at paras 74-79.
[65] Canadian Internet Policy and Public Interest Clinic, "Re: Bell Canada/Bell Sympatico Use of Deep Packet Inspection: PIPEDA Complaint" (9 May 2008), online: CIPPIC < https://www.cippic.ca/sites/default/files/Bell-DPI-PIPEDAcomplaint_09May08.pdf>.
[66] See *Ibid* at para 38.

openness principle, given its failure to disclose "in a clear and conspicuous manner to the public its use of DPI for traffic management purposes."[67]

After some delays[68], CRTC ruled in *CAIP-Bell* case in November 2008. The Commission denied CAIP's application, ruling that Bell treated all of its customers (retail and wholesale) in the same throttled manner. This ruling pointed to the challenge at the heart of this case – that it was not about discriminatory network practices per se, but rather about wholesale shaping in a specific context. The Commission sided with Bell on most key issues. It agreed that there was network congestion due to peer-to-peer usage and that Bell was therefore acting reasonably by implementing some network management techniques to address the congestion concerns. Moreover, it rejected fears that Bell's actions were motivated by a desire to undermine competition and it concluded that the mere act of reducing Internet speeds did not rise to the level of controlling content – and hence a violation of the *Telecommunications Act*.[69]

The decision was not a total loss for net neutrality supporters, however, as the Commission made a clear commitment to addressing the issue of net neutrality and network management in a formal proceeding in July 2009.[70] The Commission noted that part of that hearing would seek to establish the criteria for authorizing specific traffic management measures.[71] By that time, there seemed to be an emerging consensus on the easy issues such as no content blocking and better transparency[72] of network management practices. In fact, in the aftermath of the decision, and in response to Bell's claim[73] that the CRTC had "confirmed" Bell's position on the issue of throttling, the Vice-Chairman of the CRTC clarified that the *CAIP-Bell* decision was not an "endorsement" of Internet throttling.[74]

---

[67] See *Ibid* at para 45.
[68] See "CRTC delays ruling on Bell's throttling", *CBC* (17 October 2008) online: CBC <http://www.cbc.ca/>.
[69] See CRTC, *Telecom Decision CRTC 2008-108: The Canadian Association of Internet Providers' application regarding Bell Canada's traffic shaping of its wholesale Gateway Access Service*, (Ottawa: CRTC, 2008), online: CRTC <http://www.crtc.gc.ca/>. For sample media coverage of the CRTC decision, see "CRTC allows Bell to continue internet throttling", *CBC* (20 November 2008) online: CBC <http://www.cbc.ca/>; Chris Sorensen, "Bell can squeeze downloads, CRTC rules", *The Toronto Star* (20 November 2008) online: The Toronto Star <http://www.thestar.com/>; and Nate Anderson, "Canadian regulators allow P2P throttling", *Ars Technica* (20 November 2008) online: Ars Technica <http://arstechnica.com/>.
[70] See CRTC, *Telecom Public Notice CRTC 2008-19 – Notice of consultation and hearing: Review of the Internet traffic management practices of Internet service providers*, (Ottawa: CRTC, 2008), online: CRTC <http://www.crtc.gc.ca/ >. The CRTC also launched an online consultation on net neutrality in March 2009. Topics included the impact on user experience, innovation, the role of the CRTC, network management, and ISP transparency.
[71] See *Ibid* at para 9(5).
[72] The CRTC required Bell to provide its wholesale customers with advanced notice of its traffic management plans. See CRTC, *Telecom Decision CRTC 2008-108*, (Ottawa: CRTC, 2008) at para 74, online: CRTC < http://www.crtc.gc.ca/ >.
[73] See "Bell welcomes CRTC decision allowing wholesale Internet network management", *Bell Canada* (20 November 2008) online: Bell Canada <http://www.bce.ca/>.
[74] See Peter Nowak, "We're not endorsing internet throttling: CRTC", *CBC* (20 November 2008) online: CBC <http://www.cbc.ca/>.

The decision to hold a hearing devoted to Internet traffic management practices sparked a flurry of submissions and commentary. The Privacy Commissioner of Canada took note of the CRTC decision, stating "the time has come for net neutrality, both as an economic and a social policy issue, to be examined by the Canadian government…we look forward to being a part of that discussion."[75] The Privacy Commissioner would subsequently become part of discussion by filing a submission to the CRTC network management hearing on the privacy implications of network management that uses DPI technologies.[76] The submission noted concerns with several uses of DPI, including scanning Internet traffic for certain content such as spam, copyright infringing materials, and hate content as well as for monitoring traffic loads to measure network performance. The Commissioner expressed the need to factor privacy into the network management analyis, stating that:

> *"We respectfully submit that in order to advance the privacy objectives contained in the Act, telecommunications policy, decisions and regulation with respect to Internet traffic management practices in general, and DPI specifically, should consider the potentially invasive nature of DPI technology, and the manner in which it has been implemented by ISPs."*[77]

> *"There is concern that the implementation of DPI for Internet traffic management has been done in a manner that is less than transparent and potentially inconsistent with an individual's/consumer's expectations. There has been some evidence in a number of jurisdictions suggesting that such technology has been used for 'unreasonable network management practices.'"*[78]

A number of important submissions were made to CRTC in response to its *Notice of Consultation and Hearing* on net neutrality.[79] The Canadian Association of the Deaf emphasized that "[a] disability lens needs to be applied to any and all traffic management proposals to make sure unintended consequences on Deaf or other people with disabilities do not impact the communities negatively."[80]

Pelmorex Media, the owner the Weather Network, strongly supported net neutrality in its submission. More particularly, however, it emphasized *wireless* net neutrality:

> *"It is Pelmorex's submission that the Commission should adopt a more expansive definition of net neutrality and traffic management that would encompass the commercial*

[75] See Daphne Guerrero, "CRTC begins dialogue on traffic shaping" (21 November 2008), online: Office of the Privacy Commissioner of Canada <http://blog.priv.gc.ca/>.
[76] Privacy Commissioner of Canada, "Re: Telecom Public Notice CRTC 2008-19" (18 February 2009), online: CRTC <http://www.crtc.gc.ca/public/partvii/2008/8646/c12_200815400/1027577.PDF>.
[77] See *Ibid* at para 21.
[78] See *Ibid* at para 31.
[79] *Supra* note 78.
[80] Canadian Association of the Deaf, "Re: Public Notice 2008-19" (16 January 2009) at para 8, online: CRTC <http://www.crtc.gc.ca/public/partvii/2008/8646/c12_200815400/1008694.DOC>.

> *practices of both wire-line and wireless network operators. In our view, the Commission needs to take steps to ensure that, with respect to both wire-line and wireless network operators, traffic management practices are applied equitably and treat like-traffic in the same or comparable manner. Any management practices that treat certain types of content, particularly content produced or provided by the ISP or network operator, in a preferential or advantageous manner should not be permitted.*"[81]

Pelmorex was not alone in focusing on wireless issues[82], but its submission was noteworthy for including a list of alleged wireless net neutrality violations by Canadian carriers. While the carriers were not named, the allegations included: blocking ads from a mobile site; stripping out tracking codes embedded in web pages (thereby limiting ability to deliver ads); establishing "walled gardens" that provided preferential access; forcing users through the carrier's homepage when accessing the Internet on feature phones; requiring prior approval of applications for use on smart phones; charging extra fees for text messages that included ads; and limiting to whom ads in text messages might be sold.[83]

The Canadian Film and Television Production Association (CFTPA) cited the growing use of peer-to-peer applications as a legitimate business model and the potential threat to such models from traffic throttling practices:

> *"while P2P applications are undeniably used for the distribution of unauthorized content (as are email, newsgroups and the web), they also are increasingly serving as the foundation for new business models that will enable independent producers to make full use of broadband as a delivery vehicle for Canadian audio-visual programming. Consequently, the CFTPA is concerned that discriminatory traffic throttling may inhibit the development of new applications that would facilitate the ability of independent producers and other content providers to better monetize their content – whether self-distributed, distributed by authorized third parties, or even "pirated" content that finds its way onto the Internet."*[84]

[81] See Pelmorex Media Inc., "Re: Telecom Public Notice CRTC 2008-19," (23 February 2009) at para 36, online: CRTC <http://www.crtc.gc.ca/public/partvii/2008/8646/c12_200815400/1029399.pdf>.
[82] *Score Media* also noted that its mobile site traffic nearly equaled its fixed Internet site [Score Media Inc., "Re: Telecom Public Notice CRTC 2008-19," (23 February 2009) at para 3, online: CRTC <http://www.crtc.gc.ca/public/partvii/2008/8646/c12_200815400/1029790.pdf>].
[83] *Supra* note 89 Appendix.
[84] See Canadian Film and Television Production Association, "Re: Telecom Public Notice CRTC 2008-19" (23 February 2009) at para 58, online: CRTC <http://www.crtc.gc.ca/public/partvii/2008/8646/c12_200815400/1030120.PDF>.

The CFTPA, therefore submitted that the CRTC should require "as a condition of service that ISPs refrain from employing any traffic management practice that discriminates on the basis of application or protocol."[85] Meanwhile, the Documentary Organization of Canada (DOC) argued:

> *"The ISP practice of throttling to manage Internet traffic is a particular concern to the Canadian documentary filmmaking community. DOC supports the notion of Net Neutrality. By employing traffic shaping techniques that target P2P applications, ISPs are effectively taking on the role of gatekeepers."*[86]

The CBC also made a submission in support of net neutrality:

> *"In CBC/Radio-Canada's view, an Internet traffic management practice would contravene section 36 of the Act if it involved either blocking access to a website or altering a communication over the Internet so as to significantly distort the content of the communication or frustrate timely access to the content."*[87]

And according to the Canadian Conference of the Arts (CCA):

> *"One cannot argue simultaneously that Canadians' access to content is now unlimited, if the companies from which Canadians obtain access to that content, decide to and actually impose their own limits on users' access to, that content, for reasons that involve profit, as much as or even more than they involve 'pure' traffic management to manage traffic congestion."*[88]

The Alliance of Canadian Cinema, Television and Radio Artists (ACTRA)[89] and the Canadian Media Guild adopted similar positions.[90] These submissions indicated that the upcoming net neutrality hearings would extend beyond the business, innovation, and consumer concerns and would inevitably engage the Canadian culture connection to the issue.

---

[85] See *Ibid* at para 81 [emphasis in original]. In a later submission by the CFTPA that argued Bell's throttling practices unduly disadvantaged peer-to-peer content, peer-to-peer applications, and end-users accessing legal peer-to-peer content [available online: DSL Reports <http://www.dslreports.com/r0/download/1441998~60cdd142c47391b7bfd55f76129c2a3d/Part%20VII%20Application%20-%20CFTPA.pdf>].

[86] See Documentary Organization of Canada, "Re: Telecom Notice of Public Consultation and Hearing CRTC 2008-19" (23 February 2009) at 2, online: CRTC <http://www.crtc.gc.ca/public/partvii/2008/8646/c12_200815400/1030141.PDF >.

[87] See CBC, "Re: Review of the Internet traffic management practices of Internet service providers, Telecom Public Notice CRTC 2008-19" (23 November 2009) at para 23, online: CRTC <http://www.crtc.gc.ca/public/partvii/2008/8646/c12_200815400/1030285.PDF >.

[88] See Canadian Conference of the Arts, "Re: Review of the Internet traffic management practices of Internet service providers, Telecom Public Notices CRTC 2008-19, -19-1, -19-2" (23 February 2009) at para 8, online: CRTC <http://www.crtc.gc.ca/public/partvii/2008/8646/c12_200815400/1030237.DOC>.

[89] See Alliance of Canadian Cinema, Television and Radio Artists, "Re: Telecom Public Notice CRTC 2008-19" (23 February 2009), online: CRTC <http://www.crtc.gc.ca/public/partvii/2008/8646/c12_200815400/1031363.PDF>.

[90] See Canadian Media Guild, "RE : Telecom Public Notice CRTC 2008-19" (23 February 2009), online: CRTC <http://www.crtc.gc.ca/public/partvii/2008/8646/c12_200815400/1031064.PDF>.

Another influential submission to the CRTC's *Notice of Consultation* on net neutrality came from the Open Internet Coalition, which included companies such as Google, eBay, Amazon and PayPal. The Coalition urged the CRTC to take a "nuanced regulatory approach":

> *"…the Commission should distinguish between content and application-neutral traffic management– which may be permissible in some cases – and unlawful application-specific traffic management, which discourages investment in broadband networks, diminishes consumer choice, interferes with users' freedom of expression, and inhibits innovation."*[91]

The B.C. Government, through Network B.C., also made a submission:

> *"Net neutrality should be accepted as the bedrock upon which the Internet rests. Net neutrality also depends heavily on investment in robust and scalable network infrastructure. However, "aggressive traffic shaping" practices contributes little to network infrastructure investment and only leads to a short-term false sense of security that existing and legacy networks can be squeezed to meet future capacity requirements. Further, the use of aggressive traffic shaping practices potentially defers what should be ongoing network upgrade practices thus potentially leading to the need for massive network investments in the future."*[92]

> *"…aggressive traffic shaping as a net management practice, particularly where an ISP is reliant on a solitary Gateway Service Provider, is antithetical to the policy objectives outlines in section 7(a)(b)(g)(f) and (h) on the Telecommunications Act."*[93]

In May 2009, two months before the start of the Internet traffic management hearing, the Canadian Association of Internet Providers (CAIP) filed an application with the CRTC that called on the Commission to rescind its November 2008 Bell throttling decision.[94] The application alleged multiple errors of fact and law in the decision and pointed specifically to the CRTC's lack of a full understanding of the issues raised in the proceeding.

Moreover, CAIP highlighted a concern raised by many in the net neutrality world – that the CRTC had already decided many of the bigger issues even before the July hearings. CAIP noted:

> *"In effect, the Commission has pre-judged certain factual and legal issues raised in the PN 2008-19 proceeding, thereby narrowing the scope of the Commission's decision in*

[91] See Open Internet Coalition, "RE : Telecom Public Notice CRTC 2008-19" (23 February 2009) at paras 2-3, online: CRTC <http://www.crtc.gc.ca/public/partvii/2008/8646/c12_200815400/1029708.pdf>.
[92] See Network BC, "RE : Telecom Public Notice CRTC 2009-19" (17 February 2009) at para 4, online: CRTC <http://www.crtc.gc.ca/public/partvii/2008/8646/c12_200815400/1030213.zip>.
[93] See *Ibid* at para 44

[94] See Canadian Association of Internet Providers, "Application to Review and Vary Telecom Decision CRTC 2008-108" (21 May 2009), online: Canadian Advanced Technology Alliance <http://www.cata.ca/files/CAIP/R_V_on_Throttling_%2820May09FINAL%29-1.pdf>.

> *the PN 2008-19 proceeding even before it is made. As long as Decision 2008-108 stands, the perception that the Commission has pre-judged the outcome of PN 2008-19 on the key issue of the legality of CAP-based throttling pursuant to subsection 27(2) and section 36 of the Act will persist."*[95]

The application continued with specific examples of error in fact and law including errors in fact on peer-to-peer activities and the use of DPI technologies as well as errors in law, particularly in the way the CRTC had interpreted sections 27(2) and 36 of the *Telecommunications Act*. The CAIP application came as a surprise given that most of the attention had moved to the upcoming net neutrality hearings, placing the CRTC on the defensive just weeks before the hearing were scheduled to take place.

Meanwhile, Charlie Angus, the NDP digital affairs critic, introduced another net neutrality private member's bill[96], which was slightly tougher than his previous bill[97]. The Liberal Party also took a stance as the CRTC was preparing to start the net neutrality hearings. In June 2009, industry critic and Liberal MP Marc Garneau asked during the Question Period:

> *"Mr. Speaker, in a free and open democracy in the 21st century, in an innovative and progressive knowledge economy, no tool is more paramount than the Internet. The Internet is the backbone of today's flow of free ideas and sharing. My party, the Liberal Party, supports the principle of net neutrality and an open and competitive Internet environment. Do the Conservatives support the principle of net neutrality?"*[98]

Then-Industry Minister Tony Clement responded by pointing to his upcoming digital economy strategy conference, but did not take a position on the issue. The ensuing Liberal press release indicated that Liberals viewed traffic management as an anti-competitive behaviour as well as a privacy concern.[99] This marked a critically important development for net neutrality in Canada just weeks before the CRTC hearings on network management. With two major parties – Liberals and NDP – standing squarely in favour of protecting an open Internet, pressure was building on the Conservatives to take a position, particularly given the growing emphasis on developing a national digital strategy for Canada.

The CRTC's net neutrality hearing followed in July 2009, resulting in the arguably the most important legal framework on net neutrality in Canada. The hearing and the resulting *Internet Traffic Management Practices* (ITMPs) guidelines are discussed in the next section.

4. 2009: The CRTC Establishes Internet Traffic Management Practices (ITMPs)

[95] See *Ibid* at para 12.
[96] Bill C-398, *An Act to amend the Telecommunications Act (Internet neutrality)*, 2nd Sess, 40th Parl, 2009.
[97] *Supra* note 52.
[98] *House of Commons Debates*, 40th Parl, 2nd Sess, Vol 144 No 078 (18 June 2009) at 1445.
[99] "Liberals speak out in support of net neutrality", *Liberal Party Newsroom* (19 June 2009) online: Liberal Party of Canada <http://www.liberal.ca/>.

The CRTC's traffic management hearing pitted Canada's telecom and cable companies against a broad range of consumer, creator, and technology groups. The thrust of telecom and cable companies' arguments was that managing their networks, which might include using DPI technologies to identify subscriber activity and limiting available bandwidth for certain applications – i.e. throttling –, was essential to ensure optimal access for all subscribers.[100] Consumer associations, independent ISPs, broadcasters, creator groups, and technology companies, on the other hand, emphasized privacy, competition and consumer rights concerns. During the new media hearing, Rogers Communications had claimed "there is no walled garden, there is no preferred content, it's just a pipe… We are moving to a big, wide-open pipe."[101] At the heart of the traffic management hearing was the quest to assess the validity of this claim.

a. The Technical Issues

From the beginning of the hearing, and based on their questions, it seemed that the CRTC Commissioners had accepted the carriers' claims that congestion was a problem and that inhibiting the use of DPI technologies could result in increased consumer costs for Internet access. In fact, the hearing began with presentations by a number of DPI service providers such as Sandvine Incorporated arguing the need for "prioritizing" technologies in times of congestion – which is not always predictable[102]– and that "an unmanaged network is not a neutral network."[103] The company argued that prioritization could serve a number of legitimate purposes such as "to scrub malicious traffic from a network; to guarantee quality of service for an emergency transmission; to inform a subscriber that he or she may incur extra charges; [and] to boost bandwidth for a file download as part of an on-demand service…".[104] Moreover, DPI service providers claimed that "[g]iven the variety of network architectures between and within

[100] Interestingly, the same telecom and cable companies that now argued that managing their networks was essential, had offered a somewhat different take when confronted with the prospect of doing so in the name of supporting Canadian content in the CRTC's new media hearings a couple of months before. For example, Shaw now maintained that traffic management was necessary to ensure fast, reliable and affordable access. Yet when Shaw's CEO had been asked about the prospect of identifying traffic during the new media hearings, he had told the Commission, "We can only tell you how many bits are coming in or out. We don't know what kind of bit it is. It could be anything from an e-mail to a porno … We don't know that. We spend no time trying to figure out what bits are going to your house. We just don't know." [see CRTC, *Canadian broadcasting in new media hearings*, vol 9 (Gatineau: CRTC, 2009) at para 10263, online: CRTC <http://www.crtc.gc.ca/ >]. It is also noteworthy that even in the new media hearings, an expert witness for MTS Allstream acknowledged that "deep packet sniffing… does happen on some basis. It happens, for instance, under the purview of intelligence agencies quietly…[of which] the consumers haven't been directly told" [see *Ibid* vol 10 at para 11249]

[101] See *Ibid* vol 9 at paras 9822-23.

[102] The issue of whether congestions are predictable or not is relevant to whether ISPs can design their networks so that they could respond to peak periods without resorting to less controversial traffic management practices. See, for instance, the conversation in CRTC, *Transcript of Proceeding: Review of the Internet traffic management practices of Internet service providers*, vol 1 (Gatineau: CRTC, 2009) at paras 247-56, online: CRTC <http://www.crtc.gc.ca/>.

[103] See *Ibid* at para 50. Sandvine subsequently clarified this claim by arguing that when the Internet was first created, users were on equal footing. Over time, however, users have become self-interested and some use more bandwidth compared to others. Consequently, an unmanaged Internet would lead to some users being able to serve their interests at the cost of others [see *Ibid* at paras 321-23.].

[104] See *Ibid* at para 51.

access types, the dynamic nature of networks, Internet applications and congestion management solutions…any new rules around acceptable traffic management practices, particularly any that are prescriptive, would quickly become outdated and could damage the ongoing health of the Internet."[105] Sandvine cautioned against a policy targeting disproportionate users of bandwidth and, instead, advocated a policy that would prioritize time-sensitive and non-bandwidth-intensive applications.[106] It also argued that prioritizing technologies did not necessarily raise privacy concerns, which would depend on how the technology was used.[107]

b. Groups Supporting Net Neutrality

Various Canadian consumer groups focused on who should bear the burden of demonstrating that DPI and other Internet traffic controls were consistent with the law. They proposed that all DPI and other Internet traffic controls were *prima facie* violations of Section 36 of the *Telecommunications Act* and that the onus therefore should fall on the carriers to show that (1) there existed a serious problem and a pressing need to be addressed; (2) the solution minimally impaired users' rights; and (3) the solution was proportional to the harm. Further, if the application for "legitimate" violations of s. 36 was granted based on this three-step test, the consumer should be fully informed of the impact on their content rights. Such disclosure should be made prominently on the ISP's website. Bell, for instance, had refused to indicate how its throttling policies were carried out. Moreover, the groups argued that the guidelines should treat all competitors, users, applications and traffic equally; should increase consumer protection; should facilitate emergency services; and should protect the privacy and security of users.

The consumer groups maintained that DPI technologies should only be used to protect users from unsolicited and malicious content. They stressed that it was "totally unacceptable" when DPI technologies were used for a provider's financial gain. They added that the existing policies were "highly invasive" and that DPI technologies looked deeply into packets revealing what websites had been visited and for how long. For this violation of the privacy of their customers, ISPs did not obtain customers' permission nor did they disclose that they were collecting such information.[108] It is also noteworthy that the consumer groups argued that privacy violations occurred even when the DPI technologies were only used for network management purposes. The CRTC's Chairperson, however, responded that he was not prepared to accept that using DPI technologies was a violation of privacy *per se*.[109]

[105] See *Ibid* at para 54. The company further argued that each traffic management practice should be judged individually at any given time implying that regulation would be unnecessary. [*Ibid* at para 87]
[106] See *Ibid* at paras 62-65.
[107] See *Ibid* at paras 75-77.
[108] See *Ibid* at paras 730-811. Note that the consumer groups believed that s 36 –i.e. the right for content to pass without being observed or changed– was a "fundamental right" that deserved a high standard of protection [*Ibid* at paras 928-30].
[109] See *Ibid* at paras 823-24.

The Open Internet Coalition (OCI), which described its primary purpose as working to keep the Internet fast, open, and available to everyone, made four main arguments. The first focused on innovation with OCI arguing that an open Internet would drive innovation, and that robust access to an open Internet is important to public policy. The second argument was closely related to the first as the OCI argued that application-specific traffic management practices would make the Internet less attractive to users. They pointed out that slower applications would change user behaviour and undermine the Internet's competitive market in applications. Third, the OCI argued that certain traffic managements would be acceptable. As the Internet had moved towards greater online use of multimedia format over time, congestion had become a greater problem. However, the OCI also emphasized that increased capacity had been the primary means of dealing with this issue in the past. Finally, the OCI argued that acceptable traffic management would pass the light-touch "test" derived from the interpretation of ss. 27(2) and 36 of the *Telecommunications Act*. They distinguished between useful traffic management and traffic management that would discriminate, claiming that evidence showed that carriers could manage their networks, reduce congestion, and keep the Internet open at the same time.

Maintaining that they believed discrimination between applications constituted discrimination under s. 27 of the *Act*, the OCI went on to explain their three-part "test" derived from ss. 27 and 36 of the *Telecommunications Act* – namely whether the traffic management practice at issue (1) furthers a pressing and substantial objective; (2) is narrowly tailored to the objective; and (3) is the least restrictive means of achieving the objective. In regards to the first step of the test, the OCI argued that while a debilitating network could be a substantial and pressing objective, the available evidence did not established the existence of debilitating network congestion. They also expressed doubt that peer-to-peer applications such as BitTorrent would "exploit" the Internet. In regards to the second step of the test, they argued that throttling was almost never narrowly tailored to the objective. Further, they argued that throttling had negative effects on innovation and that there were better means of lessening congestion. In regards to the third step of the test, the OCI argued in favour of techniques that were more effective at reducing congestion and that did not discriminate between applications such as increased network capacity.[110]

Various creator and producer groups also expressed support for net neutrality, highlighting the economic potential of BitTorrent-based distribution. For example, the Independent Film and Television Alliance (IFTA) and the Canadian Film & Television Production Association (CFTPA) indicated in their presentations that independent producers were important content creators in Canada and the U.S.; that the Internet was a necessary tool (and sometimes the only tool) for financing, producing and distributing independently produced works; that industry consolidation – i.e. the vertical integration of ISPs with production companies – threatened independently produced works due to preferential treatment (and higher speeds) for allied

[110] For the *OCI* presentation, see *Ibid* vol 2 at paras 991-1055.

productions; that network congestion must be more clearly defined; that increasing capacity would be the best way to ensure broadband service would meet the demand; that traffic management practices must be disclosed and transparent to the customer; and that the CRTC should reconsider whether ISPs should be immune from s. 27(2) of the *Act*. References were made to other methods of dealing with congestion without resorting to throttling –*e.g.* increasing last-mile capacity or deploying content delivery networks.[111]

The Council of Canadians with Disabilities and ARCH Disability Law Centre (ARCH) urged the CRTC to establish clear guidelines and interpretive framework for s. 36 and s. 27. They argued that traffic management practices must not be directly or indirectly discriminatory and should not force people with disabilities to forego their privacy. ARCH also presented its own three-step approach to s. 36 disputes –*i.e.* (1) consideration of whether the traffic management practice at issue is caught under s. 36; (2) determination of whether the practice is contrary to law and amounts to unjust discrimination; and (3) determination of whether the practice can be saved based on neutral/positive intervention criteria (e.g. by using the minimum impairment test as suggested by the OIC). Finally, given the myriad of helpful programs on the Internet, the groups insisted that a white-list approach to obtaining special exemptions from traffic control (e.g. in the case of necessary services for disabled people) was impractical. Hence, disclosure of traffic management practices would be critical for people with disabilities.[112]

The Canadian Internet Policy and Public Interest Clinic (CIPPIC) on behalf of Campaign for Democratic Media (CDM) recommended the establishment of normative guidelines and boundaries for ISP behavior, particularly for determining whether throttling practices violated ss. 27(2) and 36. CDM viewed the problem as the encroaching on the physical and theoretical space of the "public Internet" in service of private concerns. In regard to congestion, CDM argued that both the user and supply side of the equation should be taken into account: the ISPs were not provisioning to the best of their ability, nor was peer-to-peer a reason for the congestion. CIPPIC, therefore, argued that "[f]unctional marketplaces meet demand with supply, not by squashing demand." Moreover, CIPPIC and CDM strongly supported the values of open Internet to reject the legitimacy of throttling practices by ISPs. It was argued that the main way to allow ISPs to compete would be to increase bandwidth offerings, so they would not monetize on artificially created scarcity. It was also reminded that no one – including the ISPs – had a legitimate proprietary claim to the Internet. CDM also question a number of assumptions and definitions held by CRTC such as the definition distinction between the "public Internet" and "private services" and the assumption that unrestricted traffic increases would lead to congestion and then to the deterioration in services. Instead, CDM maintained that congestion would occur if increased Internet traffic were not met with adequate provisioning. CDM also questioned the CRTC's assumption that certain Internet traffic management practices might be appropriate. Any such practice, CDM argued, was an act of "traffic interference." According to CDM, peer-to-

[111] See *Ibid* vol 3 at paras 2040-2117.
[112] See *Ibid* at paras 2282-2348.

peer specific traffic management was discriminatory against a class of applications and users and a *prima facie* violation of s. 36 by controlling content and message.[113]

Many telecom companies and independent ISPs also expressed support for CRTC action. MTS Allstream, a leading Manitoba-based telecom provider, argued that market competition should be promoted since that would obviate the need for regulation or traffic controlling. It maintained that Internet traffic management practices should only be applied in a retail context and should never be imposed on a wholesaler from the dominant carrier (for, according to MTS Allstream, once sold to a wholesaler, the traffic would be out of the dominant carrier's network and would not create congestion in that network). Moreover, MTS Allstream maintained that the CRTC should implement a pragmatic case-by-case approach to assessing and justifying each Internet traffic management practice. One criterion for assessing the reasonableness of a traffic management practice might be whether such arrangements were applied to all content providers. ISPs manage their network by network planning and engineering, by compliance with laws of general application, by applying measures agnostic in their treatment of content, and by content application protocols (CAP) –e.g. blocking, expediting, throttling, DPI technologies. MTS Allstream maintained that using CAP measures would be necessary in some cases (e.g. unanticipated traffic surges on the network); and that DPI technologies were just one tool among many for a larger network management strategy.[114]

The Union des Consommateurs, a Quebec-based consumer group, suggested that there was insufficient evidence of actual congestion. It urged the CRTC to consider many issues including concentration of ownership, quality of service affordability, and competition. The Union maintained that for an acceptable throttling of a specific application, there should be clear evidence that there was congestion in the network; that time-sensitive applications were experiencing unsatisfactory quality of service; and that the throttled application was a significant cause of the congestion. According to the Union, it was not clear from the presented data that peer-to-peer applications were the primary cause of the congestion; and the "modest growth rates" in peer-to-peer traffic could be accommodated by reasonable increases in network capacity.

If it was determined that network management was necessary, the Union argued that there were several options other than "application-specific throttling" (e.g. controlling the rates of individual users during peak periods). The Union believed that the use of DPI technologies and their processing of the payload and the "application layer header" would raise privacy concerns, threaten robustness by violating layer design principles, and promote the practice of data encryption. Instead, the Union proposed the use of Shallow Packet Inspection (SPI) technologies, since they did not involve any examination of packet payloads which alleviated the privacy concerns. In SPI technologies, statistical features were collected for each flow and, based on

[113] See *Ibid* vol 4 at paras 3306-3424.
[114] See *Ibid* vol 3 at paras 2586-2679.

these features, the flows could be categorized into application classes. According to the Union, experimental studies had shown that this classification approach can be very accurate. UdC stated that the classes are sufficiently specific for network management.[115]

The CAIP maintained that congestion was a symptom of the lack of competition in Canadian ISP landscape. It urged CRTC to prevent dominant carriers from traffic management on their wholesale traffic, except for network security (e.g. to prevent network attacks). In order to drive competition, the use of traffic management for retail should be end-user determined, that is, consent must be required. On behalf of "independent ISPs", CAIP argued that internet traffic management practices done in an aggregate fashion and without customer's consent would contradict s. 36 and s. 27(2) by interfering with the "purpose or meaning of telecommunications." CAIP also reiterated the argument that building network capacity and unbundling networks would be a less intrusive solution for network management.[116]

During the follow-up questions, CAIP emphasized the necessity of disclosure but maintained that Internet traffic management practices did not use personal data although it might occur in the future for commercial reasons. As a result, CAIP argued that there was no need to go beyond the existing privacy framework (i.e. *PIPEDA* and CRTC's decisions on confidentiality). Moreover, CAIP emphasized that congestion should never drive policies relating to Internet traffic management practices. Instead, the inquiry should be about consumer choice and competition. CAIP also referred to some of MTS Allstream's evidence that showed in the U.K., many wholesale services had been unbundled to solve the problems caused by the vertical integration of British Telecom. This unbundling policy led to more competition and, in turn, alleviated the net neutrality problem. CAIP also stressed that wholesale customers were not causing congestion since their markets were far too small. The fact that Bell had first applied its traffic management practices to its retail markets, and only later to its wholesale markets indicated that the two can be segregated and that the wholesale customers were not an immediate concern for Bell. CAIP further clarified that at the retail level, any form of Internet traffic management practice should be allowed if consented by the end users.[117]

c. Against Net Neutrality

Consumer, creator groups, and some independent and regional telecommunications companies may have lined up in favour of net neutrality, but the incumbent telecom and cable operators opposed new regulatory measures. Telus maintained that it had the right to manage the traffic if congestion became a more serious problem. The company also viewed network capacity building as one of the solutions to capacity challenges. Other solutions included traffic management and consumption-based pricing. Telus further argued that ex ante "one size fits all" regulation could increase the risk for telecommunications companies. Instead, Telus suggested the CRTC could

[115] See *Ibid* vol 6 at paras 4718-70.
[116] See *Ibid* vol 4 at paras 2956-3031.
[117] See *Ibid* at paras 3050-3275.

outline broad principles. Then if there was a problem of undue preference, Telus maintained, it should be brought forward and be dealt with – i.e. an ex post approach. Finally, Telus argued that in addition to undue preferences, the CRTC should be concerned about the necessity of allowing fair forms of discrimination.[118]

During the follow-up questioning period, Telus argued that while the Internet services are equivalent to public utility, because of the competition among the ISPs, they are not themselves a public utility. Telus also claimed that the vast majority of Internet users were not concerned with traffic management decisions by the ISPs; though it also admitted that if traffic management practices were to infringe users' privacy rights, then they would care about it. Yet Telus maintained it was dealing with congestion management which, from the customer's perspective, meant better service; and that the already existing federal privacy legislation was sufficient to address potential concerns.[119]

In its presentation, Rogers Communications Inc. noted that Canada had the highest penetration of cable modem service in the world and the highest penetration of broadband among the G8 countries. All of this had been accomplished, according to Rogers, with a minimum of government regulation. Rogers argued that market forces, not government intervention, were responsible for this achievement. Confirming their commitment to an open Internet and denying any anti-competition or anti-privacy measure on their part, Rogers urged the Commission not to establish Internet traffic management guidelines. Instead, Rogers believed that it was better to adopt the FCC's approach of looking at individual Internet traffic management practices on a case-by-case basis. In that way, the Commission would ensure that Canadian ISPs had the flexibility needed for proper management of their networks. Rogers pointed out that their traffic management practices did more than simply shape traffic. It also protected customers and the network from spam, prevented denial of service attacks and virus attacks, and blocked access to child porn sites.

Rogers acknowledged that it did rate shape upstream peer-to-peer traffic to make the network fair for other users. It emphasized that its practices did not simply favour its own services and that without traffic management practices, competitive VOIP providers would also be hurt by congestion. In regards to expansion of network capacity as a solution to congestion, Rogers believed that it would require a huge amount of additional upstream capacity to solve the congestion problem leading to increased cost for all consumers. For wholesale customers, Rogers believed that there should be sufficient disclosure to allow them to understand the nature of the services they were acquiring and to respond to their own customers' inquiries appropriately. In regards to privacy, Rogers argued that privacy issues raised by consumer groups were largely theoretical and not based on actual practice. Rogers noted that they did not at the time rate shape

[118] See *Ibid* vol 5 at paras 4065-4114.
[119] See *Ibid* at paras 4140-4366.

their mobile wireless data traffic, but believed that with the growth of use of wireless services, some form of traffic management would be necessary in the future.

In regard to s. 36 of the *Telecommunications Act*, Rogers maintained that its traffic management practices did not control the content of peer-to-peer file sharing traffic; nor did it change the meaning or purpose of the file in question.[120] Furthermore, in regards to s 27(2), Rogers maintained that the section was to protect application providers and not the application themselves.

Videotron, the largest service provider in Quebec, also argued that the CRTC should not impose regulation. Although at the time, it only used "economic measures" to deal with potential problems, it refused to rule out the use of technical measures (i.e. traffic management) in the future. Videotron also argued that regulation should only be implemented if a "real problem" was identified. Videotron, however, believed that dominant networks should apply Internet traffic management practices only to their own end-users and not to their reseller customers. Moreover, network management was necessary because of the high costs of capacity expansion and the fact that it was only the underlying network operator, and not the reseller, who should pay for the these high costs.[121]

Shaw Communications Inc. noted that even with significant investments, it still experienced network congestion challenges, particularly from peer-to-peer traffic. Therefore, Shaw argued it needed to combine investment with appropriate and necessary network management strategies. It noted that the *Telecommunications Act* already prohibited ISPs from granting an undue preference or from interfering with the meaning of a communication, and maintained that the existing regulatory framework was working effectively to protect consumers.

Shaw stated that it used DPI technologies to shape upstream peer-to-peer traffic because this was "the most effective and efficient measure" to address the bandwidth consumption of peer-to-peer applications. Shaw noted that while its traffic management devices operated on a 24/7 basis, the devices automatically shaped traffic only during periods of congestion. Shaw maintained that it was acceptable for individual ISPs to select their own network management strategy that might include a combination of approaches such as DPI technologies, bandwidth limits, excess bandwidth usage charges, time of day pricing, caching, increased capacity or any other practices that did not breach s. 27(2) or s. 36 of the *Telecommunications Act*. As for the DPI technologies, Shaw believed that they did not influence the meaning or purpose of the communication.

In its opening remarks, Bell Canada argued that the heart of the hearing was a dispute about innovation. It noted that the practices it had implemented were (i) narrowly focused and limited to non-time sensitive traffic, (ii) confined to a defined period of time; and (iii) did not block access to content. In regards to privacy, Bell confirmed that its DPI technologies did not inspect

[120] See *Ibid* vol 6 at paras 4892-4939.
[121] See *Ibid* at paras 5332-81.

the user content of communications, and guaranteed that those technologies were being used by Bell only for purposes of traffic management. Bell stated that contrary to what had been presented to the CRTC by others, retail users and wholesale GAS users shared the same network. As a result, wholesale traffic impacted retail traffic and vice-versa. Bell also claimed that wholesale customers of Bell had downplayed their impact on Bell's retail network by pointing to their overall market share.

Bell proposed three guidelines for the CRTC's consideration: (1) limiting negative impacts – that ISPs should make "reasonable" efforts to limit the negative impacts of their Internet traffic management practices on users, services, protocols or applications; and "reasonable" implied the recognition that different networks faced different problems and therefore ISPs needed flexibility; (2) transparency – that ISPs should disclose to affected retail and wholesale customers "the general nature of implemented … [Internet traffic management practices] in a manner that does not compromise the security of networks and commercially sensitive information"; and (3) privacy – that ISPs should implement Internet traffic management practices in a manner consistent with applicable privacy laws. In regards to s. 36 of the *Telecommunications Act*, Bell believed it would rarely be applicable to traffic management issues.[122]

Bell maintained that existing privacy legislation (e.g. PIPEDA) would permit the use of aggregated data for marketing with customer consent.[123] Bell also maintained that a "least intrusive test" would imply that there was one correct "least intrusive" method while there was no consensus as what constituted "least intrusive." It would be better, Bell argued, to avoid such correctness standard and instead, use a reasonableness standard. This was why Bell supported an ex post, not ex ante, framework. According to Bell, the problem with protocol-agnostic approaches was that these approaches would slow down all of a user's traffic including time-sensitive traffic. While some would argue this non-discriminatory system would be a positive thing, Bell believed that it would be unreasonable – and in fact more intrusive.[124]

In its presentation, Cogeco Cable Inc. stated that it employed traffic shaping measures as part of its network management, targeting peer-to-peer traffic applications that consumed a disproportionate amount of bandwidth. Cogeco cited ensuring a "fair and sustainable" Internet service as the reason behind traffic management practices. Cogeco then summarized the key features of its traffic-shaping technology including no interference with the content; no blocking or disruption of the telecommunication (but slowing down the transmission of peer-to-peer traffic by inspecting the header and the payload of each packet to the minimum extent required in order to identify the specific signature of peer-to-peer protocols); and no inspection of any personal identifier. Cogeco also maintained that no regulatory measure for Internet traffic

[122] See *Ibid* vol 7 at paras 5972-6032.
[123] See *Ibid* at paras 6319-33.
[124] See *Ibid* at paras 6348-74.

management practices was required, nor were any additional rules need to protect personal privacy.[125]

Primus Telecommunications Canada Inc. asserted that all ISPs should be able to manage their networks and to employ Internet traffic management practices as they saw fit; that all such practices were generally acceptable and with consent, there was nothing a priori wrong about them; and that DPI technologies were only for network management and planning during congested moments. Primus believed that all ISPs should disclose their Internet traffic management practices on both retail and wholesale services, but should not disclose security-related practices.[126]

Barrett Xplore Inc., a satellite Internet provider, discussed traffic management from the perspective of a small ISP that focuses on rural communities. Barrett believed that each ISP should be permitted to adopt traffic management tools that were consistent with its particular circumstances, network configurations and business models. It particularly emphasized the need to employ appropriate tools to manage traffic at peak usage times to ensure best possible quality of service for all customers.

In regards to application-specific traffic management, Barrett maintained that to discriminate against bandwidth hogging applications was not unjust or unreasonable under s. 27(2) of the *Telecommunications Act*. The employed traffic management technologies were not directed at individual users or individual applications. Instead, they were directed at excessive use of bandwidth at peak periods and were applied without discrimination to all; and as long as customers were made aware of service limitations when they subscribed, these traffic management tools were both reasonable and necessary. Without these traffic management tools, Barrett argued, affordable services would not be viable for the rest of the customers and there would be no business rationale for the extension of services to rural and remote areas of Canada via satellite wireless networks.

d. The Decision

Having heard from all sides, the CRTC released its net neutrality decision in October 2009.[127] Although the CRTC's ITMPs decision did not go as far as some advocates might have hoped[128],

[125] See *Ibid* vol 5 at paras 4401-71.
[126] See *Ibid* vol 4 at paras 3779-3855.
[127] CRTC, *Telecom Regulatory Policy CRTC 2009-657: Review of the Internet traffic management practices of Internet service providers*, (Ottawa: CRTC, 2009), online: CRTC <http://www.crtc.gc.ca/>.
[128] For instance, the CRTC allowed usage billing and bandwidth caps. The increasing use of these methods, however, has begun to attract increasing critical attention in both the media and at the political level; for these methods further undermine choice, accessibility and pricing for the Internet in Canada. In early 2011, the CRTC released its decision on usage based billing [CRTC, *Telecom Decision CRTC 2011-44: Usage-based billing for Gateway Access Services and third-party Internet access services*, (Ottawa: CRTC, 2011), online: CRTC <http://www.crtc.gc.ca/>]. The content of the decision, however, indicated that the CRTC itself was not certain on how to deal with the issue [see an extensive analysis of the decision and the underlying issues in Michael Geist,

it was a move forward on several important fronts. The decision signified that traffic management was no longer a free-for-all tool at the disposal of ISPs. That said, the decision nevertheless guaranteed that traffic management practices such as throttling would continue. The key elements of the decision on retail services were as follows:

> *(1) A new framework for considering traffic management is introduced. Consumers can complain about traffic management practices or the Commission can bring an action on their own. Where there is a credible complaint, the ISP will be required to:*
>
> > *describe the ITMP being employed, as well as the need for it and its purpose and effect, and identify whether or not the ITMP results in discrimination or preference.*
>
> *If there is any degree of discrimination or preference:*
>
> - *demonstrate that the ITMP is designed to address the need and achieve the purpose and effect in question, and nothing else;*
> - *establish that the ITMP results in discrimination or preference as little as reasonably possible;*
> - *demonstrate that any harm to a secondary ISP, end-user, or any other person is as little as reasonably possible; and*
> - *explain why, in the case of a technical ITMP, network investment or economic approaches alone would not reasonably address the need and effectively achieve the same purpose as the ITMP.*
>
> *(2) There are two key additional considerations. First, traffic management that degrades or prefers one application over another may warrant investigation under section 27(2) of the Act. Second, economic traffic management practices (i.e. bit caps) are generally viewed as acceptable.*
>
> *(3) The Commission engaged the throttling issue. It ruled that for time-sensitive Internet traffic (i.e. real-time audio or video), where the throttling creates noticeable degradation, this "amounts to controlling the content and influencing the meaning and purpose of the telecommunications in question." The Commission will require prior approval for such activities. Even for non-sensitive traffic, the CRTC ruled that it is possible to slow down the traffic to an extent that it amounts to blocking or controlling the content, in which case prior approval will be required.*

"Unpacking The Policy Issues Behind Bandwidth Caps & Usage Based Billing" (1 February 2011); see also Michael Geist, "What to do About Retail Usage Based Billing: A Modest Proposal" (7 April 2011); Michael Geist, "Why Net Neutrality and Usage Based Billing Are Two Sides of the Same Coin" (11 July 2011); and Michael Geist, "Competition, Not Congestion Driving Internet Data Cap Debate" (18 July 2011), online: Michael Geist's Blog <http://www.michaelgeist.ca/>].

> *(4) The Commission mandated new disclosure requirements. It required ISPs to disclose their traffic management practices to customers, including: why there are being introduced; who is affected; when it will occur; what Internet traffic is subject to the traffic management; and how it will affect an Internet user's experience (including specific impact on speed).*
>
> *(5) The Commission also established new privacy requirements on the use of information obtained from deep-packet inspection. It mandated ISPs "not to use for other purposes personal information collected for the purposes of traffic management and not to disclose such information."*[129]

In addition to the retail side of the issue, the decision also addressed wholesale services. Where incumbents treat independent ISPs in the same manner as their retail customers, the same complaints-based approach applies. Where the approach is more restrictive, prior approval is required.[130]

As mentioned in the summary above, the decision introduced a test that was similar to what consumer groups had recommended during the hearings; it acknowledged the problems with application-specific measures; it also introduced new disclosure requirements, new privacy safeguards, and an agreement that throttling can violate the law in certain circumstances.

5. 2009-12: Enforcement of ITMPs and other Net Neutrality Laws

Prior to ITMPs hearings, the CRTC was not particularly assertive in enforcing net neutrality principle in Canada. As for ss. 27(2) and 36 of *Telecommunications Act*, for instance, the CRTC had sought to limit the applicability of these provisions.[131] As discussed in the previous section, the introduction of ITMPs framework by the CRTC in 2009 was viewed as a positive move by many net neutrality advocates in Canada. From the beginning, however, the big question was how to enforce these new rules. Indeed, by placing the onus squarely on consumers, the CRTC had virtually guaranteed continued throttling and a steady stream of cases.

Several proposals emerged to address these concerns. These included asking the CRTC to conduct regular compliance audits of ISP traffic management practices, calling on the government to require the CRTC to monitor ISP compliance with its traffic management

[129] *Supra* note 128 at paras 20-99.
[130] *Ibid* at paras 68-95.
[131] See, e.g., CRTC, *Telecom Decision CRTC 2005-28: Regulatory framework for voice communication services using Internet Protocol*, (Ottawa: CRTC, 2005); and CRTC's hand-off approach to the Internet regulation in CRTC, *Broadcasting Regulatory Policy CRTC 2009-329: Review of broadcasting in new media*, (Ottawa: CRTC, 2009), online: CRTC <http://www.crtc.gc.ca/>. Note that the New Media decisions refer to one of CRTC's initiatives in determining how to adapt Canadian regulation to new media environments such as the Internet. The New Media Project initiative analyzes whether new media should be regulated and assesses the impact of regulation on the creation and distribution of Canadian content. The initiative also considers critical access issues including network neutrality –which is sometimes referred to as "Internet traffic prioritization."

guidelines and providing financial support to consumer groups who wish to conduct their own investigations and more engagement by the federal government (e.g. in establishing neutrality for wireless Internet access).

By the early 2010, the policy responses of the biggest ISPs – including Bell, Rogers, Shaw, Telus, Cogeco and Vidéotron – to the new guidelines were mixed. Among these six players, Telus and Vidéotron did not use throttling or traffic shaping technologies that limited the speeds of some applications at the time. Of the remaining four providers, no one made it easy to find the disclosures and at least two were arguably not compliant with the CRTC requirements. Bell featured the most detailed disclosure, providing specific information about its policies and their impact in compliance with what CRTC had asked. The Rogers policy was not quite as extensive, yet it also covered much the same terrain, including a description of the policy, the frequency of traffic shaping, and the resulting limitations in their service (including the specific impact on speed). By contrast, neither Shaw nor Cogeco appeared to meet the CRTC requirements. Shaw's policy did not disclose the actual speeds users encounter when it throttled peer-to-peer activity. Cogeco, while implausibly claiming that its traffic management practices will not affect customer experience, similarly did not disclose the actual speeds.

Some two years after the CRTC conducted its much-publicized hearing on net neutrality, there seemed to be a net neutrality "enforcement failure" in Canada. During these two years, virtually all major Canadian ISPs were the target of complaints, but there were few, if any, consequences arising from the complaints process. In fact, the CRTC frequently dismissed complaints as being outside of the scope of the policy, lacking in evidence, or sided with Internet provider practices.[132] Rogers Communications was the target of nearly half of all cases opened in response to net neutrality complaints but the company suffered no serious consequence. For instance, in the fall of 2010, a complaint was sent to the CRTC regarding Rogers degrading peer-to-peer traffic. Rogers attempted to downplay the issue but finally acknowledged that the traffic management requires a change in publicly disclosed policy.[133] In response to the complaint, the CRTC sent a letter to the company advising that the company's public disclosures had not been compliant with CRTC Internet traffic management policy requirements. Although Rogers had already admitted the lack of disclosure and had promised to address the issue, the CRTC found that the disclosures only focused on the impact of its practices on uploading.[134] Rogers responded to the CRTC maintaining that there was no need to update its disclosure practices regarding downstream traffic. It further questioned why Rogers was being singled out for changing its disclosure policies, arguing that while it was true that upload traffic shaping might impact download speeds in some applications, that was the responsibility of the application provider, not

[132] See, Michael Geist, "Canada's Net Neutrality Enforcement Failure" (8 July 2011), online: Michael Geist's Blog <http://www.michaelgeist.ca/>.
[133] See "Rogers' BitTorrent Throttling Experiment Goes Horribly Wrong" (13 December 2010), online: TorrentFreak <http://torrentfreak.com>.
[134] An electronic copy of the letter is available online: Michael Geist's Blog <http://www.michaelgeist.ca/component/option,com_docman/task,doc_download/gid,38/>.

the ISP. The company did offer a minor modification to its disclosure statement.[135] Two days later, the CRTC closed the net neutrality complaint against Rogers, concluding that it was satisfied with the ISP's response and disclosure practices.[136]

Bell Canada was hit with a complaint in November 2010 over throttling download speeds from a music storage website. Bell admitted its deep-packet inspection technology was mistakenly treating downloads from the website as peer-to-peer activity and slowing connection speeds. Bell promised a fix, but only after asserting that it was compliant with the guidelines.[137]

By July 2011, there had been only one complaint that had led to a clear change in provider policy. In January 2010, ExaTEL, an Ontario-based Internet phone company, filed a complaint against Barrett Xplore, a satellite Internet provider. ExaTEL alleged that Barrett Xplore was degrading Internet telephony traffic, creating an unfair advantage for its own phone service. The CRTC ruled that there was no undue preference, but that the throttling of time sensitive traffic violated its guidelines. Faced with the prospect of changing its practices or seeking special approval from the CRTC, Barrett Xplore changed its throttling approach to ensure that Internet telephony was unaffected.[138]

On occasion, the CRTC itself proved to be the source of the problem. In March 2010, for instance, a complaint was filed against Cogeco, which traffic shaped peer-to-peer applications on a 24/7 basis. Given the CRTC's requirement that traffic management limits be linked to actual network congestion, the Cogeco policy raised red flags. Even so, the CRTC demanded that the complainant provide more evidence before it would investigate. As another example, in a December 2009 complaint against Bell over throttling access to the MediaMonkey.com website, the CRTC dismissed the complaint on the grounds the site did not appear in Bell's list of affected sites.[139] Even when the CRTC pursued a complaint, there was little actual investigation. Most activity was limited to exchanging correspondence or prodding Internet providers to respond. This typically led to revised disclosures, rather than real changes.

In 2011, the issue of throttling online gaming emerged as a serious concern. In July 2011, the CRTC issued a warning to Rogers in the ongoing dispute over its alleged throttling of the online game, World of Warcraft. The Commission said it was not persuaded the issue had been

---

[135] An electronic copy of the response is available online: Michael Geist's Blog <http://www.michaelgeist.ca/component/option,com_docman/task,doc_download/gid,45/>.
[136] An electronic copy of the notice of closure is available online: Michael Geist's Blog <http://www.michaelgeist.ca/component/option,com_docman/task,doc_download/gid,46/ >.
[137] See *Supra* note 146.
[138] *Ibid*. *Xplornet Communications Inc*. (formerly *Barrett Xplore Inc*.) issued a press relapses in July 2011 regarding the matter. For the press release and Michael Geist's response see Xplornet Communications Inc., "Warning to Editors re: Allegations made by Michael Geist" (12 July 2011), online: CNW Group <http://www.newswire.ca/en/story/745965/warning-to-editors-re-allegations-made-by-michael-geist>; and Michael Geist, "The Xplornet's Release: Digging into the Documents" (14 July 2011), online: Michael Geist's Blog <http://www.michaelgeist.ca/>.
[139] See *Supra* note 146.

completely resolved and asked the company to address ongoing concerns.[140] No material improvement followed and frustrated online gamers launched a new group to monitor and test net neutrality concerns.[141] In August 2011, the CRTC asked Rogers again to probe complaints from an online gaming group about throttling another popular online game, Call of Duty.[142] Later, Rogers admitted that it "may" be throttling online games and the CRTC requested Rogers to stop slowing down speeds of online games.[143]

After more than 30 investigations in nearly two years, and it was clear improvements were needed. The CRTC released new guidelines for responding to complaints and enforcing net neutrality rules in September 2011.[144] The decision included a commitment to publish quarterly reports featuring a summary of the number and types of complaints the CRTC has received, including the number of active and resolved complaints. Moreover, any findings of non-compliance would be published on the Commission's website and would include the ISP's name and the nature of the complaint. The move toward greater transparency was welcome and an important step in pressuring ISPs to comply with the guidelines. The new guidelines also established a strict timeline for responses by complainants and ISPs in order to avoid Xplorenet-type situations that dragged on for months before the ISP addressed complaints over its traffic management practices.

The new guidelines also set out the specific requirements for individual complaints. It noted that complaints are appropriate if:

> *"the ISP has not met the disclosure requirements of the ITMP policy;*
>
> *the ISP's ITMP adversely affects his or her ability to access certain applications (for example, if he or she is continuously disconnected from an application, resulting in the application becoming unusable);*
>
> *the ISP has changed an ITMP to make it more restrictive or has introduced a new ITMP without providing 30 days' notice;*
>
> *the ISP has otherwise failed to comply with the requirements of the ITMP policy; or*

[140] An electronic copy of the warning is available online: Dropbox <http://dl.dropboxusercontent.com/u/9038867/Rogers/Rogers_process_letter_13_July.pdf>.
[141] See Jason Koblovsky, "Canadian Gamers Fed Up With CRTC on Net Neutrality issues", *Open Media* (4 August 2011); and , "It's Official: Gamers have Caught Rogers Violating Internet Openness Rules", *Open Media* (27 October 2011) online: Open Media <https://openmedia.ca/>.
[142] See "Rogers asked to probe possible game throttling", *CBC* (30 August 2011) online: CBC <http://www.cbc.ca/>.
[143] See Peter Darbyshire, "CRTC tells Rogers to stop throttling online games", *The Province* (16 September 2011) online: The Province <http://www.theprovince.com>.
[144] See CRTC, *Telecom Information Bulletin CRTC 2011-609: Internet traffic management practices – Guidelines for responding to complaints and enforcing framework compliance by Internet service providers*, (Ottawa: CRTC, 2011), online: CRTC <http://www.crtc.gc.ca/>.

the ISP's ITMP violates the Act."[145]

The CRTC also decided that the complainant must provide evidence describing

"what part of the ITMP framework the complainant believes the ISP has not followed (see the list above for examples of circumstances that would warrant a complaint);

when the problem occurred and whether it is a recurring problem;

what application was affected;

how the application was affected; and

any steps taken to resolve the complaint directly with the ISP, including the ISP's response(s)."[146]

These requirements seemed to be beyond the capabilities of most Internet users, however, who typically lack the technical expertise to mount an effective complaint. The fact that the CRTC kept its user complaints-based approach (in contrast to conducting pro-active audits of ISP practices) undermined serious enforcement of net neutrality rules. Furthermore, the CRTC still lacked tough penalty power – e.g. the power to levy financial penalties for net neutrality violations.

Despite these major shortcomings, the new guidelines indicated that the Commission was prepared to adopt a more muscular approach. Rogers became the first ISP to face "enforcement" actions in response to its throttling of online games.[147] Around the same time, Bell advised its wholesale Internet provider customers that it was dropping its throttling practices, citing reduced network congestion from peer-to-peer file sharing. This announcement raised the prospect that the company's ongoing retail throttling practices might be violating the CRTC's guidelines due to the decline in congestion.[148] The two cases, Rogers and Bell, were viewed on how successful – or serious– the CRTC would be on the enforcement side.

In January 2012, the CRTC notified Rogers that it had concluded its investigation and that the company had indeed violated the ITMPs rules. The CRTC stated that Rogers's use of technical ITMP to unidentified time-sensitive traffic using default peer-to-peer ports would amount to noticeable degradation of such traffic and hence require prior. The CRTC gave Rogers two weeks to rebut the evidence or become compliant with the law, leading to Rogers' announcement

[145] *Ibid* at para 13 [footnote omitted].
[146] *Ibid* at para 14 [footnote omitted].
[147] The CRTC sent Rogers file to its Compliance and Enforcement Sector on October 27, 2011 [an electronic copy of CRTC's letter to complainant is available online: Open Media <https://openmedia.ca/sites/openmedia.ca/files/Koblovsky_File-545613_27-10-2011.pdf>].
[148] See Michael Geist, "Net Neutrality Enforcement Put to the Test" (8 November 2011), online: Michael Geist's Blog <http://www.michaelgeist.ca/>.

that it would drop Internet throttling for all customers by the end of 2012.[149] The CRTC also fulfilled its promise to release net neutrality complaints statistics via its website.[150] These developments indicated that once the CRTC demonstrates its willingness to enforce the guidelines, it quickly spelled the end of most traffic shaping.[151]

6. Conclusion

The emergence of Canadian net neutrality regulation provides an important lesson in the role that public can play in shaping regulatory policy. Powerful incumbent telecom companies, government policy makers, and regulators initially dismissed the issue, yet it gradually gained momentum through an unlikely combination of consumer groups, technology companies, and creator interests. Those groups successfully leveraged the policy process to force the issue onto the policy agenda and open the door to a regulatory approach that carefully struck a balance between reasonable traffic management practices and activities that could prove harmful to consumer or competition interests.

In the aftermath of the new Internet traffic management practice policy, the challenge of effective enforcement emerged as a key concern. The experience highlights the potential disconnect between policy and enforcement, with the danger of complacency arising within the policy realm once an issue has been addressed. The Canadian experience suggests that developing the policy is only the first step in a process that requires all participants – most notably regulators – to remain vigilant in enforcing the newly developed rules and regulations.

The development of Canadian net neutrality rules are also notable for their inclusion of more than just competition concerns that could arise from a two-tier Internet or from throttling Internet traffic. The privacy implications of traffic management practices played an important role throughout the policy process, as is reflected in the final guidelines that establish specific rules on the use of deep packet inspection. The connection between privacy and net neutrality may not be immediately apparent, but the involvement of the Privacy Commissioner of Canada, privacy groups, and technical experts, succeeded in convincing the Canadian regulator that multiple-use technologies such as DPI could have significant privacy implications. Rather than

[149] An electronic copy of the letter is available online: CRTC <http://www.crtc.gc.ca/eng/archive/2012/lt120120.htm>; See also Rita Trichur, "Rogers vows end to Internet 'throttling' in 2012", *The Globe and Mail* (3 February 2012) online: The Globe and Mail <http://www.theglobeandmail.com/>. It is noteworthy that in spite of Rogers's announcement, the CRTC kept monitoring the company, sent another letter to Rogers following the identification of yet another violation of the ITMPs rules, and asked the company for immediate addressing of the new traffic shaping case [an electronic copy of the letter is available online: CRTC <http://www.crtc.gc.ca/eng/archive/2012/lt120229.htm>].

[150] See CRTC, "Status Report – Complaints Related to Internet Traffic Management Practices (ITMPs)", online: CRTC <http://www.crtc.gc.ca/eng/publications/reports/itmp-pgti.htm>.

[151] See Michael Geist, "How the CRTC Helped to Put An End to Internet Throttling" (2 March 2012); and Michael Geist, "Celebrating the Canadian Digital Policy Success Stories" (1 July 2013) online: Michael Geist's Blog <http://www.michaelgeist.ca/>.

simply barring the use of such technologies, the regulator chose to establish strict limitations designed to ensure consistent privacy protections both online and offline.

While the Canadian experience may provide a model for other countries considering net neutrality regulation, the limits of the policy should also be borne in mind. Enforcement shortcomings remain a concern, particularly since the policy is dependent on complaints from users that may not have the technical expertise to fully investigate potential violations. Moreover, the policy was conceived at a time when wireless Internet access was in its infancy. Although some stakeholders specifically cited the need to develop an inclusive policy that addresses both wired and wireless Internet services, the wireless side of the equation has yet to be fully tested.

Even with those future challenges, the Canadian story of developing a consensus around one of the most contentious Internet issues provides a useful illustration of the benefits of active civil society groups and a regulator with the framework and willingness to address challenging policy issues.

Criminal Policy on Net Neutrality and Communication Confidentiality:

The legal, practical and academic status and prospects of Net Neutrality and Communication Confidentiality in the United Kingdom and Europe

Professor Christopher T. Marsden,

University of Sussex

Consultancy Report for Korean Institute of Criminology

13 October 2013

Contents

Introduction

This report sets out the legal, practical and academic status and prospects of net neutrality and communication confidentiality in the United Kingdom (UK) and Europe. I begin by explaining the development of United States law, European net neutrality in law, and the prospects for reform set out by the European Commission in September 2013. The key issue analyzed is the definition of 'reasonable traffic management'. Most legal frameworks appear to grant exceptions to net neutrality for ISPs to cure temporary short-term congestion, prevention of spam and security concerns, and legal enforcement. However, there are also significant privacy concerns with net neutrality. I explain the technical and legal framework for illegal interception of communications confidentiality – which in Europe is termed breach of 'electronic privacy' or e-privacy. The relevant current European laws in addition to the 2009 telecoms directives are the existing Privacy Directive 95/46/EC and the Data Retention Directive (2006/24/EC) which amends the E-privacy Directive (2002/58/EC). I also explain the UK legal framework for interception of communications which is directly related to both e-privacy and net neutrality. Privacy regulators adjudicate where content discrimination contains traffic management practices which collate personal subscriber data.[1] I consider the prospects for reform of European net neutrality and e-privacy laws as proposed by the European institutions in 2012-13. I examine in detail the PHORM/British Telecommunications plc (BT) trial of behavioural advertising using Deep Packet Inspection (DPI) in the UK. I go on to consider the 2011-12 reforms to UK e-privacy and interception law brought about as a result of a legal case brought by the European Commission for inadequate user protections in UK implementation of e-privacy laws. Finally, I explain the difficulties in regulating network neutrality unless there is very strong national and international cooperation between privacy and telecommunications regulatory functions.

[1] See Directive 95/46/EC of 24 October 1995, OJ L 281/31 (1995); Directive 2002/58/EC, OJ L 201/37 (2002); Directive 2006/24/EC of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC OJ L105/54 (2006).

Net neutrality in law and regulation

Network neutrality is a growing policy controversy[2]. Traffic management techniques used by Internet Service providers (ISPs) affect all Internet content and user rights. To take an example, an access provider that also provides a bundled voice service to its subscribers may degrade the rival voice over internet protocol (VoIP) service of an ISSP/ISP that needs that access to end-users. This degradation may form a breach of network neutrality. Note that it is access providers that are most likely to intercept communications by users to breach net neutrality, and become subject to criminal penalty for interception of communications, a subject to which we return in considering the PHORM and Comcast cases. (The term 'ISP' has different legal meaning in different contexts, though it is used much more often than more legally specific terms for access providers in both Europe[3] and the United States[4]. General

2 See Marsden, C. (2013) *Network Neutrality: A Research Guide* Chapter 16 in 'Handbook Of Internet Research', I. Brown, ed., Edward Elgar, at SSRN: http://ssrn.com/abstract=1853648

[3] In Europe, a provider of internet access is an Electronic Communications Network Provider (ECNP), whereas a provider of content and services is termed an Information Society Service Provider (ISSP) under the Electronic Commerce Directive (ECD). Directive 2000/31/EC, Art 2(a) (OJ L 178/1, 17 July 2000), reiterating Art 1(2) of Directive 98/34/EC (OJ L 204/37, 21 July 1998) as amended by Art 1(2)(a) and Annex V of Directive 98/48/EC (OJ/L 217/18, 5 August 1998). See Directive 2010/13/EU, Art 1(a)(i) and Art 2 of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive)(codified version) OJ/L 95/1, 15 April 2010. Under the European Framework Directive (2002/21/EC, OJ L 108/33), Art 2(c) 'electronic communications service' means a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but exclude services providing, or exercising editorial control over, content transmitted using electronic communications networks and services. The definition explicitly excludes ISSPs 'which do not consist wholly or mainly in the conveyance of signals on electronic communications networks'.

[4] In the US, the access provider is an Internet Access Provider (IAP), and the service provider an Online Service Provider (OSP) under the Digital Millennium Copyright Act (DMCA). See Online Copyright Infringement Liability Limitation Act (OCILLA) which amended the 1976 Copyright Act, passed as a part of the 1998 Digital Millennium Copyright Act (DMCA) and referred to as the 'Safe Harbor' (sic) provision because it added Section 512 to Title 17 of the United States Code. Digital Millennium Copyright Act 1998, s 512(k)(1)(A–B): 'an entity offering transmission, routing, or

liability limitations apply to all ISPs, though with some specific applications that only apply to access providers. The distinction is most important, as network neutrality relates to the manner in which access providers employ QoS across their networks, and how this in turn improves or degrades the end-user's experience.)

In the absence of any regulatory oversight, ISPs could use Deep Packet Inspection (DPI) to block some content altogether, if they decide it is not to the benefit of ISPs themselves, copyright holders, parents or the government. ISP blocking is currently widespread in controlling spam email, and in some countries in blocking sexually graphic illegal images, which are both legal and reasonable uses of traffic management.

In 1999, fears of potential foreclosure of Instant Messaging and video led to the first calls for net neutrality on cable networks[5]. As network neutrality extends to all consumer ISP users equally, it may not be subject to competition law assessments of dominance, as abuse of dominance is not necessarily an accurate analysis of the network neutrality problem.[6] Dominance is neither a necessary nor sufficient condition for abuse of the termination monopoly to take place, especially under conditions of misleading advertising and consumer ignorance of abuses perpetrated by their ISP.[7] This paper analyses these legal developments, and in particular the difficulty in assessing reasonable traffic management and illegal (criminal)

---

providing connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received' or 'a provider of online services or network access, or the operator of facilities thereof.' See further distinction lies between access providers classified under Title I and Title II of the Telecommunications Act 193447 USC §201(a) and (b).

5 See Lemley, MA and Lessig, L. (2000) *The End of the end-to-end: preserving the architecture of the internet in the broadband era*, UC Berkeley Public Law Research Paper No 37. See further Marsden, C. (1999) Council of Europe MM-S-PL(1999)012: '*Pluralism in the multi-channel market. Suggestions for regulatory scrutiny*', at S.5.1: http://www.coe.int/t/dghl/standardsetting/media/Doc/MM-S-PL(1999)012_en.asp

6 See Marsden (2010) *Net Neutrality: Towards a Co-regulatory Solution*, Bloomsbury Academic: London at p 1.

7 Some authors question the distinction between degrading and prioritizing altogether, as they find that the latter naturally presupposes the former. See, eg Filomena Chirico, Ilse Van der Haar and Pierre Larouche, 'Network Neutrality in the EU', TILEC Discussion Paper (2007), <http://ssrn.com/abstract=1018326>.

interception of user communications and personal data. It also assesses net neutrality law against the international legal norms for user privacy.

Network neutrality[8] is the latest phase of an eternal argument over control of communications media. The internet was held out by early legal and technical analysts to be special, due to its decentred construction[9]. Dividing net neutrality into its forward-looking positive (or 'heavy' and backward-degrading negative (or 'lite') elements is the first step in unpacking the term, in comprehending that there are two types of problem: charging more for more, and charging the same for less[10]. Abusive discrimination in access to networks is usually characterized in telecoms as a monopoly problem, manifested where one or two ISPs have dominance, typically in the last mile of access for end-users. ISPs can discriminate against all content or against the particular content that they compete with when they are vertically integrated. Conventional US economic arguments are broadly negative to net neutrality, preferring the introduction of tariff-based congestion pricing.[11] Hahn and Wallsten explain that net neutrality[12] 'usually means that broadband service providers charge consumers only once for Internet access, don't favor one content provider over another, and don't charge content providers for sending information over broadband lines to end users.'

European legal implementation of network neutrality principles has been slow, with the European Commission referring much of the detailed work to the Body of European Regulators of Electronic Communications (BEREC)[13]. Netherlands and Slovenian Parliaments

8 See Marsden, supra n.6.

9 The 'Internet' is a network of Autonomous Systems, of which about 40,000 are of a scale that is relevant. See Haddadi, Hamed et al (2009) *Analysis of the Internet's structural evolution*, Technical Report Number 756 Computer Laboratory UCAM-CL-TR-756 ISSN 1476-2986.

10 I have argued that the real problem lies in the 'middle mile' of interconnection, Marsden supra n.6.

11 See David, Paul (2001) 'The Evolving Accidental Information Super-Highway', 17(2) Oxford Review of Economic Policy pp159–187.

12 Hahn, Robert and Scott Wallsten, (2006) 'The Economics of Net Neutrality' AEI Brookings Joint Center for Regulatory Studies: Washington, DC at <www.aei-brookings.org/publications/abstract.php?pid=1067>.

13 See generally http://berec.europa.eu/eng/about_berec/working_groups/net_neutrality_expert_working_group_/282-net-neutrality-expert-working-group

passed laws in 2012, prompting a proposed new European law in 2013. I now briefly summarize the legal debate to date.

While issues about potential discrimination by ISPs have been current since at least 1999, the term 'network (net) neutrality' was coined by Tim Wu in 2003.[14] FCC Chair Michael Powell declared in 2004: "I challenge the broadband network industry to preserve the following Internet Freedoms: Freedom to Access Content; Freedom to Use Applications; Freedom to Attach Personal Devices; Freedom to Obtain Service Plan Information."[15] The 'Four Freedoms' were applied in the *Internet Policy Statement*,[16] *Madison River*[17], the AT&T and Verizon mergers, and the *Comcast* action. In *Madison River*, the vertical integration of the ISP with its voice telephone service meant it had obvious incentives to block its competitor, and the practice was intended to degrade its customers' internet access. It was an example of negative network neutrality: customers signed up for broadband service with the ISP, but it chose to degrade that service in the interest of preserving its monopoly in telephone service. Madison River is a small consumer ISP, not a large behemoth national carrier. The merger of AT&T and BellSouth undertook various commitments not to block other companies' applications directed to their users.[18] FCC made a 2008 Order against Comcast, a major cable broadband ISP.[19] Comcast deposition to the FCC stated that it began throttling P2P filesharing application BitTorrent in May 2005–2006, slowed by use of Sandvine technology. The FCC ruling was against Comcast's attempts to stop P2P by using DPI to identify Peer-to-peer (P2P) users and sending them phantom RST reset packets[20].

---

14 Wu, T (2003) 'Network Neutrality, broadband discrimination', 2 Journal on Telecommunications and High-Tech Law 141.

15 Powell (2004) Four Freedoms speech, at <http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-243556A1.pdf>.

16 FCC (2005) Internet Policy Statement 05-151.

17 FCC (2005) *Madison River Communications, LLC*, Order, DA 05-543, 20 FCC Rcd 4295

18 FCC (2007) *In AT&T Inc and BellSouth Corp* Application for Transfer of Control, 22 FCC Rcd 5562.

19 FCC (2008) Memorandum Opinion and Order, 23 FCC Rcd 13028 ('ComcastOrder').

20 See Karpinski, R, Comcast's Congestion Catch22, 23 January 2009, at <http://telephonyonline.com/residential_services/news/comcast-congestion-0123/index1.html>

American Recovery and Reinvestment Act 2009 included a broadband open access stimulus[21] extending broadband into under-served areas, with open access and net neutrality provisions built into the grants.[22] FCC made a 2010 Order,[23] currently challenged before the courts in 2013. FCC in 2011-13 refused several times to intervene in interconnection and peering disputes that were claimed by CDNs to unreasonably impair traffic contrary to the controversial and *sub judice* net neutrality rules[24]. Implementation of the technical means for measuring reasonable traffic management are tested in a self-regulatory forum, the Broadband Industry Technical Advisory Group (BITAG). Its specific duties include that to offer 'safe harbor' opinions on traffic management practices by parties making formal reference for an advisory technical opinion.[25]

European Legislation and Regulation of Network Neutrality

European law upholds transparency on a mandatory basis, and minimum Quality of Service on a voluntary basis, under provisions in the 2009 electronic communications framework. Both the 28 Member States, European Economic Area members and the 47 members of the Council of Europe must also conform to the human rights law of the European Convention on Human Rights, which protects users' freedom of expression in Article 10 and their privacy and respect for family life in Article 8[26]. This is supplemented in the European Union by data protection legal instruments which are implemented using both the decisions of national and

[21] American Recovery and Reinvestment Act 2009, at Division B, Title VII, Section 6001(k)2, A, D, E.

[22] FCC (2009) *Report on a Rural Broadband Strategy*, 22 May 2009, at pp 15–17 especially footnotes 62–63.

[23] FCC (2010) *Report and Order Preserving the Open Internet*, 25 FCC Rcd 17905.

[24] Frieden, Rob (2012) Rationales for and Against Regulatory Involvement in Resolving Internet Interconnection Disputes 14 Yale J.L. & Tech 266 at: http://yjolt.org/sites/default/files/FriedenFinal.pdf

[25] Broadband Industry Technical Advisory Group (2011) *By-laws of Broadband Industry Technical Advisory Group* S. 7.1

[26] See Koops, Bert-Jaap and Sluijs, Jasper P. (2012) *Network Neutrality and Privacy According to Art. 8 ECHR*, European Journal of Law and Technology 2(3); at http://dx.doi.org/10.2139/ssrn.1920734; Sluijs, Jasper P. (2012) *From Competition to Freedom of Expression: Introducing Art. 10 ECHR in the European Network Neutrality Debate*, Human Rights Law Review 12(3) at http://dx.doi.org/10.2139/ssrn.1927814

European courts[27], and taking account of the advice of the group of European Union privacy commissioners[28]. Over 2007–8, the volume of regulatory reform proposals in the USA, Japan, Canada, and Norway had grown along with consumer outrage at ISP malpractice and misleading advertising, notably over advertisements for maximum speeds and 'reasonable terms of usage'—which meant capacity constraints on a monthly basis, some of these on mobile as low as 100MB download totals.[29] The concerns were about ISPs discriminating against content they dislike, or in favour of affiliated content.[30]

European law provided the framework for ISP Quality of Service (QoS) to be regulated by National Regulatory Authorities (NRAs) in the 2009 revisions to the 2002 Electronic Communications Services (ECS) package.[31] The European Commission noted the US debate in its initial explanation of its reasons to review the previous raft of 2002 Directives[32]. Net neutrality became a significant issue, in the European Parliament First Reading of the 2009 telecoms package, in May 2009. Amendments on consumer transparency and network

[27] See Case C-461/10: *Bonnier Audio AB and others v Perfect Communication Sweden* AB, OJ C 317, 20/11/2010 P. 0024—0024 final judgment 19 April 2012 at http://curia.europa.eu/juris/document/document.jsf?doclang=EN&text=&pageIndex=0&mode=DOC&docid=121743&cid=848081.

[28] Marsden C. [2012] *Regulating Intermediary Liability and Network Neutrality*, Chapter 15, pp701-750 in 'Telecommunications Law and Regulation' (Oxford, 4th edition)

[29] Leading to a significant emphasis in SEC(2007) 1472 *Commission Staff Working Document: Impact Assessment* at 90–102.

[30] See Jasper P Sluijs, Florian Schuett and Bastian Henze, Transparency regulation in broadband markets: Lessons from experimental research, (2011) 35 Telecommunications Policy 592–602 for an experimental analysis of transparency regulation in broadband.

[31] See Directive 2009/140/EC (OJ L 337/37 18 December 2009); Directive 2009/136/EC (OJ L 337/11 18 December 2009).

[32] COM (2006) 334 *Review of the EU Regulatory Framework for electronic communications networks and services*, Brussels, 29 June 2006 at section 6.2–6.4.

openness were offered to the Parliament in the Conciliation process, collated in the European Commission 'Declaration on Net Neutrality',[33] appended to Directive 2009/140/EC:

> 'The Commission attaches high importance to preserving the open and neutral character of the Internet, taking full account of the will of the co-legislators now to enshrine net neutrality as a policy objective and regulatory principle to be promoted by [NRAs] (Article 8(4)(g) Framework Directive), alongside the strengthening of related transparency requirements[34] and the creation of safeguard powers for [NRAs] to prevent the degradation of services and the hindering or slowing down of traffic over public networks (Article 22(3) Universal Service Directive)[35].'

The new laws which became effective in Member States in May 2011[36] state that Member States may take action to ensure particular content is not discriminated against directly (by blocking or slowing it), or indirectly (by speeding up services only for content affiliated with the ISP). The Commission added that it will introduce 'a particular focus on how the 'net freedoms' of European citizens are being safeguarded in its annual Progress Report to the European Parliament and the Council'. Legal provisions in the Directives permit greater 'symmetric' regulation on all operators, not simply dominant actors. A new wider scope for solving interoperability disputes may be used in future.

This Declaration, and the more legally relevant Directive clauses, rely heavily on the implementation at national level and proactive monitoring by the Commission itself, together with national courts, and privacy regulators where content discrimination contains traffic management practices which collate personal subscriber data. Traffic management, consistent with Article 8 and 10(2) ECHR, may only in limited circumstances be acceptable and should

---

33 European Commission (2009) *Declaration on Net Neutrality*, appended to Directive 2009/140/EC, O J L 337/37 at p 69, 18 December 2009 at <http://eur-lex.europa.eu/LexUriServ/LexUriServdo?uri=OJ:L:2009:337:0037:0069:EN:PDF>

34 Articles 20(1)(b) and 21(3)(c) and (d) Universal Service Directive

35 Article 22(3) of the Universal Service Directive, stipulates that regulatory authorities should be able to set minimum quality-of-service standards: 'In order to prevent the degradation of service and the hindering or slowing down of traffic over networks, Member States shall ensure that [NRAs] are able to set minimum quality of service requirements'.

36 Directive 2009/136/EC (the 'Citizens Rights Directive') and Directive 2009/140/EC (the 'Better Regulation Directive') both of 25 November 2009, which must be implemented within 18 months.

be regulated by information commissioners as well as by telecoms regulators[37]. The introduction of network neutrality rules into European law was under the rubric of consumer information safeguards and privacy regulation, not competition policy. The European Data Protection Supervisor has recently expressed its privacy concerns in this area.[38] European Commissioner Reding stated prior to the vote on the new telecoms law[39]:

> "The new rules recognize explicitly that Internet access is a fundamental right such as the freedom of expression and the freedom to access information. The rules therefore provide that any measures taken regarding access to, or use of, services and applications must respect the fundamental rights and freedoms of natural persons, including the right to privacy, freedom of expression and access to information and education as well as due process.

The Council of Europe also issued soft law instruments to guide member states in observance of citizens' rights to privacy and free expression[40].

Reasonable Network Management and Regulatory Consultation

The phrase 'reasonable' in connection with ISP traffic management was first included in footnote 15 to the FCC *Internet Policy Statement*[41]. It was designed to ensure that an ISP must demonstrate both that its management purpose is reasonable and that it has used a minimally invasive means of so doing, in language borrowed from the US courts' approach to freedom of speech. It was thus a tough two-part test that the ISP "practice should further a critically important interest and be narrowly tailored to serve that interest."[42] The FCC expanded on this

37 BoR (10) 42 at p 20.

38 European Data Protection Supervisor (2011) Opinion on net neutrality, traffic management and the protection of privacy and personal data, at <http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-10-07_Net_neutrality_EN.pdf>

39 Reding (2009 undated).

40 See Declaration of the Committee of Ministers on network neutrality adopted 29/9/2010: 1094th meeting of the Ministers' Deputies, a soft law instrument to guide member states in the application of net neutrality rules: aspirations of Articles 6/8/10 of the Convention

41 20 FCC Rcd 14986 (2005) ("Internet Policy Statement")

42 Formal Complaint of Free Press and Public Knowledge Against Comcast Corp. for Secretly Degrading Peer-to-Peer Applications; Broadband Industry Practices; Petition of Free Press et al. for

principle to explain exceptions in 2009: ISPs "may employ generally accepted technical measures to provide acceptable service levels to all customers, such as caching and application-neutral bandwidth allocation, as well as measures to address spam, denial of service attacks, illegal content, and other harmful activities"[43]. Note that this means ISPs can deploy to prevent behavioural advertising by third parties, but not to enhance that advertising, as BT/PHORM implemented in the UK (see later section). Denial of Service (DoS) is a technique to damage websites via a flood of traffic causing congestion.

The FCC makes clear that it is intended to prohibit all non-critical traffic management, though noting that technologies will differ in criticality as between co-axial cable, copper telecoms, fibre broadband and wireless systems: "We believe that a bright-line rule against discrimination, subject to reasonable network management and enumerated exceptions, may better fit the unique characteristics of the Internet" than a less clear rule. It was however less tightly drawn than the 2005 language of 'narrowly drawn' and 'critically important' which it described as "unnecessarily restrictive".

The question is what 'harmful activities' involves, related to what is not 'generally accepted technical measures'. This must be subject to change over time, such that industry can agree on particular measures commonly used. Harmful measures will depend on both the network's robustness and the particular measure, with DoS an obvious example of harmful activity. It will thus be legal for an ISP to intervene to stop a flood of DoS traffic (though such activities will change over time: a million simultaneous requests in 2003 on dial-up would cripple an ISP, in 2013 on broadband that is less likely).Commissioner Copps stated that: "What constitutes reasonable network management in a 768 Kbps world will likely be different from reasonable network management in a 50 or 100 Mbps world"[44].

The Canadian regulator in 2009 also defined reasonable traffic management, explaining that the ISP must prove that any proven discrimination is reasonable by only on a case-by-case basis: "the burden of establishing that any such discrimination, preference, or disadvantage is

---

Declaratory Ruling that Degrading an Internet Application Violates the FCC's Internet Policy Statement and Does Not Meet an Exception for "Reasonable Network Management," Memorandum Opinion and Order, 23 FCC Rcd 13028 (released Aug. 20, 2008) ("Comcast Order"), at p47.

43 Broadband Initiatives Program; Broadband Technology Opportunities Program Notice, 74 Fed. Reg. 33104, 33110–11 (July 9, 2009) (Broadband NOFA).

44 Copps, Michael, quoted in FCC (2009) 09-93 at pp.94-95.

not unjust, undue, or unreasonable is on the primary ISP"[45]. It permits usage based billing (UBB), also known as data caps, as they are justified and discriminate based on user preferences[46]. 147 consumer complaints about UBB, gaming and MMORPGs followed in 2009-2012, and the acting chair of CRTC stated that: "[largest ISPs Bell and] Rogers ...eventually announced that it would stop throttling traffic by the end of 2012... Both companies indicated that new investments in network capacity were helping them put an end to the practice." Clearly with greater capacity, such gamer throttling would become more unreasonable. In 2013, CRTC has fallen silent on the traffic management issue, either demonstrating that Bell and Rogers have implemented its rulings fully by increased capacity or that more enforcement lies ahead.

The European regulators group BEREC has also analysed 'reasonable' and concluded it is:

> "more reasonable to simply throttle P2P applications in times of congestion to the benefit of, for example, time-sensitive applications... Those practices would be considered more reasonable than totally blocking special applications because they induce fewer side effects."[47]

The European Commission closed its consultation on network neutrality implementation on 30 September 2010[48]. BEREC issued their response to the EC consultation in September 2010. They concluded that mobile should be subject to the net neutrality provisions, listing some breaches of neutrality: "there are not enough arguments to support having a different approach on network neutrality in the fixed and mobile networks. And especially future-oriented approach for network neutrality should not include differentiation between different types of

[45] CRTC (2009) Review of the Internet traffic management practices of Internet service providers, Telecom Regulatory Policy CRTC 2009-657, File No. 8646-C12-200815400 (Oct. 21, 2009), available at http://crtc.gc.ca/eng/archive/2009/2009-657.htm

[46] CRTC (2011) Telecom Decision CRTC 2011-44, Ottawa, 25 January 2011: Usage-based billing for Gateway Access Services and third-party Internet access services, File number: 8661-C12-201015975

[47] BEREC (2012) Differentiation practices and related competition issues in the scope of net neutrality, BoR (12) 132 at p.56 paragraph 265.

48<http://ec.europa.eu/information_society/policy/ecomm/library/public_consult/net_neutrality/index_en.htm>

the networks."[49] BEREC in December 2011 published its guidelines on transparency and Quality of Service[50]. On transparency, 'BEREC states that probably no single method will be sufficient'[51] and points out the limited role of NRAs. Governments' consumer and information commission bodies are likely to also play a key role.

The response of NRAs to the new powers in the 2009 Directives varied widely, though by the end of 2012, three member states had introduced net neutrality laws: Finland, Netherlands and Slovenia. The new 2012 Netherlands and Slovenian laws prohibit traffic management that discriminates with few exceptions[52]. In Netherlands, these are:

a) "[a] to minimize the effects of congestion, whereby equal types of traffic should be treated equally;
b) [b] to preserve the integrity and security of the network and service of the provider in question or the terminal of the end-user"
c) plus to stop spam and enforce legal requirements[53].

In Slovenia they are:

[49] BoR (10) 42 BEREC Response to the European Commission's consultation on the open Internet and net neutrality in Europe, p3 at <http://www.erg.eu.int/doc/berec/bor_10_42.pdf>.

[50] Documents BoR 53(11) Quality of Service and BoR 67(11) Transparency, at <http://erg.eu.int/documents/berec_docs/index_en.htm>.

[51] See BoR 67 [11] at p 5.

[52] Unofficial translations from Netherlands Article 7.4a Telecommunications Act, 14 June 2011; Slovenian Law on Electronic Communications, No. 003-02-10/2012-32 Article 203, 20 December 2012. Netherlands Telecommunications Act 2012, translated by the Dutch government at http://www.government.nl/files/documents-and-publications/notes/2012/06/07/dutch-telecommunications-act/tel-com-act-en-versie-nieuw.pdf (not official legal translation). Slovenian Law on Electronic Communications, No. 003-02-10/2012-32, 20 December 2012, http://www.uradni-list.si/1/content?id=111442 Helpful translation of key aspects at https://wlan-si.net/en/blog/2013/06/16/net-neutrality-in-slovenia/

[53] Netherlands regulators were not required to implement net neutrality until summer 2013, a deadline delayed by the need for the Ministry to issue secondary legislation and guidance to the regulator on the form that such implementation should take. It is therefore too soon to draw firm conclusions about the efficacy of the Netherlands law.

1. “applying necessary technical measures in order to ensure a smooth use of the Internet network (e.g. to avoid traffic congestion),
2. applying necessary precautions to preserve the integrity and security of networks”
3. plus spam/legal requirements.

Slovenia’s law makes clear that these must be temporary fixes: “proportionate, non-discriminatory and time limited and applied only to the extent necessary.” They both prohibit ‘limited Internet offers’ which block certain traffic, for instance by mobile providers, as the Dutch law commands ISPs: “do not make the price of the rates for internet access services dependent on the services and applications which are offered or used via these services.” The new proposed European net neutrality regulation also adopts similar language on what is ‘reasonable’.

On 11 September 2013, the European Commission adopted a proposed regulation that would substantially impact and harmonise net neutrality provision, allowing priority ‘specialized services’ and generally preventing ISPs from blocking or throttling third party content[54]. The proposal was extensively strengthened from a July 2013 draft, and its essential items are in part positive and in part negative for net neutrality policy. Article 23(5) enforces net neutrality ‘lite’, thus conforming to the Netherlands and Slovenian laws: “Within the limits of any contractually agreed data volumes or speeds for internet access services, providers of internet access services shall not restrict the freedoms provided for in paragraph 1 by blocking, slowing down, degrading or discriminating against specific content, applications or services, or specific classes thereof, except in cases where it is necessary to apply reasonable traffic management measures.” These are defined as “transparent, non-discriminatory, proportionate and necessary to: a) implement a legislative provision or a court order, or prevent or impede serious crimes; b) preserve the integrity and security of the network, services provided via this network, and the end-users' terminals; c) prevent the transmission of unsolicited communications to end-users who have given their prior consent to such restrictive measures; d) minimise the effects of temporary or exceptional network congestion provided that equivalent types of traffic are treated equally.”

54COM(2013) 627 final 2013/0309 (COD) Proposal for a Regulation laying down measures concerning the European single market for electronic communications and to achieve a Connected Continent

It continues "Reasonable traffic management shall only entail processing of data that is necessary and proportionate to achieve the purposes set out in this paragraph." Articles 21-24 then explain users' contractual remedies to switch providers who discriminate unreasonably.

As with all telecoms licensing conditions, net neutrality depends on the physical capacity available, and it may be that de facto exclusivity results in some services for a limited time period as capacity upgrades are developed.[55] Interoperability requirements can form a basis for action where an ISP blocks an application.[56] Dominance is neither a necessary nor sufficient condition for abuse of the termination monopoly to take place, especially under conditions of misleading advertising and consumer ignorance of abuses perpetrated by their ISP.[57] 2009 Directives permit greater 'symmetric' regulation on all operators, not only dominant actors. Access Directive, Art 5(1) states NRAs are able to impose obligations "on undertakings that control access to end-users to make their services interoperable". Article 20 of the Framework Directive provides for the resolution of disputes between ISPs and content providers. The potential outcome of disputes based on the transparency obligations can provide a 'credible threat' for undertakings to behave in line with those obligations, since violation may trigger the imposition of minimum quality requirements on an undertaking, in line with Article 22(3) Universal Service Directive.

[55] See GN Docket No 09-191 Broadband Industry Practices WC Docket No 07-52 'In the Matter of Further Inquiry into Two Under-Developed Issues in the Open Internet Proceeding Preserving the Open Internet', and Andersen et al, Joint Reply Comments Of Various Advocates For The Open Internet, 4 November 2010, Comments on Advancing Open Internet Policy Through Analysis Distinguishing Open Internet from Specialized Network Services.

[56] See Marsden (2010) Net Neutrality, at p 1.

[57] Some authors question the distinction between degrading and prioritizing altogether, as they find that the latter naturally presupposes the former. See, eg Filomena Chirico, Ilse Van der Haar and Pierre Larouche, 'Network Neutrality in the EU', TILEC Discussion Paper (2007), <http://ssrn.com/abstract=1018326>.

Introduction to technologies to intercept communications

ISPs have many reasons to manage traffic:

1. It is required for government law enforcement and security purposes.[58]
2. Network providers already provide filters against the more obvious types of 'spam' – unsolicited commercial communications.
3. Network providers cooperate with national security agencies in tracing potential terrorist activities on the Internet.
4. Network providers can trace non-encrypted Voice over IP (e.g. Skype) and block these packets.
5. Network providers are increasingly adopting specialized services for their networks in order to prevent users from over-straining the network at times of peak usage, and charge content owners for value-added high-volume services such as video files.

These new developments allow network providers to block file transfers, or to charge the users a carriage fee for sending large files. This is generally termed as a 'walled garden' to denote the isolation of content on the network from other content on the wider Internet. ISPs are using 'black boxes' in their networks to look inside the packets that carry communications, and to examine their content, in a change to DPI which has very serious regulatory implications.

The range of network and information security requirements at European level, which must then be implemented as national law in the European countries, imposes costs on the network. They are in addition to existing costs for spam filtering, protection against distributed denial of service (DDOS) attacks, phishing and other 'malware' that ISPs typically invest in to protect their subscribers from the worst excesses of IP traffic. Security is a growing problem as dependence on broadband (as a key element of the critical information infrastructure) grows and as the Internet moves towards pervasive computing, and the 'Network of Things'. There is an escalating arms race as criminal behaviour become more sophisticated.[59] The objectives and requirements are also changing on both sides: on the attacking side, the evolution from unauthorized access to data corruption, exposure or access denial; on the defending side, the

[58] See generally Bendrath (2009) 'Deep Packet Inspection Reading List', at http://bendrath.blogspot.com/2009/03/deep-packet-inspection-reading-list-and.html and the Syracuse DPI project papers at http://dpi.ischool.syr.edu/Papers.html

[59] See Brown, Edwards and Marsden (2006).

change in data collection, storage, processing locations (centralized or not), data exchange and transfer of liability among buyers, sellers and ISPs. Loss of Internet privacy, openness and end-to-end connectivity is one potential casualty of security concerns.

ISPs can either throttle users by cutting off their connections at peak times or once they have exceeded monthly quotas, or try looking inside the packets to see whether they are P2P or not. The latter becomes a very dangerous business to engage in because as we will see, governments are not only encouraging ISPs to look, they are actually subsidizing the DPI equipment to do so – and this sometimes in breach of both European and UK privacy and interception laws (the latter intended to prevent private spying, even if encouraged by government policy). Felten worried that regulators are used to standards bodies and classes of companies, when, for instance, BitTorrent is a protocol, not a company or a single standard.[60] Blocking BitTorrent or P2P more widely will eventually fail because the protocol designers will route around via encryption or other techniques.

Regulating Deep Packet Inspection and Interception of Traffic

Blocking and other forms of traffic shaping are controversial because, under current network management tools, it is a blunt tool. For instance, all P2P traffic using a certain protocol may be blocked. P2P can respond by encrypting its traffic or otherwise spoofing, but this creates an 'arms race' much like that found in security software responses to the threat of breaches. Future networks may try to cap P2P more effectively, which can itself lead to an 'arms race' between encrypted P2P content and attempts by ISPs to detect P2P traffic using DPI.[61]

ISPs have limited liability where they act as 'mere conduits' but not where they have constructive or actual knowledge of illegal content. Their traffic is thus something of a Pandora's box – if they look inside using DPI, all liabilities flow to them, from child pornography to terrorism to copyright breaches to libel to privacy breaches. The Canadian Privacy Commissioner's submission to the CRTC proceedings on traffic management practices, expressed concern that:

---

[60]http://www.freedom-to-tinker.com/blog/felten/comcast-and-bittorrent-why-you-cant-negotiate-protocol

[61] In May 2009, uTorrent announced a future protocol change to UDP, which indicates that [a] TCP may not be the main P2P traffic protocol; [b] that will annoy those who use TCP for YouTube etc.; [c] it will annoy ISPs; [d] so more discriminatory actions can be expected. It is the arms race continuing at higher level, as filtering UDP is a new departure for many consumer ISPs. See http://www.theregister.co.uk/2008/12/01/richard_bennett_utorrent_udp/

> "DPI can look into the content of the message sent over the Internet. To use a real-world example, using DPI is akin to a third part opening an envelope sent by surface mail, and reading its contents before it reaches its intended destination...it is not clear that examination of content is necessary for network management and may constitute an unreasonable invasion of an individual's privacy."[62]

Cooper analysed the choices of whether to introduce DPI equipment into ISP networks, restricting traffic as an alternative to increasing capacity, with the consequent decision to invest in DPI and other management servers instead of greater bandwidth (Cooper 2013: 109-120). She points out that US cable companies at the time of the *Internet Policy Statement* in 2005 hoped that the burden of proof on 'reasonable' techniques would fall on complainants, with the presumption that ISPs were acting reasonably. That has not been the case in the US, or Canada. It is for the ISP to demonstrate that its use of technologies such as DPI is reasonable, a test that Comcast failed in its deployment of Sandvine DPI. The presumption that DPI may be unreasonable based on Comcast has been profound for US ISPs. Cooper concluded that while marketing directors still encouraged DPI use and were likely to authorise such expenditure in order to better target services at customers, regulatory departments discouraged its use and had the reverse effect on engineering choices to deploy[63]. More research is needed into the causes for such differences, but it is very likely that a lack of knowledge and education about the criminal offences for breaching data protection law and intercepting traffic amongst marketing departments of ISPs may account in part for their cavalier approach to installing DPI equipment to monitor customers. By contrast, engineers' typical preference in Cooper's study was to increase bandwidth rather than manage traffic more minutely.

---

[62] Privacy Commissioner of Canada (2009) Letter to Robert A. Morin, Secretary General, Canadian Radiotelevision and Telecommunications Commission, Re: Telecom Public Notice CRTC 2008-19 – Review of the Internet traffic management practices of Internet service providers, Canadian Radio-television and Telecommunications Commission. February 18, 2009, at http://www.crtc.gc.ca/public/partvii/2008/8646/c12_200815400/1027577.PDF at paragraphs 13, 32.

[63] Cooper, Alissa (2013) How Regulation and Competition Influence Discrimination in Broadband Traffic Management: A Comparative Study of Net Neutrality in the United States and the United Kingdom, Thesis submitted for the degree of DPhil, University of Oxford, September 2013. PP.122-132. Cooper interviewed 70 elite decision-makers in ISPs, regulators and content companies in the period 2011-12, the broadest sample known.

It is also notable from Cooper's study that foreign content providers were unable to influence domestic ISPs' traffic management practices, so that MMORPG (massively multiplayer online role playing game) providers such as *World of Warcraft* were often significantly impeded in delivering their service because of unreasonable traffic management, a problem significantly worse in the UK where DPI and other traffic management techniques were used much more invasively than in the US[64]. Cooper's conclusions have particularly negative outcomes for those free-to-play MMORPGs such as are commonly found in South Korea, as there would be no likelihood that such MMORPG creators could negotiate or even complain successfully when foreign ISPs block their world.

Cooper establishes that different countries' regulators view of litigation and reputation is likely to colour their view of what is 'reasonable' and how strict their interpretation of that provision may be. Thus the US regulators are not scared of litigation or enforcement and so are likely to prosecute cases more strictly, whereas the lawyer-light UK regulator is committed to alternatives to enforcement and is likely to prosecute only as a last resort. UK regulators, notably the Information Commissioner, has shown no willingness to prosecute even in the infamous case of PHORM/BT's illegal DPI trial (see Annex I), whereas the US regulator Federal Trade Commissioner successfully brought strict settlements with multi-million dollar fines against social networks misusing their subscribers' data, notably Google and Facebook in August 2012[65]. In the Google case, the FTC declared their first:

> "FTC settlement order [that] has required a company to implement a comprehensive privacy program to protect the privacy of consumers' information. In addition, this is the first time the FTC has alleged violations of the substantive privacy requirements of the U.S.-EU Safe Harbor[66] Framework"[67].

[64] Cooper 2013: 200-204

[65] Lardinois Frederic (2012) Facebook And FTC Settle Privacy Charges — No Fine, But 20 Years Of Privacy Audits, Tech Crunch, August 10th, http://techcrunch.com/2012/08/10/facebook-ftc-settlement-12/

[66] Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, Official Journal of the European Communities, 25 August 2000, L-215, 7-47. See also www.export.gov/safeharbor

The likelihood of criminal or civil prosecution for breaches of net neutrality and other abuses of trust with ISP users are thus conditioned by the regulators' willingness to actually enforce regulation. In the US this is clearly the case, in Europe very much less so. This is despite the US corporate need to satisfy European regulators that the theoretically weaker US personal data privacy rules can satisfy European law under existing Directive 95/46/EC. As has become apparent in the wake of the 2013 Snowden revelations, US companies are both constantly in breach of the safe harbour themselves for corporate policy reasons, and obliged by US law enforcement and espionage to mistreat personal data of citizens of other countries including Europeans and Koreans. Belatedly this has become a significant issue in the renegotiation of the 'Safe Harbor' and the proposed European Data Protection Regulation[68] in 2013.

Proposed European Data Protection Regulation 2014 and ongoing Snowden inquiries

European laws are meant to protect citizens' privacy and liberty. Directive 95/46/EC[69] is the main law giving member states responsibilities and citizens data protection rights against corporate actors. This European law sets a high standard for data protection, arguably higher than that in the United States. National data protection agencies have a permanent joint working group (the Article 29 Working Group) and are required to implement the Directive as uniformly as possible, tasks including cooperating with each other and the European Commission in a transparent manner to ensure the development of consistent regulatory practice, contributing to a high level of protection of personal data and privacy and ensuring that the integrity and security of public communications networks are maintained.[70]. The European institutions are also required by law to consider the Opinions issued on prospective legislation by the European Data Protection Supervisor, established in 2002. Directive 2002/58/EC (the 'Electronic Privacy Directive')[71] includes measures intended to prevent spam,

---

[67] At the time of finalizing this report, the FTC and FCC websites had been mothballed due to the ongoing US federal shutdown. For a mirror copy, see http://www.netcompetition.org/antitrust/ftc-google-privacy-settlement-takeaways#sthash.TvMNpXvP.dpuf

[68] European Commission (2012) Consultation on the Commission's comprehensive approach on personal data protection in the European Union", 4 November 2012, available at http://ec.europa.eu/justice/news/consulting_public/news_consulting_0006_en.htm

69 Directive 95/46/EC.

70 Directive 2002/21/EC.

71 Directive 2002/58/EC.

supplemented by a 2004 Communication[72] on spam.[73] The critical test in both 2002/58/EC and 1995/46/EC is that subscribers have to opt for arrangements that may otherwise infringe their personal privacy, and that sensitive data must not be passed to third parties unless authorized and anonymized.

The new European comprehensive data protection law will amend 2002/58/EC and replace and repeal 1995/46/EC. It is likely to reach the plenary sitting of the European Parliament for a full vote in March 2014[74]. It is currently being considered in Committee and by the Council of Ministers' groups of national experts, and has become very complex as there are thousands of amendments to be considered[75]. The draft Regulation (COM/12/11) in particular contains Sections 42-43 relating to transfer of data outside the European Union, insisting on Binding Corporate Rules (BCR) for such transfers to take place subject to enforcement by national data protection regulators (NDPRs)[76].

One area in which European regulators have been forced to investigate potential interception, very much against net neutrality principles, is that of illegal surveillance of ISP users perpetrated by agencies in the 'five eyes' multinational espionage coalition[77]. Note that though nation-states

72 Communications from the Commission, and Resolutions of the Council are not European legislation and therefore non-binding on member states but have important 'signaling' effects on member states and companies, and therefore are termed 'soft law'.

73 COM/2004/0028.

74 For current progress on the matter, numbered 2012/0011(COD), see http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2012/0011(COD)#tab-0

75 For European Parliament Committee progress, see http://www.europarl.europa.eu/RegistreWeb/search/simple.htm?language=EN&reference=LIBE%2F7%2F08739&relName=DOSSIER&currentPage=2

76 COM (2012) 11 final Draft Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). COM/2012/09 final Safeguarding Privacy in a Connected World: A European Data Protection Framework for the 21st Century. See also IP/12/46 (2012) Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses, 25 January 2012 at http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en

77 Campbell, Duncan (1999) The state of the art in communications Intelligence (COMINT) of automated processing for intelligence purposes of intercepted broadband multi-language leased or

funded these activities, they were carried out with the more or less willing cooperation of Internet companies including ISPs acting against their own users' interests in net neutrality. Illegal as well as legal interception activity by 'Five Eyes' within European, Latin American and other nations was exposed by the whistle-blower Edward Snowden and *The Guardian* newspaper in June-October 2013[78]. 'Five Eyes' (or more formally AUSCANNZUKUS) describes the cooperation between the intelligence (i.e. espionage) agencies of the Anglo-Saxon powers during what in English-speaking countries was called the Cold War between US/allies and Warsaw Pact/allies[79]. United States and United Kingdom, Canada, Australia and New Zealand are formal partners, though other allies have subsidiary and subsequent agreements that permit some level of intelligence sharing[80].

Packet-sniffing schemes such as Carnivore, a system implemented by the Federal Bureau of Investigation that was designed to monitor email and electronic communication, have been active since at least 1997, Carnivore had used a customizable packet sniffer that can monitor all of a target user's Internet traffic.[81] A larger-scale operation was built by various Western governments, called Echelon, which was investigated by the European Parliament in a report released on 5 September 2001.[82] Intelligence agencies' surveillance has vastly increased, as

---

common carrier systems, and its applicability to COMINT targetting and selection, including speech recognition European Parliament Ref.: EP/IV/B/STOA/98/1401

[78] Bowden, Caspar (2013) The US National Security Agency (NSA) surveillance programmes (PRISM) and Foreign Intelligence Surveillance Act (FISA) activities and their impact on EU citizens' fundamental rights, European Parliament Civil Liberties Committee, 24.9.2013.

[79] Richelson, Jeffrey T., Ball, Desmond (1985) The Ties That Bind: Intelligence Cooperation Between the UKUSA Countries. London: Allen & Unwin. ISBN 0-04-327092-1.

[80] The initial formal UK-US agreement was signed in 1947 after the successful conclusion of the Second World war and just prior to the outbreak of the Korean War of 1950-53, with final partner New Zealand joining only in 1980. See AUSCANNZUKUS (2013 undated) History, at http://www.auscannzukus.net/history.html

[81] For a legal perspective on private packet sniffing, see Frieden, Rob (2007) Internet Packet Sniffing and its Impact on the Network Neutrality Debate and the Balance of Power between Intellectual Property Creators and Consumers, Available at SSRN: http://ssrn.com/abstract=995273 or http://dx.doi.org/10.2139/ssrn.995273

[82] See European Parliament (2001) Final Report on the Existence of a Global System for the Interception of Private and Commercial Communications (ECHELON Interception System),

exposed thoroughly by Glenn Greenwald and colleagues at *The Guardian* using evidence supplied by former National Security Agency contractor, Edward Snowden[83]. Echelon was later replaced by US programme PRISM[84] and in 2011 UK-US joint operation Tempora (with sub-programmes called "Mastering the Internet" and "Global Telecoms Exploitation"), which intercepts communications in fibre-optic cables destined for trans-Atlantic transmission[85]. Law in this area is rapidly outflanked by technological capabilities of public and private parties, which has resulted in inquiries in response to the Snowden revelations, notably by the Intelligence and Security Committee:

> "Although we have concluded that GCHQ has not circumvented or attempted to circumvent UK law... We are examining the complex interaction between the Intelligence Services Act, the Human Rights Act and the Regulation of Investigatory Powers Act, and the policies and procedures that underpin them, further. We note that the Interception of Communications Commissioner is also considering this issue."[86]

This press release absolved GCHQ of any illegality, but a proper inquiry led by the Deputy Prime Minister is also following in winter 2013/14.

The Snowden revelations allege illegal interception of ISP traffic, which support earlier European Parliament investigations, has been brought complaints about violations of criminal law to the attention of the European human rights court, and national parliaments and

---

Temporary Committee on the ECHELON Interception System, approved September 5, 2001, Brussels: EP, at http://www.fas.org/irp/program/process/rapport_echelon_en.pdf

[83] For examples, see Borger, Julian (2013) Inquiry into snooping laws as committee clears GCHQ Intelligence and security committee also confirms GCHQ's use of NSA Prism surveillance material for first time, 18 July 2013 at http://www.theguardian.com/world/2013/jul/17/prism-nsa-gchq-review-framework-surveillance

[84] Government code name for a data-collection effort known officially by the SIGAD US-984XN

[85] See Shubber, Kadhim. "A simple guide to GCHQ's internet surveillance programme Tempora". Wired.com, 24 June 2013 at http://www.wired.co.uk/news/archive/2013-06/24/gchq-tempora-101

[86] Intelligence And Security Committee Of Parliament (undated July 2013) Statement on GCHQ's Alleged Interception of Communications under the US PRISM Programme, paragraphs 6-7.

information commissioners[87]. The interception laws of most nation states do not permit ISPs to allow or condone interception by third parties, let alone foreign state agencies. Brown provides a useful summary of such laws in several states, including 'Five Eyes' signatories themselves[88].

Note that the personal data of EU citizens captured by non-EU countries is subject to European law under the 1995 and 2002 legislation as well as the new proposed law[89]. In the next year, there will be profound investigations into the invasion of user traffic streams throughout Europe, with investigations announced in the United Kingdom, Netherlands, Belgium, France, Germany, Luxembourg and many other nations, as well as by the European Parliament. Focus is thus far on foreign spying, but as details emerge of the interception techniques used, more attention must focus on the specific national criminal violations by agents acting on behalf of 'Five Eyes', notably ISPs.

While this type of interception is not classified as net neutrality violation, given that it is carried out under the orders of government and is thus presumed to be for law enforcement, should it be proven unlawful it will amount to interception of user personal data for illegal purposes. Regulators may therefore need to issue instructions to ISPs and others not to cooperate with foreign state agencies and others who instruct them to cooperate with data gathering. In extreme circumstances, that could potentially require ISPs not to interconnect with US and UK-based ISPs, a particularly difficult request with which to conform but one proposed by the Brazilian President in an Internet governance summit she will convene in April 2014[90]. This will also be discussed at the Seoul Conference in Cyberspace 2013[91], following previous events in London (2011) and Budapest (2012).

---

[87] Brown, Ian (2013a) Expert Witness Statement for Big Brother Watch and Others Re: Large-Scale Internet Surveillance by the UK Application No: 58170/13 to the European Court of Human Rights. Available September 27 at SSRN: http://ssrn.com/abstract=2336609

[88] Brown Ian (2013b) Lawful Interception Capability Requirements, in *Computers and Law*, at http://www.scl.org/site.aspx?i=ed32980

[89] Rauhofer, Judith and Caspar Bowden (2013) Protecting Their Own: Fundamental Rights Implications for EU Data Sovereignty in the Cloud, Edinburgh School of Law Research Paper No. 2013/28: Available at SSRN: http://ssrn.com/abstract=2283175 or http://dx.doi.org/10.2139/ssrn.2283175

[90] Agence France-Presse (2013) October 9, 2013 17:31 Brazil to host Internet governance summit next year

[91] See http://www.seoulcyber2013.kr/en/program/speakers_4.html

The Organisation for Economic Cooperation and Development has also recently renewed its privacy guidelines, and referred to the need to ensure that Internet policy conforms to fundamental rights of users[92]. At the 2011 Paris meeting in which the latter declaration was made, the Korean delegation requested that the OECD pay attention to the need for more research and coordinated policy towards net neutrality.

Alleged Criminal Breaches of UK interception of communications related to e-privacy

The continued attempts by ISPs to intercept communications on their own networks are by themselves legal under the law of interception. However, they may not allow others to intercept on their behalf or grant to others the right to intercept for their own purposes. UK law is clear on this point. Interception of communication is subject to the Regulation of Investigatory Powers Act 2000 (RIPA) Section 2(2):

> For the purposes of this Act, but subject to the following provisions of this section, a person intercepts a communication in the course of its transmission by means of a telecommunication system if, and only if, he –
>
> (a) so modifies or interferes with the system, or its operation,
>
> (b) so monitors transmissions made by means of the system, or
>
> (c) so monitors transmissions made by wireless telegraphy to or from apparatus comprised in the system,
>
> as to make some or all of the contents of the communication available, while being transmitted, to a person other than the sender or intended recipient of the communication.

[92] OECD (2013) Recommendation of the Council concerning Guidelines governing the Protection of Privacy

and Transborder Flows of Personal Data (2013) [C(80)58/FINAL, as amended on 11 July 2013 by C(2013)79] at http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf. See also OECD (2007) Recommendation on Cross-Border Co-operation in the Enforcement of Laws Protecting Privacy; OECD (2008) The Seoul Declaration for the Future of the Internet Economy; OECD (2011) Recommendation on Principles for Internet Policy Making at http://www.oecd.org/internet/ieconomy/49258588.pdf. OECD (2013) also referred to European law and the Asia Pacific Economic Cooperation's Cross-Border Privacy Rules System (APEC CBPR).

One element of intercepting is that making available some or all of the contents of the communication to a person other than the sender or intended recipient is not permitted. Whether some of these contents (via the channels) are made available to anyone other than the ISP or a third party, they are *available* to someone other than the sender/recipient. The UK test is strict and requires both parties (sender and receiver) to consent.

The most controversial of all attempts by UK network owners to intercept users' communications without consent were the experiments conducted by the behavioural advertising company Phorm with the UK's largest ISP, BT (and discussions with the next two largest, TalkTalk and Virgin Media[93]). Phorm employs a user-tracking system by which British Telecom and other ISPs intend to target users more effectively than Google. A variant of this technology was first deployed widely in US wireless ISPs.[94] Phorm operated a behavioural advertising system called WebWise, intending to offer its ISP and website clients a more accurate tracking of customers' Internet use, in order to more closely target advertising and other marketing via that data.

Phorm used DPI to take a copy of ISP subscribers' Web browsing, in order to insert targeted advertising. The original Phorm system trials by BT in 2006 and 2007 did not inform users or ask for their permission.[95] The government department responsible for interception of electronic communications was aware of, and tried to provide helpful regulatory guidance on, the trials and the behavioural advertising system. It emerged in April 2009 that the department, when contacted by Phorm in August 2007, had responded by asking 'If we agree this, and this becomes our position do you think your clients and their prospective partners will be comforted?'[96] It appears that the consultations between the department and Phorm were extensive and amounted to forming a collaborative view of the law, with comments such as 'My personal view accords with yours, that even if it is "interception", which I am doubtful of, it is lawfully authorized under section 3 by virtue of the user's consent obtained in signing up to the ISPs terms and conditions.' In an email dated 22 January 2008, a Home Office official wrote

93 http://www.theregister.co.uk/2009/04/22/virgin_media_phorm_nma/

94 http://energycommerce.house.gov/cmte_mtgs/110-ti-hrg.071708.DeepPacket.shtml

95 Dubious value is given to such permission in BT internal documents, see http://wikileaks.org/wiki/British_Telecom_Phorm_PageSense_External_Validation_report

96 BBC (2009) Home Office 'colluded with Phorm', 28 April at http://news.bbc.co.uk/2/hi/technology/8021661.stm

again to Phorm and said: 'I should be grateful if you would review the attached document, and let me know what you think.' The publication of this history of emails resulted in a debate in the House of Lords in 2009. Baroness Miller stated that[97]:

> The fact the Home Office asks the very company they are worried is actually falling outside the laws whether the draft interpretation of the law is correct is completely bizarre.

As a result of the legal controversy that followed when the trials were made public in early 2008, the ISPs and Phorm itself agreed to insert both notification and consent into any future trial or deployment of the technology, and BT did so for its third trial in December 2008. In legal terms, the system is not just contrary to permissions required in European privacy law under the 1995 and 2002 Directives, but also unlawful interception under the exclusively UK RIPA. In March 2008, the Foundation for Information Policy Research (FIPR) wrote to the Information Commissioner arguing that Phorm's system involved illegal interception contrary to RIPA.[98] Citizens' complaints about the use of behavioural advertising by internet service providers were handled by the UK Information Commissioner's Office (ICO), the UK personal data protection authority and the police forces responsible for investigating cases of unlawful interception of communications. All had failed to adequately investigate the criminal complaints, in part due to ICO's weak powers to fine aberrant providers. The UK's Information Commissioner ruled that a 'technical' breach of the law occurred in BT's 2006-2007 trials, and had strong reservations about the nature of the explanation provided for participating in BT's 2008 trial, but took no action.

Clayton, security expert at Cambridge University, presented a report on the system, to which Phorm responded to ensure technical accuracy.[99] Clayton stated: "Examining the detail makes it crystal clear that our earlier letter came to the right conclusion. Website data is being intercepted. The law of the land forbids this." The illegality stems not from breaching the Data Protection Act directly, but arises from the fact that the system intercepts Internet traffic. BT

97 LINX Public Affairs (2009) https://publicaffairs.linx.net/news/?p=993

98 See FIPR (2008) Continuing concerns about Phorm, 6 April at http://www.fipr.org/press/080406phorm.html

99 Clayton, R. (2008) The Phorm\Webwise System, at http://www.cl.cam.ac.uk/~rnc1/080404phorm.pdf and later version http://www.cl.cam.ac.uk/~rnc1/080518-phorm.pdf

appeared to ignore the fact that they can only legalize their activity by getting express permission not just from their customers, but also from the Web hosts whose pages they intercept, and from the third parties who communicate with their customers through Web-based email, forums or social-networking sites.

In response to UK citizens' complaints that ICO was failing to prosecute Phorm and BT for breaching the Directive in not asking consent for the original trial, the European Commission formally asked the UK government to explain why action had not been taken. The European Commission is tasked with monitoring member states' implementation of European law, in this case Directive 2002/21/EC, the Electronic Privacy Directive (EPD)[100]. The EU Data Protection Directive (DPD) of 1995 specifies that user consent must be 'freely given specific and informed', a formula repeated on the EPD[101]. The critical test in both EPD and DPD is that subscribers have to opt for arrangements that may otherwise infringe their personal privacy, and that sensitive data must not be passed to third parties unless authorized and anonymized. The EPD requires EU Member States to ensure confidentiality of the communications and related traffic data by prohibiting unlawful interception and surveillance unless the users concerned have consented to this[102]. Article 24 DPD requires Member States to establish appropriate sanctions in case of infringements. Article 28 requires that independent authorities must be charged with supervising implementation. These DPD provisions also apply to confidentiality of communications.

When the UK response received was unsatisfactory, the EC repeated its request for information in stronger terms. When that second response was unsatisfactory, the Commission in January 2009 threatened legal action[103] and launched legal action in an infringement procedure against the UK in April 2009[104] (IP/09/570). Commissioner Reding declared:

---

[100] The Electronic Privacy Directive supplemented by the 2004 Communication on unsolicited commercial communications ('spam') COM(2004)0028.

[101] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data: Article 2(h)

[102] Directive 2002/58/EC on Privacy and Electronic Communications: Article 5(1)

[103] http://www.theregister.co.uk/2009/02/11/phorm_eu_action_threat/

[104] See Press Release IP/09/570.

> "I call on the UK authorities to change their national laws ... This should allow the UK to respond more vigorously to new challenges to ePrivacy and personal data protection such as those that have arisen in the Phorm case."

The Commission requested the UK authorities in October 2009 (IP/09/1626) to amend their rules to comply with EU law, due to inadequate national legal implementation in three main areas:

- no independent national authority to supervise the interception of some communications, although the establishment of such authority is required under EPD and DPD, in particular to hear complaints regarding interception of communications;
- Existing UK law allowed the interception of communications not only where the relevant internet users have consented to this but also where the person intercepting the communications has "reasonable grounds for believing" the consent to intercept has freely been given under the Regulation of Investigatory Powers Act 2000 (RIPA). RIPA obviously pre-dates the EPD. This is contrary to EPD which define consent as being "freely given, specific and informed indication of a person's wishes";
- UK laws prohibiting and providing sanctions in the case of unlawful interception were limited to intentional interception only, whereas EU law was wider, requiring member states to impose penalties for any unlawful interception irrespective of whether it was committed intentionally or not. UK law did not correctly implement confidentiality of electronic communications, and powers to fine in sanctions for breaches by the UK Information Commissioner's Office (the UK personal data protection authority) were inadequate under Article 28 DPD.

European laws meant to protect citizens' privacy and liberty also include the Framework Directive which lays down the tasks of NRAs, which include cooperating with each other and the Commission in a transparent manner to ensure the development of consistent regulatory practice, contributing to a high level of protection of personal data and privacy and ensuring that the integrity and security of public communications networks are maintained.[105]

In IP/10/121, the referral of the UK to the European Court of Justice reflected the Commission's view that the UK was breaching its obligations under the DPD and EPD, implemented in the UK through the Data Protection Act 1998 and Privacy and Electronic

[105] Directive 2002/21/EC, Article 8(4)f at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0021:en:NOT.

Communications (EC Directive) Regulations 2003 respectively, stating "the Commission considers that UK law does not comply with EU rules on consent to interception and on enforcement by supervisory authorities". The case therefore challenged much of the legitimacy of the UK communications privacy regime and its powers to enforce those rules, notably by ICO and the police forces.

Reform of UK interception law

The European Commission closed the infringement case on 26 January 2012 in recognition that UK national legislation was amended to properly implement EU law on the confidentiality of communications such as email or internet browsing.[106] Following the Commission's 2010 decision to refer the case to the Court of Justice of the European Union (CJEU),[107] the UK amended the Regulation of Investigatory Powers Act 2000 (RIPA), removing references to implied consent if the interceptor had 'reasonable grounds for believing' that consent had been granted. It also established a new sanction against unlawful interception in Section 1A and Schedule A1 of RIPA,[108] administered by the Interception of Communications Commissioner (ICC), who has published guidance with practical information on how it will exercise these new functions.[109] The maximum monetary penalty that can be imposed by a monetary penalty notice is £50,000 under the amended legislation. The ICC guidance notes at Paragraph 2.15 that,

> "The Commissioner shall consider serving a monetary penalty notice on a person only if, after investigation, he is satisfied that: the person has without lawful authority intercepted a communication; the conduct cannot be explained by an attempt to carry out an interception warrant; and the person has not committed an offence under section 1 of RIPA."

Criminal Investigation into BT/Phorm Dropped

---

[106] See Press Release IP/12/60,'Digital Agenda: Commission closes infringement case after UK correctly implements EU rules on privacy in electronic communications'.

[107] See Press Release IP/10/1215.

[108] Regulation of Investigatory Powers (Monetary Penalty Notices and Consents for Interceptions) Regulations 2011, SI 2011/1340.

[109] Interception of Communications Commissioner, Investigation of Unintentional Electronic Interception: Monetary Penalty Notice, Exercise Of Powers Under Section 1a And Schedule A1 Of The Regulation Of Investigatory Powers Act 2000, (2011) at <http://www.intelligencecommissioners.com/docs/Interception_Commissioner_Guidance_RIPA.pdf>

The conduct of the criminal investigation into the Phorm trials was finally abandoned on 8 April 2011, choreographed on the precise day upon which the legislative reform was announced. In 2008, the City of London Police started an investigation which was referred to the Crown Prosecution Service Complex Casework Centre, which in 2011 stated that the case was dropped of "several public interest factors against prosecution:

- "BT and Phorm received considerable legal advice concerning the use of this software and were advised its use was unlikely to be contrary to section 1 of RIPA. The Home Office also provided informal advice that stated the same. Following the second trial, BT received further and conflicting legal advice that led to it halting the covert trials. As there was no evidence to suggest either company acted in bad faith, it could be reasonably argued that any offending was the result of an honest mistake or genuine misunderstanding of the law;
- "Both companies cooperated with the police investigation;
- "The behaviour in question is unlikely to be repeated. After the first two trials, BT conducted a further single, public trial of the technology (in late 2008). Phorm now requests the user's consent;
- "The trial was of limited duration and limited application. The data gathered was anonymised and processed without human intervention and later destroyed;
- "There has already been an investigation by a regulator, the Information Commissioner's Office, which concluded there was "no evidence to suggest significant detriment to the individuals involved" and took no action;
- "There is no evidence to suggest that anyone affected by the trial suffered any loss or harm as a result;
- "Taking into account all of the above, a court would be likely to impose only a nominal penalty."[110]

Note that factors included assessments by ICO which was itself considered by the European Commission to have inadequate powers, and the lack of significant capacity to fine the parties for their illegal behaviour. It is also noteworthy that in 2009-10 ICO reprimanded the two ISPs

[110] Crown Prosecution Service (2011) CPS decides no prosecution of BT and Phorm for alleged interception of browsing data, of 08/04/2011 at http://blog.cps.gov.uk/2011/04/no-prosecution-of-bt-and-phorm-for-alleged-interception-of-browsing-data.html

that had decided after discussions not to trial Phorm's system, both Talk Talk and Virgin Media being reprimanded for their interception of subscribers' communications, in experimental applications of anti-net neutrality blocking of peer-to-peer and streaming services (which will likely become illegal under the proposed European regulation in 2014). In relation to Talk Talk, the Information Commissioner stated: "In the light of the public reaction to BT's trial of the proposed Webwise service, I am disappointed to note that this particular trial was not mentioned to my officials during the latest of our liaison meetings."[111] UK authorities will not prosecute for interception of confidential communications by ISPs, preferring to issue warnings.

The details that would be accessed by ISPs and Phorm may be illegal even with the subscribers' consent. Committees of both the US Congress and the UK Parliament carried out inquiries into behavioural advertising in 2009.[112] Article 15 ECD has also required European member states not to impose undue restrictions on ISPs since 2002[113] which continually causes member states to either derogate from ECD in the interests of crime fighting and anti-terrorism law or simply ignore the provision altogether. So many features of wire-tapping and anti-terrorism law have been passed or amended since 2001 that there would by now be several thousand derogations across the European member states, given that interception of communications by

[111] Sir Christopher Graham quoted in Beaumont, Claudine (2010) Information Commissioner reprimands Talk Talk: The Information Commissioner's Office has criticised internet service provider Talk Talk for failing to disclose details of a malware trial that tracked which websites users had visited, Daily Telegraph 08 Sep 2010 at http://www.telegraph.co.uk/technology/internet/7989262/Information-Commissioner-reprimands-Talk-Talk.html

112 See http://www.theregister.co.uk/2009/04/24/deep_packet_inspection/ on the US investigation, and http://www.apcomms.org.uk/category/Activities/ announcing 'Can we keep our hands off the net?' apComms to investigate the role for Government over Internet traffic.

[113] Directive 2000/31/EC Article 15 states: "No general obligation to monitor 1. Member States shall not impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14, to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances, indicating illegal activity. 2. Member States may establish obligations for information society service providers promptly to inform the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service or obligations to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service with whom they have storage agreements.

ISPs on behalf of governments formally requires a notification for derogation from Article 15 for each of the 28 Member States whenever anti-terrorist law is reformed in this area. The definition of the limits on general obligations to monitor – which are relevant for any imposition of for instance copyright monitoring on ISPs by member states – were explained by the European Court of Justice in the 2012 leading case of *SABAM v Netlog NV*[114]. The Court held that imposing a copyright filtering system on an ISP would infringe on the prohibition on general obligation to monitor, and (Paragraph 48):

> "may also infringe the fundamental rights of that hosting service provider's service users, namely their right to protection of their personal data and their freedom to receive or impart information ...[Para. 49] Indeed, the injunction requiring installation of the contested filtering system would involve the identification, systematic analysis and processing of information connected with the profiles created on the social network by its users [protected personal data]"

Note that the proposed reforms of the ECD including Article 15 were abandoned in 2012 by the European Commission in its E-Europe Action Plan. It is well established that no governmental authority or court can impose a general duty to intercept and monitor, because it infringes privacy rights.

Other Criminal Investigations into Interception of Communications

Interception of communications has eventually been prosecuted when carried out by private investigators such as those employed by Mr Rupert Murdoch's newspapers in the celebrated 'phone hacking' affair which included computer hacking[115]. However, this has little relationship to net neutrality discussions, and Mr Murdoch's ISP Sky Broadband has not been implicated in interception of its clients' communications.

---

[114] Case C-360/10, REFERENCE for a preliminary ruling under Article 267 TFEU from the rechtbank van eerste aanleg te Brussel (Belgium), made by decision of 28 June 2010, received at the Court on 19 July 2010, in the proceedings Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV, at http://curia.europa.eu/juris/document/document.jsf?text=&docid=119512&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=161927

[115] See BBC (2013) Phone hacking: Arrests by investigation, 13 June at http://www.bbc.co.uk/news/uk-politics-17014930

Note that individuals can bring complaints about alleged illegal interception by public authorities to the Investigatory Powers Tribunal, which publishes its most notable rulings on its website[116]. However, complaints about private parties including ISPs cannot be brought to the Tribunal, but instead to ICO or the police. It confirmed the analysis by Bowden[117] and Davies that UK law as implemented fails to protect citizens from interception, whether by government or private company, and heralding the European Parliament's decision to:

> "hold a full inquiry into US surveillance programmes, including the bugging of EU premises... It urged them to examine whether those programmes are compatible with EU law. This element of the inquiry could open up a number of sensitive Signals Intelligence relationships between Europe and the US – particularly the close operational partnership enjoyed by the US, Germany and the UK."[118]

It should be noted that criminal law enters the net neutrality debate in the field of counterfeiting and copyright. Civil liability includes potential to pay damages for every copyrighted item copied, for attorney fees for copyright holders pursuing the case, and for exemplary damages for such 'wilful' abuse of copyright. By contrast, until 2012, it was assumed that criminal liability would be limited as 'in exercising its power to render criminal certain forms of copyright infringement, [the United States] has acted with exceeding caution.'[119] However, the proposed extradition to the United States following the January 2012 arrest of MegaUpload executives in New Zealand has caused some surprise and uncertainty in the

[116] See http://www.ipt-uk.com/sections.asp?pageID=73&sectionID=19&type=rulings noting "That procedure runs no risk of disclosure of any information to any extent, or in any manner, that is contrary to or prejudicial to the matters referred to in section 69(6)(b) of RIPA and [Investigatory Powers Tribunal Rules (Statutory Instrument 2000 No. 2665)] rule 6(1)".

[117] Bowden, Caspar (2013) PRISM: The EU must take steps to protect cloud data from US snoopers, The Independent 10 July 2013 at http://www.independent.co.uk/voices/comment/prism-the-eu-must-take-steps-to-protect-cloud-data-from-us-snoopers-8701175.html

[118] Davies, Simon (2013) European Parliament votes to hold inquiry into US spying 4 July 2013, at http://www.privacysurgeon.org/blog/incision/european-parliament-votes-to-hold-full-inquiry-into-us-spying/

[119] *Dowling v United States*, 473 US 207, 222 (1985).

application of criminal law,[120] as it follows a 2005 restatement of enforcement policy.[121] The 'wilful' requirement in criminal law must be proved beyond reasonable doubt.[122] Nevertheless, a more aggressive prosecution of counterfeiting and other 'piracy' (sic) websites was signalled in 2011 with the taking down of domain names belonging to suspected overseas 'rogue sites'.[123] The cooperation of several national police forces in the Mega Upload case indicates a more general trend towards aggressive policing of counterfeiting. This overtook the controversies in the latter half of 2011 over US Congress and Senate versions of a more aggressive anti-infringement Bill.[124]

Conclusion: Regulatory Problems in Implementing Net Neutrality

The net neutrality privacy problem is not a lack of regulatory tools per se, but potentially a lack of forensic skills to analyse the potential consumer harms that can be created by unjustified or 'unreasonable' discrimination. Because net neutrality raises a set of new issues for regulators, the necessary skill set needs to be acquired and developed in consultation with other national and international regulators. It is important that governments consider where best the issue is regulated, by telecoms regulator or by ministry. Regulators can monitor both commercial transactions and traffic shaping by ISPs to detect potentially abusive discrimination. No matter what theoretical legal powers may exist, their usage in practice and forensic gathering of evidence may make the regulatory task very burdensome. DPI is a technique that may be both unreasonable and invasive of user privacy, and it may be that information/privacy commissioners are best placed to investigate such potentially criminal breaches of user rights.

---

[120] See Department of Justice Office of Public Affairs (19 January 2012) Justice Department Charges Leaders of Megaupload with Widespread Online Copyright Infringement.

[121] US ATTORNEY BULLETIN (2005) Novel Criminal Copyright Infringement Issues Related To The Internet available at <http://www.cybercrime.gov/usamay2001_5.htm>.

[122] See US Attorney Prosecuting IP Crimes Manual, Criminal Copyright Infringement Issues, §II.B.2 (2006), available at <http://www.cybercrime.gov/ipmanual/02ipma.html#II.B.2.a>.

[123] See Affidavit in Support of Application for Seizure Warrant Pursuant to 18 USC §§2323, 981, United States v Domain Names (defendants in rem), (31 January 2011) (No 18 MAG 262).

[124] See Law Professors (2011) Letter in Opposition to 'Threats to Economic Creativity and Theft of Intellectual Property Act of 2011' Draft 27 June 27 2011, available at <http://www.scribd.com/doc/59241037/PROTECT-IP-Letter-Final>.

Currently, neither is it a requirement for most ISPs to notify customers when they block vital P2P-distributed applications, nor are the security reasons given within the remit of typical economic telecoms regulators. The increasing use of behavioural advertising by third parties is also very concerning to privacy regulators, and any cooperation between ISPs and third parties to share such revenue is likely to need explicit consent of all ISP users, following the precedent of the Phorm case and European opinions recently issued about behavioural advertisers[125]. Where the security reasons given by ISPs for blocking P2P traffic, which carries malware and other harmful content, is typically the concern of the Ministry of the Interior (UK Home Office) and occasionally the Ministry of Industry, the regulator defers to these senior agencies because it has little technically specific knowledge of data security.[126] More joined up regulation is needed with urgency in this field.

[125] Recommendation CM/Rec(2010)13 of 23 November 2010 of the Council of Europe Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling; Article 29 Working Party WP203, 00569/13/EN Opinion 03/2013 on purpose limitation: p45; Article 29 Working Party (2011) Letter addressed to Ms Le Bail to deliver input to the Commission on the current practices at national level, the problems encountered in implementing the Directive as well as some suggestions for improvements or changes in relation to special categories of data ("sensitive data"), notification and the practical implementation of the Article 28(6) of the Directive 95/46/EC of 20.04.2011; Article 29 Working Party (2011) Opinion 16/2011 on EASA/IAB Best Practice Recommendation on Online Behavioural Advertising WP 188 (08.12.2011); Article 29 Working Party (2011) Press Release Brussels, 15 December 2011: "adherence to the EASA/IAB Code on online behavioural advertising and participation in the website www.youronlinechoices.eu does not result in compliance with the current e-Privacy Directive".

[126] See Brown, I. Edwards, L. and Marsden, C. (2006), Legal and institutional responses to Denial of Service Attacks, Communications Research Network/Department for Trade and Industry joint seminar on Spam/DDoS, 13 November, at www.communicationsresearch.net/object/download/1846/doc/marsden-edwards.ppt and on file with the author.

Annex: Government Interception of Communications Data: UK Inquiry

The Interception of Communications Commissioner (ICC) has submitted Annual Reports to the Prime Minister in the summer after the conclusion of the previous calendar year, with the latest issued in July 2013 reporting on calendar year 2012[127]. Despite the urgency of the public revelations of the potentially illegal use of Tempora programmes by GCHQ in June 2013, the ICC announced that he would publish their investigation into the GCHQ use of Tempora to intercept communications in the 2013 annual report in July 2014:

> "[ICC] is required by section 58(4) of RIPA to report annually to the Prime Minister. The Prime Minister lays the report before Parliament except for any sensitive parts of it which he decides to exclude under section 58(7)."[128]

He further explained that "my role is defined in Section 57(2) of RIPA. I am not appointed or authorised to oversee all of the activities of the intelligence agencies, only those specified in Section 57(2) of RIPA. Part I Chapter 1 of RIPA provides the statutory authority for lawful interception that takes place within the British Islands. I can confirm that I am currently conducting an investigation into the various recent media reports relating to disclosures about interception attributed to Edward Snowden."

Much of the relevant intercepted data is metadata, which is more useful to intelligence services and behavioural advertisers than content of communications which is not machine-readable and therefore too time-intensive to usefully be examined in large volumes. Part I Chapter 2 of RIPA 2000 covers the acquisition and disclosure of communications data (rather than the content of the communications). The ICC explained that:

> "I considered carefully the recommendations made by the Joint Committee on the Draft Communications Data Bill... The annual inspections under Part I Chapter 2 of RIPA will commence in January 2014."

Therefore some element of scrutiny of public authorities' use of metadata will commence and be reported in July 2015. Metadata is also a key concern of the Article 29 Working Group in its 2013/14 study of reform of European e-privacy law[129].

---

127 HC 571 2012 Annual Report of the Interception of Communications Commissioner, Ordered by the House of Commons to be printed on 18th July 2013, SG/2013/131

128 ICC (2013) Sir Anthony May's response to the Article published in the Independent, 16 July 13, at http://www.iocco-uk.info/sections.asp?sectionID=8&chapter=4&type=top

129 For instance see Article 29 Working Party (2010) Opinion 2/2010 on online behavioural advertising WP 171, at p7 (22.06.2010): "Article 29 Working Party is deeply concerned about the privacy and data protection implications of this increasingly widespread practice."

연구총서 13-B-03

망 중립성(Net Neutrality)과 통신비밀보호에 관한 형사정책

발 행 / 2014년 2월
발행인 / 박상옥
발행처 / 한국형사정책연구원
서울특별시 서초구 태봉로 114
(02)575-5282/5283
등 록 / 1990. 3. 20. 제21-143호
인 쇄 / (사)한국신체장애인복지회인쇄사업장
(02)6401-8891

정가 10,000원
ISBN 978-89-7366-019-3 93360