이용자 권리 보호와 ICT 산업 발전을 위한 플랫폼사업자의 책임원칙

정보매개자책임의 국제적 흐름

International Trends on Intermediary Liability

Designing Intermediary Liability Regime for Promotion of User Rights and ICT Industry

Contents

Contents

[제1세션] 정보매개자책임에 대한 이해
[Session 1] Safe Harbor (other parts of the world) vs. Limited Liability (Korea)

[제2세션] 정보매개자 책임과 ICT 생태계
[Session 2] Intermediary Liability and Digital Ecosystem

[제3세션] 정보매개자 책임과 저작권 제도
[Session 3] Intermediary Liability and Copyright

Open Net - Harvard Berkman Center Seminar on
Intermediary Liability

Designing Intermediary Liability Regime for Promotion of
User Rights and ICT Industry

Time	Title	Speakers
09:00~10:00	Registration	
10:00~10:20	Opening Remarks	MPs and Hosts
10:20~10:30	Introduction	Prof. **K.S. Park** (KU, Director of Open Net)
10:30~12:00	**Session 1** Safe Harbor (other parts of the world) vs. Limited Liability (Korea)	**Moderator** Prof. **K.S. Park** (KU, Director of Open Net) **Main Speaker** Prof. **Urs Gasser** (Harvard Berkman Center for Internet and Society) : *Online Intermediaries Project: Findings and Recommendations* **Panelists** Prof. **Youngjoon Kwon** (SNU Center for Law and Technology) Dr. **Yoo Hyang Kim** (Head, NARS Science, Media and Telecommunications Team) Mr. **Kyung Oh Jung** (Attorney at Law, Hanjung Partners) **Case Study** Ms. **Naoko Mizukoshi** (Partner, Endeavour Law Office) : *Intermediary Liability Rules in Japan*
12:00~13:30	Lunch	
13:30~15:00	**Session 2** Intermediary Liability and Digital Ecosystem	**Moderator** Prof. **Jewan Kim** (KU Law School Research Institute) **Main Speaker** ▪ Prof. **Anupam Chander** (UC Davis School of Law) : *The "Electronic Silk Road" and Intermediary Liability* ▪ Mr. **Oliver Süme** (President, EuroISPA) : *E-Commerce Directive and Experience of European ISPs* **Panelists** Prof. **Minjeong Kim** (Hankuk University of Foreign Studies) Mr. **Jongsoo Yoon** (Partner, Shin&Kim) Prof. **Inho Lee** (Chung-Ang University)
15:00~15:20	Coffee Break	
15:20~16:50	**Session 3** Intermediary Liability and Copyright	**Moderator** Prof. **Deok-Young Park** (Yonsei University) **Main Speaker** ▪ Prof. **Eric Goldman** (Santa Clara University School of Law) : *ISP Liability under DMCA* ▪ Dr. **Rebecca Giblin** (Monash University Faculty of Law) : *Evaluating Graduated Response* **Panelists** Dr. **Kyuhong Lee** (Presiding judge, Seoul Central District Court) Prof. **Pilwoon Jung** (Korea National University of Education) Mr. **Kyong-soo Choe** (Chief Senior Researcher, Korea Copyright Commission)
16:50~18:00	Wrap-up Session	

정보매개자책임의 국제적 흐름

이용자 권리 보호와 ICT 산업 발전을 위한 플랫폼사업자의 책임원칙

시 간	주 제	연 사
09:00~10:00	참석자 등록	
10:00~10:20	개회식	축사 / 인사말씀
10:20~10:30	세미나 취지 소개	**박경신** 교수 (고려대, 오픈넷 이사)
10:30~12:00	**제1세션** 정보매개자 책임에 대한 이해 (임시조치 등)	**좌 장** **박경신** 교수 (고려대, 오픈넷 이사) **주제발표** **어스 개서** 교수 (미 하버드대, 버크맨센터 소장) : 온라인 정보매개자 프로젝트 : 연구결과와 제안 **토 론** **권영준** 교수 (서울대 기술과법센터) **김유향** 팀장 (국회입법조사처 방송통신팀) **정경오** 변호사 (법무법인 한중) **특별토론** **나오코 미즈코시** 변호사 (일본 엔데버 법률사무소) : 일본의 정보매개자 책임 원칙
12:00~13:30	점 심 시 간	
13:30~15:00	**제2세션** 정보매개자 책임과 ICT 생태계	**좌 장** **김제완** 교수 (고려대 법학연구원) **주제발표** ▪ **아누팜 챈더** 교수 (미 UC데이비스 로스쿨) : "e-실크로드"와 정보매개자 책임 ▪ **올리버 쥬메** 회장 (유럽ISP협회) : EU 전자상거래지침과 유럽 ISP의 경험 **토 론** **김민정** 교수 (한국외대, 한국언론법학회 연구이사) **윤종수** 변호사 (법무법인 세종) **이인호** 교수 (중앙대, 정보법학회 회장)
15:00~15:20	휴 식	
15:20~16:50	**제3세션** 정보매개자 책임과 저작권 제도	**좌 장** **박덕영** 교수 (연세대 법학전문대학원) **주제발표** ▪ **에릭 골드먼** 교수 (미 산타클라라대 로스쿨) : 미국 디지털밀레니엄저작권법(DMCA)상 ISP의 책임 ▪ **레베카 긴린** 교수 (호주 모나쉬대) : 삼진아웃제에 대한 비교법적 평가 **토 론** **이규홍** 부장판사 (서울중앙지방법원 지재전담) **정필운** 교수 (한국교원대, 한국인터넷법학회 총무이사) **최경수** 수석연구위원 (한국저작권위원회)
16:50~18:00	종합토론 및 정리	

Opening Remarks

개회식

축사

Lim, Seong-Ho
임성호

▪ –	Ph.D 박사.	Political Sicence, Massachusetts Institute of Technology 미국 M.I.T 정치학
▪ –	M.A. 석사	Political Science, Sogang University 서강대학교 정치학
▪ Present	Professor 교수	Dept. of Political Science & Int'l Relations, Kyung Hee University 경희대학교 정치외교학과
▪ Present	Chief 국회입법조사처장	National Assembly Research Service (NARS) 국회입법조사처
▪ Present	Member 조사분석지원위원	Research and Analysis Support Committee, NARS 국회입법조사처 조사분석지원위원
▪ 2013	Member 위원	Reform Advisory Committee, National Assembly 국회개혁자문위원회

인사말씀 1

Park, Joo Sun
박주선

▪ 1976	M.A. 석사	Graduate School of Law, Seoul National University 서울대학교 법과대학
▪ Present	Member 제19대 국회의원	National Assembly of the Republic of Korea 대한민국 국회
▪ Present	Member 국회의원	New Politics Alliance for Democracy Party 새정치민주연합 소속
▪ Present	Member 위원	Education, Culture, Sports and Tourism Committee, National Assembly 국회 교육문화체육관광위원회
▪ 2014	Chairman 위원장	Special Committee on Supporting PyeongChang 2018 Olympic Winter Games and International Game, National Assembly 국회 평창동계올림픽및국제경기대회지원특별위원회
▪ 2011	Chairman 위원장	Special Committee on Developing Inter-Korean Relation, National Assembly 국회 남북관계발전특별위원회

인사말씀 2

Yeom, Dong Yeol
염동열

▪ 2012	Ph.D. 박사	Graduate School of Public Administration, Kookmin University 국민대학교 대학원 행정학
▪ Present	Member 제19대 국회의원	National Assembly of the Republic of Korea 대한민국 국회
▪ Present	Chairperson 위원장	Gangwon Province Council, Saenuri Party 새누리당 강원도당
▪ Present	Member 위원	Education, Culture, Sports and Tourism Committee, National Assembly 국회 교육문화체육관광위원회
▪ Present	Vice Chairman 부위원장	Special Committee on Ethics Reform, National Assembly 국회 윤리특별위원회
▪ Present	Member 위원	Special Committee on Creative Economy, National Assembly 국회 창조경제활성화특별위원회

인사말씀 3

Yoo, Seung-hee
유승희

▪ 2007	Ph.D. 박사	Graduate School of Public Administration, Han-yang University 한양대학교 대학원 행정학
▪ Present	Member 제19대 국회의원	Member of the National Assembly Republic of Korea 대한민국 국회
▪ Present	Member 위원	Science, ICT, Future Planning, Broadcasing and Communications Committee, National Assembly 국회 미래창조과학방송통신위원회
▪ Present	Chairperson 위원장	Chairperson, Special Committee on Freedom of Expression, New Politics Alliance for Democracy Party 새정치민주연합 표현의자유특별위원회
▪ Present	Member of the Supreme Council 최고위원	New Politics Alliance for Democracy Party 새정치민주연합
▪ Present	Member 위원	Euljiro Committee, New Politics Alliance for Democracy Party 새정치민주연합 을지로위원회

임성호
국회입법조사처장

안녕하십니까?

국회입법조사처장 임성호입니다.

오늘 “정보매개자책임의 국제적 흐름”이란 주제로 국제 세미나가 개최되는 것을 매우 뜻깊게 생각합니다.

바쁘신 의정활동에도 불구하고 이번 세미나를 공동 개최해주신 박주선 의원님, 염동열 의원님, 유승희 의원님께 감사드립니다. 그리고 이번 세미나를 기획하고 준비해주신 오픈넷 그리고 여러 학회 관계자 여러분께도 감사의 말씀을 드립니다. 아울러 귀중한 시간을 내어 이 자리에 참석해주신 내외귀빈 여러분, 그리고 이번 세미나에 주제 발표 및 토론에 참여해주신 해외 및 국내의 전문가분들께도 진심으로 감사의 말씀을 전해드립니다.

정보화 사회의 진전에 따라 우리는 인터넷을 통해 새로운 정보를 얻고, 다양한 생각을 공유할 수 있었으며, 경제적으로도 인터넷이 만들어내는 새로운 부가가치는 우리 경제의 중요한 축이 되고 있습니다. 하지만 다른 한편, 인터넷상의 저작권 및 사생활 침해 정보 등 각종 불법·유해 정보로 인해 발생하는 사회적 문제는 우리가 해결해야 하는 과제로 남아있습니다.

이와 같이 인터넷상에서 이루어지는 다양한 정보의 유통의 중심에는 정보매개자가 있습니다. 인터넷상 정보의 흐름은 발신자, 매개자, 수신자 차원에서 구성될 수 있으며, 인터넷 정보 유통을 중개하는 매개자에 대한 책임과 권한의 설정 문제는 인터넷 생태계의 선순환을 위해 매우 중요한 문제입니다. 이 때문에 오랜 기간 우리사회에서도 인터넷상 정보매개자에 대한 법적 규율을 어떠한 방식에서 해야 하는가에 대한 논의가 있어왔습니다.

즉 인터넷정보매개자에 대한 법적 규제는 인터넷상의 정보유통을 제약하고, 이는 인터넷상 참여와 소통의 문제를 침해하는 문제를 가져올 뿐만 아니라 인터넷 산업의 위축을 가져오기 자율규제를 강화하자는 입장이 있는 반면, 인터넷상에서 이루어지는 불법·유해 정보는 큰 사회적 문제를 가져올 수 있기 때문에 인터넷정보매개자의 법적 책임을 강화하자는 주장도 꾸준히 제기되고 있습니다.

이러한 현실에서 해외 각국의 사례를 살펴보는 것은 우리의 인터넷 규제를 정립하고 발전시켜나가는데 시사하는 바가 크다고 생각합니다. 일찍이 해외 각국은 인터넷상에 정보매개자의 권리와 책임에 대한 사회적 합의 아래 규제를 마련해왔으며, 이러한 기준 하에서 인터넷상 정보매개자에 대한 자율과 규제에 대한 접점을 찾아왔습니다.

아울러 우리의 규제를 국제적 기준에서 비교 검토해보는 것은 우리의 인터넷 경쟁력을 강화하기 위해서도 의미가 있다고 생각합니다. 인터넷이 갖고 있는 개방성은 인터넷 규제에 있어 국경이 없다는 것을 말해줍니다. 이러한 측면에서 우리의 인터넷 규제가 글로벌한 수준에 접근하지 못한다면 국내 인터넷 산업 경쟁력의 약화와 직결되는 문제이기도 합니다.

이번 세미나가 해외의 사례를 참고하면서 인터넷 규제에 대한 글로벌 스탠다드가 어떠한 방향으로 수렴하고 있는지를 검토해보고, 우리나라의 인터넷 규제가 어떠한 방향에서, 어떠한 수준에서 이루어져야 하는지를 고민하는 자리가 되길 바랍니다. 그리고 이번 세미나에서 나온 결과가 국회에서 효율적인 입법적 대안을 만드는데 도움이 되길 기원합니다.

다시 한번 바쁘신 가운데 이번 세미나 개최를 위해 애써주신 여러 관계자 여러분, 그리고 세미나에 사회, 발표, 토론을 맞아주신 국내외의 저명한 전문가 여러분께 감사의 말씀을 전하면서 오늘 세미나가 한국의 인터넷산업의 지속적인 성장과 발전을 위한 생산적인 논의의 장이 되길 기원합니다.

감사합니다.

박주선
국회의원

안녕하십니까?

국회 교육문화체육관광위원회 소속 박주선 의원입니다.

먼저 바쁜 일정에도 불구하고 오늘 “정보매개자 책임의 국제적 흐름” 국제 세미나에 참석하여 이 자리를 빛내주신 내외 귀빈 여러분께 감사의 말씀을 드립니다.

특히 지구 반 바퀴라 표현해도 될 만큼 먼 거리임에도 미국, 영국, 호주 등 여러 나라의 전문가들께서 참석해주셨습니다. 미국의 어스 개서 하버드대학교 버크맨센터 소장님, 아누팜 챈더 UC데이비스 로스쿨 교수님, 에릭 골드먼 산타클라라대 로스쿨 교수님, 올리버 쥬메 유럽ISP협회 회장님, 호주의 레베카 깁린 모나쉬대 교수님, 일본의 나오코 미즈코시 변호사님께 더욱 깊은 감사의 인사를 드립니다.

아울러 좌장으로서 오늘 세미나를 이끌어 주실 박경신·김제완·박덕영 교수님을 비롯하여, 이규홍 부장판사님, 권영준·김민정·이인호·정필운 교수님 등 귀한 시간을 내어 참석해 주신 모든 패널 여러분들께 진심으로 감사드립니다.

인터넷은 정보의 바다입니다. 지금 순간에도 수백만, 수천만 건의 정보가 새롭게 등록되고 있습니다. 이렇게 모여진 정보들은 인터넷 서비스 제공자(ISP), 소셜네트워크(SNS), 검색엔진 등 정보매개자들을 통해 유통되며, 이용자들 역시 정보매개자들이 제공하는 플랫폼을 이용하여 정보를 공유하거나 활용합니다. 이 과정에서 제3자인 이용자들이 유통하는 정보에 대해 정보매개자인 사업자들에게 어떠한 책임을 지울 것인지는 인터넷의 미래를 좌우할 중차대한 문제라고 할 수 있습니다.

이같은 문제에 대해 외국에서는 어떻게 대응하고 있을까요? 지난 2012년 8월 헌법재판소는 외국의 입법례를 다음과 같이 설명했습니다.

“현재 인터넷상의 불법·유해정보의 규제에 관한 외국의 입법례들을 살펴보면 미국이나 영국의 경우 인터넷상의 유해 정보에 대한 규제를 원칙적으로 업계의 자율에 맡기고 있고, 독일 등 유럽의 많은 국가들 역시 민간 주도의 자율규제를 기초로 하여 인터넷서비스 제공자의 책임제한이나 면책요건을 정하는 방식으로 관계 법령을 수립하고 있으며, 일본의 경우에도 불법·유해정보가 게시되는 때에 민관(民官)이 협조하여 사후적으로 대처하도록 규율하고 있는 등 대부분의 주요 국가들은 본인확인제와 같은 적극적인 게시판 이용규제를 시행하고 있지 않다. (2012. 8. 23. 2010헌마47·252) ”

이처럼 외국에서는 주로 면책조항(safe harbor)을 이용, 사업자의 자율규제를 유도하고 있습니다. 반면 우리나라는 다양한 법에서 사업자에게 불법정보를 차단할 의무를 직접적으로 지우는 방식을 취하고 있습니다. 예컨대 저작권법상 삼진아웃제도, 정보통신망법상 임시조치제도, 방송통신위원회와 방송통신심의위원회의 제재 및 시정요구제도, 전기통신사업법상 부가통신사업자 신고제도 등 세계적으로도 유례가 없는 규제를 시행하고 있으며, 그 밖에도 아동·청소년의 성 보호에 관한 법률, 전자상거래법 등에서 다양한 정보매개자 규제들을 두고 있습니다.

이로 인해 불법정보 뿐만 아니라 합법정보에 대한 이용자들의 표현의 자유와 정보접근권이 제한되는 경우가 종종 발생하고, 면책이 아닌 처벌 위주의 규제들은 신생기업들을 포함한 국내사업자들에게 부담으로 작용해 한국 ICT 산업의 발전을 저해하고 있는 상황입니다.

강력한 규제조치만으로 모든 문제를 해결할 수 있다면 좋겠지만, 인터넷의 특성을 감안한다면 이같은 조치는 ‘허울 좋은 명분’에 불과할 수도 있습니다. 2012년 8월 헌법재판소는 표현의 자유를 침해한다는 비판을 받아온 인터넷 본인확인제에 대해 재판관 전원 일치 의견으로 위헌결정을 내리면서 이렇게 강조했습니다.

“인터넷은 전 세계를 망라하는 거대한 컴퓨터 통신망의 집합체로서 개방성을 주요한 특징이다. 외국의 보편적 규제와 동떨어진 우리 법상의 규제는 손쉽게 회피될 수 있고 우리 법상의 규제가 의도하는 공익의 달성은 단지 허울 좋은 명분에 그치게 될 수 있다. (2012. 8. 23. 2010헌마47·252)”

하루가 다르게 변해가는 인터넷 환경은 무한한 기회의 공간입니다. 그렇다고 그냥 방치해 둘 수만도 없습니다. 이번 세미나를 통해 현재 국내의 정보매개자 규제를 외국의 제도 및 국제적 흐름과 국제적으로 비교함으로써, 이용자의 권리 보호와 ICT 산업 발전을 촉진하는 플랫폼사업자 책임원칙을 모색해보고자 합니다. 오늘 이 자리를 통해 생산적이고 창의적인 많은 담론과 제안이 펼쳐질 수 있게 되기를 진심으로 바랍니다.

저 또한 오늘 세미나에서 많은 분들이 조언해주시는 이야기를 귀담아 듣고, 인터넷 속도만 빠른 것이 아니라 인터넷을 통해 수많은 일자리와 부가가치를 창출되는 진정한 인터넷 강국이 될 수 있도록 국회 안에서 최선을 다해 노력할 것을 약속드립니다.

감사합니다.

염동열
국회의원

안녕하십니까?

강원도 태백·영월·평창·정선 출신의 국회 교육문화체육관광위원회 위원 새누리당 염동열 의원입니다.

먼저 내외귀빈 여러분과 국내외의 정보통신 및 관련법 분야의 저명한 전문가분들을 모시고 「정보매개자 책임의 국제적 흐름」이라는 주제로 오랫동안 교문위에서 함께 해 온 존경하는 새정치민주연합 박주선의원님, 그리고 미래창조과학방송통신위원회 유승희의원님과 함께 토론회를 개최한 것을 매우 뜻 깊게 생각합니다.

지금 우리 사회는 정보사회(information society)라는 말이 무색할 정도이며, 특히 인터넷을 통한 정보의 유통 및 활용은 일상이 되고 있습니다. 이와 함께 일시에 유용한 많은 정보를 주고받을 수 있다는 장점 못지않게 가상공간에서 발생하는 여러 가지 문제로 부정적인 측면도 드러나고 있습니다.

바로 이점에서 '정보매개자의 책임문제'가 중요한 이슈로 부각되고 있다고 봅니다. 오늘 토론회를 개최해 제반문제를 논의하고자 하는 것도 바로 이와 같은 문제인식에서 비롯된 것 아닌가 생각해 봅니다.

인터넷을 비롯한 가상공간에서 소통되는 정보의 생산•유통과정에서 정보제공자는 물론 정보이용자들이 윤리의식을 토대로 이용자들에게 도움이 되는 합법적이고 유용한 정보를 공유하고 확대•재생산하려는 발전적 노력이 필요합니다. 하지만 제도적·정책적 관점에서 불법정보나 반사회적 정보제공 및 유통에 대해서는 엄격한 제제나 규제조치를 취할 필요성 또한 증대되고 있습니다.

오늘 토론회는 바로 그와 같은 관점에서 수용 가능한 책임원칙 내지 수준을 어떻게 설정할 지에 대해 논의하는 자리가 될 것으로 보입니다. 느슨한 규제는 불법정보의 범람으로 가상공간을 혼란에 빠트릴 수 있는 반면, 지나치게 엄격한 규제는 정보매개자들의 자발적 네트워크를 마비시켜 정보사회의 근간을 붕괴시킬 우려도 있습니다.

이러한 쟁점에 대해 오늘 토론회에서 국내외 저명한 전문가들의 논의를 통해 합리적이고 수용 가능한 대안이 제시될 수 있을 것으로 기대합니다.

토론회를 준비해 주신 실무관계자 여러분들의 노고에 감사드리며, 특히 바쁜 일정에도 불구하고 참석해 주신 내외 귀빈 여러분과 귀중한 연구결과를 기꺼이 오늘 토론회에서 발표하고 논의해 주실 토론진 여러분께 특별한 감사를 드립니다.

다시 한 번 참석해 주신 한 분 한 분 모두 건강하시고, 가정과 직장에 만복이 충만하기를 기원합니다.

감사합니다.

유승희
국회의원
새정치민주연합
최고위원
표현의자유특별위원회
위원장

여러분 안녕하십니까.

새정치민주연합 최고위원, 서울시 성북갑 유승희 국회의원입니다.

먼저 오늘 행사를 공동으로 주최해 주신 박주선 의원님, 염동열 의원님, 국회입법조사처, 그리고 사단법인 오픈넷과 하버드대학교 버크맨 인터넷과 사회 연구센터 및 국내 관련학회 등 관계자 여러분들께 감사의 말씀 드립니다.

그리고, 오늘 심포지움을 위해 멀리 미국에서 찾아 주신 하버드대 어스 개서 교수님, UC데이비스 로스쿨 아누팜 챈더 교수님, 산타클라라대 에릭 골드먼 교수님과 호주 모나쉬대 레베카 깁린 교수님, 일본 나오코 니즈코시 변호사님, 그리고 유럽 ISP협회 올리버쥬메 회장님께도 진심으로 감사드립니다.

우리나라는 인터넷과 ICT 산업이 가장 발전한 선두 국가 중 하나입니다. 70~80년대 민주화운동을 통해 이룩한 민주주의를 더욱 공고히 하기 위해서는 지금과 같이 발전된 인터넷과 SNS 그리고 정보통신의 기능이 더욱 중요한 때입니다.

그러나 우리나라는 안타깝게도 민주주의의 핵심가치이자 헌법으로 보장된 기본권인 언론의 자유, 표현의 자유가 억압받고 후퇴되고 있는 실정입니다.

세계 인권감시단체인 프리덤하우스는 2010년부터 한국을 언론자유 측면에서 더 이상 "자유" 국가가 아닌 "부분자유" 국가로 강등시켰고, 신설한 인터넷 자유지수에서도 "부분자유" 국가로 분류하고 있습니다.

프랭크 라 뤼 국제연합(UN) 표현의자유 특별보고관도 대한민국이 이명박 정권하에서 명예훼손죄의 남용, 인터넷 표현의 자유의 제한, 선거운동에 대한 과도한 제한, 국가보안법의 남용, 방송의 독립성 침해와 정부의 통제 등에 대해 심각하게 문제를 제기하고 제도적 개선책에 대한 강력한 권고하고 있는 상황입니다.

인터넷에서의 표현의 자유 보장을 위해서는 정보 생성자와 정보를 유통하는 정보매개자에 대한 책임의 소재와 범위를 어떻게 다룰 것이냐는 문제가 매우 중요합니다.

다른 나라들은 정보매개자인 사업자들의 자율규제를 최대한 유도하고 있는 반면, 우리나라는 사업자에게 불법정보를 차단할 의무를 부과하고 있고 이로 인해 합법정보에까지 무차별하게 차단함으로써 이용자들의 표현의 자유와 정보접근권이 제한되는 부작용이 발생하는 상황입니다.

올해부터는 일명 "유승희 법 – 방송통신위원회 설치 및 운영에 관한 법률"이 시행되면서 불법적인 인터넷 콘텐츠라 할지라도 이를 삭제 또는 차단할 경우 정보를 게시한 당사자나 그 대리인에게 의견을 진술 할 기회를 부여하여 권리를 보장하고 있습니다.

그동안 무차별적인 적용으로 인해 표현의 자유를 심각하게 억압하였던 명예훼손죄도 비형사범죄화 및 친고죄로 전환하여 징역형을 폐지하고, 법 적용도 엄격하게 개선하였습니다.

제가 새정치민주연합 최고위원 선거에서 약속한 "표현의자유특별위원회"를 설치하여 자유로운 의사표현과 위기의 민주주의 수호를 위해 노력하고 있으며, 앞으로 국민의 자유로운 의사 표현과 소통을 위한 노력을 경주해 나가야 할 것입니다.

아무쪼록 어렵게 마련된 오늘 이 자리가 우리나라 인터넷 이용자들의 권리보호와 표현의 자유를 최대한 보장하고, 우리나라 ICT 산업 발전에도 크게 도움 되는 많은 논의가 이루어지기를 기대합니다.

마지막으로 오늘 행사를 후원해 주신 방송통신위원회, 한국저작권위원회와 행사 준비에 고생하신 오픈넷 관계자 여러분들께 다시한번 감사드립니다.

감사합니다.

Intro

Intermediary liability
: Not Just Backward but Going Back

Prof. **K.S. Park**
(KU, Director of Open Net)

인터넷의 특성과
임시조치 및 저작권 전송중단제도

박경신 교수 (고려대, 오픈넷 이사)

Kyung-Sin (K.S.) Park

▪ Professor at Korea University Law School

Korea University Law School Professor PARK Kyung-Sin, a.k.a. K.S. Park, one of the founders of Open Net Korea, and has written academically and been active in internet, free speech, privacy, defamation, copyright, international contracting, etc. (quoted in Freedom House report, New York Times) He has given expert testimonies in high-profile free speech and privacy cases concerning Minerva, the internet real name verification law, the military's seditious book blacklisting, the newspaper consumers' boycott, and Park Jung-Geun the one jailed for retweeting North Korean government twits. As a result, the "false news" crime in the Minerva case and the internet real name verification laws were struck down as unconstitutional, Park Jung-Geun and Minerva were acquitted, the soldiers challenging book blacklisting were reinstated, the newspaper boycotters' judgment acquitted the "secondary boycotting" charge (2010-2013).

Since 2006, he also has served as the executive director of the PSPD Law Center, a non-profit entity that has organized several impact litigations, including some of the above cases, in the areas of free speech, privacy, and copyright. There, the Law Center won the world's first damage lawsuit against a copyright holder for "bad faith" takedown (2009). On privacy, the Law Center won the world's first damage lawsuit against a major portal for warrantless disclosure of the user identity data to the police (2012). As a result of this judgment, all major portals stopped complying with such data requests by the government. As to the three major telcos that have continued to comply with user identity data requests, the Law Center won another suit in 2015 forcing them to inform the user on whether such data release has taken place on him or not. The Law Center also filed a suit against the Korean Prosecutor's Office for failing to notify an e-mail user of the fact of seizure of his emails and won a damages award (2013).

In 2008, He also founded the Clinical Legal Education Center of Korea University School of Law (f.k.a. Global Legal Clinic) which in 2009 through 2010 successfully carried on a successful campaign to enter Korea into the Supplementary Fund in the wake of one of the largest oil spill ever. In 2011, in the spirit of solidity of www.chillingeffects.org, he and his former clinic students founded www.internetlawclinic.org with law students, where people and cultural producers alike can obtain free legal advices in the areas of copyright, trademarks, publicity rights, defamation, privacy, etc.

In 2009, he served as a member of the National Media Council, an advisory body to the National Assembly set up to examine the historic bills allowing media cross-ownership, among other things. While sitting on the council, he has spearheaded an effort to oppose a new bill creating a new crime of "cyber-insult".

Until, he has been a commissioner of the Korean Communication Standards Commission, a governmental entity censoring broadcasting and internet contents, where he has given many dissenting opinions.

An alumnus of Harvard University (Class of '92, Physics) and UCLA Law School (Class of '95), licensed in California and Washington State, he represented immigrant workers in restaurant, garment, and janitorial industry. He has filed or defended, and won major lawsuits against brand-name garment manufacturers and large department stores (1995-1997, Los Angeles) and has also participated in the historic civil rights class action against the local Metropolitan Transit Authority.

He is also the founding editor (2007) and the Editor in Chief of Korea University Law Review, available on Westlaw.

Intermediary liability : Not Just Backward but Going Back[1)]

※ This is the result of collaboration with Harvard University's Berkman Center for Law and Society.

1. Introduction

[. . .]

2. Landscape of Korean intermediaries

a Market survey

1) The full paper is published online at 〈https://publixphere.net/i/noc/page/OI_Case_Study_Intermediary_liability__Not_Just_Backward_but_Going_Back〉 Also, parts of it published in Korean, "Unconstitutionality of Korea's Temporary Blinds on Internet –"Thou Shall Not Speak for 30 days What Others Do Not Like", Joongang Law Review, Vol.11 No.3 Pages 7–51 [2009] http://m.riss.kr/search/detail/DetailView.do?p_mat_type=1a0202e37d52c72d&control_no=446c374bd83dd689ffe0bdc3ef48d419

As of 2013, Korea had a total population of about 48 million people (83% urban) with an Internet penetration rate of 84%, mobile penetration rate of 110%, mobile Internet penetration rate of 75%, and Facebook penetration of 27%[2]. [. . .]

b Social significance of different intermediaries

In non-economic terms, certain intermediaries are more relevant than others – e.g. in terms of market share, popularity, usage patterns, and their impact on society. NAVER and DAUM curate and present other agencies news in their own pages, host original user-created discussion pages, and blogs (NAVER) and cafe pages (DAUM), which have become major platforms for political debates. FACEBOOK has become the socializing platform of choice for both conservative and progressive circles. TWITTER, which had become the main battleground for political discussions, became even more famous as it was later revealed that National Intelligence Services, the country's intelligence agency, had conducted major public-opinion-manipulation campaigns using TWITTER before and during the Presidential election period in 2012.[3] [. . .]

c State paternalism

Indeed, one significant factor affecting online intermediaries is state paternalism, which pervades the country's industrial institutions and practices. For instance, all Internet companies with capital larger than about USD 100K are required to register and are given a "value-added telecommunication business" number, which can be taken away if they do not operate in compliance with the government's laws and regulations or their operation "significantly hurts consumers' interests".[4]

2) We Are Social Singapore, "Global Digital Statistics 2014", January 2014 http://www.slideshare.net/wearesocialsg/social-digital-mobile-around-the-world-january-2014, page 146-146 (cited sources: ITU, Facebook, U.S. Census Bureau, Global Webindex)
3) New York Times, "Prosecutors Detail Attempt to Sway South Koran Election", November 21, 2013. http://www.nytimes.com/2013/11/22/world/asia/prosecutors-detail-bid-to-sway-south-korean-election.html?_r=0
4) Article 27 Paragraph 2 of the Telecommunications Business Act

This environment creates a cloud under which the domestic companies feel the pressure to comply with even extra-legal guidance of the government. [. . .]

3. Korea's Intermediary Liability Regime

a Intermediary liability in general

What defines the Internet? The defining feature of the Internet is its nature as an extremely distributed communication platform, so distributed that it allows almost all individuals to participate in mass-scale communication. All individuals are allowed to post individual views and opinions without anyone's approval, and all individuals are allowed to view and download all other individuals' postings.

How some people react to questionable material found online shows how they have not accustomed themselves to this freedom of the Internet. They think that Internet companies should be responsible for contents on their services. Yes, illegal activities such as defamation and copyright infringement that abuse the power of the Internet should be combated. However, unless we want to paralyze the freedom of unapproved uploading and viewing and therefore the power of the Internet, an intermediary that cannot possibly know who posts what contents, should not be held responsible for defamation or copyright infringements committed via some contents on its services. If intermediaries are held liable for these unknown contents [as in **strict liability**], the intermediaries will have to protect themselves by constantly monitoring what gets posted on their services. If that happens, one can say that, when a posting remains online, it remains online at the pleasure and tacit approval of the intermediary that saw the posting and did not block it. The power of the Internet — the freedom to post and download unapproved — will be dead.

For the same reason, no country imposes – for instance – content liability on broadband providers.[5] No common carrier will be in business if it is held liable for

5) Section 512 (a) of the Digital Millennium Copyright Act

all the criminal conspiracies and deals taking place over their networks. Now, the same reasoning should be extended to the providers of web applications that greatly facilitate the exchange of ideas and contents, i.e. "portals" and "search engines". The only difference with the common carriers will be that the Internet companies carry the unlawful contents on their servers while the telecoms serve the contents en route. While some will surely abuse free space created by these intermediaries, holding the intermediaries liable merely for creating this space would be too threatening to the future of the Internet.

However, as to other areas, many believe that there must be a limit on the exemption that the intermediary enjoys: the intermediary should not be immunized for the infringing content that it is aware of or is given notice of and yet refuses to remove. Yet this idea of a **limited liability regime** is not satisfactory because the intermediaries always face a stronger incentive to take down individual contents than an incentive to keep them on. The reason is that, firstly, they are massive content processors whose interest in individual contents are minuscule, and secondly, tort liability regimes around the world are usually such that the legal exposure for keeping a posting on (a malfeasance) is always greater than the legal exposure for not keeping it (a nonfeasance).

Therefrom, many countries decided to set up **"safe-harbor"** regimes where the intermediaries will be exempt from liability if they choose to follow certain clearly defined procedures aimed at abating unlawful content. The most widely popular such regime is the notice-and-takedown regime,[6] whereby an intermediary is given an exemption from liability as long as it removes content of which it is given notice of the infringing nature by a rights holder. [Along this line of thought, on non-copyright-related contents, the U.S. even went a little further by granting **a broad immunity** by providing that no "interactive computer service" shall be considered a speaker or a publisher of those contents.[7]]

6) DMCA section 512 (c) and (g)
7) Communications Decency Act of 1996: 47 USC 230 "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."

b Korean law: liability-exemption or liability-imposition?

In Korea, the idea that the intermediaries must be given exemption from liability in the way of safe harbor on the Internet appears to have been misinterpreted: what we have is not an intermediary liability exemption regime but intermediary liability imposition regime. The relevant provisions are as follows:

The Act Regarding Promotion of Use of Information Communication Networks and Protection of Information, Article 44-2 (Request to Delete Information) reads:

Paragraph 1. Anyone whose rights have been violated through invasion of privacy, defamation, etc., by information offered for disclosure to the general public through an information communication network may request the information communication service provider handling that information to delete the information or publish rebuttal thereto by certifying the fact of the violations.

Paragraph 2. The information communication service provider, upon receiving the request set forth in Section 1 shall immediately delete or temporarily blind, or take other necessary measures on, the information and immediately inform the author of the information and the applicant for deleting that information. The service provider shall inform the users of the fact of having taken the necessary measures by posting on the related bulletin board.

[omitted]

Paragraph 4. In spite of the request set forth in Section 1, if the service provider finds it difficult to decide whether the rights have been violated or anticipates a dispute among the interested parties, the service provider may take a measure temporarily blocking access to the information ("temporary measure", hereinafter), which may last up to 30 days

[omitted]

Paragraph 6. The service provider may have reduced or exempted the damage liability by taking necessary actions set forth in Paragraph 2.

As is immediately apparent, the provision is structured not with such phrases as "the service provider shall not be liable when it removes . . ." but starts out with a

phrase “the service provider shall remove …”.

Paragraph 6, referring to the “exemption from or reduction of liability in event of compliance with the aforesaid duties,” makes a feeble attempt to turn the provisions into an exemption provision like the notice-and-takedown of the Digital Millennium Copyright Act. [However, DMCA does not obligate the intermediaries to do anything but offers as an option to go through notice-and-takedown procedure and qualify for exemption. Korea’s aforesaid law obligates the intermediaries to go through notice-and-takedown on all contents noticed.] In fact, none of the service providers interpret Article 44-2 as an exemption provision that they are allowed to deviate from on the simple penalty of foregoing a safe-harbor. All of them interpret it as an obligatory provision that they must comply with.

[. . .]

c On-Demand (Temporary) Takedown Obligations

[. . .] Article 44-2 Paragraphs 1, 2 and 4 of the Act Regarding Promotion of Use of Information Communication Network and Protection of Information (“Network Act”) is that they require the service provider to take at least a “temporary measure” on all contents upon which the takedown request has been made regardless of the legality of the content.

[T]he statute sets up such on-demand takedown obligation explicitly. Although it speaks of an obligation to remove only when someone “whose rights have been violated” makes such request, it is impossible to know ex ante whether rights-infringement has taken place. So the only feasible interpretation is that such obligation arises whenever someone who thinks and proposes that his rights have been violated. Going further on this line of interpretation, this obligation can be instead filled by “temporary measure”, too, but that is the minimum: the intermediary should take some abatement action even against. Now, the statute thus interpreted will be against all known constitutions and international human rights treaties which allow freedom of speech to be violated only to relieve some other rights or values.

[. . . .]

[Similar provisions are in the Copyright Act as well:

Copyright Act Article 103 (Suspension of Reproduction or Transmission)

(1) Any person who asserts that his/her copyright and other rights protected under this Act are infringed (hereafter referred to in this Article as “claimant to a right”) due to the reproduction or transmission of works, etc. through the utilization of services by an online service provider (excluding cases under Article 102 (1) 1; hereafter the same shall apply in this Article), may demand the online service provider, by vindicating the said facts, to suspend the reproduction or transmission of the works, etc.

(2) Where an online service provider is requested to suspend the reproduction or transmission under paragraph (1), he/she shall immediately suspend the reproduction or transmission of such works, etc. and notify a claimant to the right of such fact: Provided, That an online service provider referred to in Article 102 (1) 3 or 4 shall notify the reproducer or transmitter of such works, etc., as well as the claimant to the right, of such fact.

. . .

(5) Where the online service provider . . .has suspended. . .the reproduction or transmission of relevant works, etc. under paragraphs (2) and (3), the liability of the online service provider for the infringement on third parties’ copyright and other rights protected under this Act. . . shall be exempted. . .]

4. Result: Private Censorship

In summary, Article 44-2 states that all contents should be taken down upon demand even if lawful. [. . .] Article 44-2 and the Court decisions together encourage private censorship by the intermediaries. [. . .] [MP Choi Moon-soon’s disclosure in November 2010[8] and MP Nam Kyung-pil’s disclosure in October 2012[9] show that the annual number of URLs taken down by NAVER hover above 100,000 and that for DAUM is about 50-70% of NAVERs.]

[. . .]

8) http://moonsoonc.tistory.com/attachment/cfile23.uf@133D7F0F4CE1EF660D3B87.hwp
9) http://www.ggetv.co.kr/news/articleView.html?idxno=16781

It is not just the volume of censorship that is problematic. Politicians and government officials often make the takedown requests on postings critical of their policy decisions that are clearly lawful as illustrated below:

- A posting[10] critical of a Seoul City mayor's ban on assemblies in the Seoul Square
- A posting[11] critical of a legislator's drinking habits and introducing his social media account;
- Clips of a television news report on Seoul Police Chief's brother who allegedly runs an illegal brothel-hotel;[12]
- A posting critical of politicians' pejorative remarks on the recent deaths of squatters and police officers in a redevelopment dispute[13]
- A posting calling for immunity from criminal prosecutions and civil damage suits on labor strikes.[14]
- A posting by an opposition party legislator questioning a conservative media executive's involvement in a sex exploitation scandal related to an actress and her suicide.[15]

5. People's Response: Constitutional Challenge

It is okay not to institute intermediary immunity regimes such as the United States' CDA Section 230 or DMCA Section 512 that shields intermediaries from liability for even unlawful contents. However, Korea does much worse: It chills the intermediaries into taking down even lawful content as evidenced by the examples above. The PSPD Public Interest Law Center and others filed a constitutional challenge against Article 44-2 of the Network Act on the theory that the total result of the aforesaid provisions is that "Thou Shall Delay Saying What Others Dislike, As Long As 30 days."[16] For the Constitution does not authorize abating a speech not violating others' rights, the aforesaid provisions [. . .] requiring even lawful contents to be abated for up to 30 days therefore are unconstitutional.

Under the current statutory scheme, the temporary removal can be up to 30 days. DAUM set it at the maximum of 30 days, while NAVER set it at a period lasting until the publisher requests reposting. NAVER's system looks a lot like a notice-and-takedown without mandatory exemption. However, the statute is requiring even NAVER to take down what is clearly lawful at least once. The rule "Thou Shall Not Say What Others Dislike Unless Thou Have Courage to Say Twice" is equally unconstitutional.

In 2012, the Constitutional Court rejected the challenge[. . .]:[17]

> When a temporary measure is taken for the reason that "it is difficult to judge whether the rights have been infringed or when a dispute between the interested parties is anticipated", the degree of restriction on the poster's freedom of speech becomes greater. . . .However, in this situation, such measure has the effect of preventing frivolous improvised attacks or the spreading of information that as a result infringe on another's rights in anonymous cyberspace. . .
>
> [. . .] That speech can be banned on the basis of a possible illegality is a far departure from the established rules of free speech such as a clear and present doctrine, void-for-vagueness, prior restraint ban, etc. The reason for such leniency is found in the earlier portions of the decision emphasizing how fast, far, and wide defamatory information travels through the Internet. However, the decision does not mention how fast, far and wide corrective information can travel. Sure, the Internet's self-corrective nature cannot be the basis for exempting all unlawful activities on the Internet. However, communicative efficiency of a medium cannot be a justification for taking down contents that are lawful on that medium. In all other media, only

10) http://blog.ohmynews.com/savenature/199381
11) The original posting now taken down is shown here. http://wnsgud313.tistory.com/156
12) http://www.hani.co.kr/arti/society/society_general/300688.html
13) http://blog.jinbo.net/gimche/?pid=668
14) http://blog.jinbo.net/gimche/?pid=492
15) http://bbs1.agora.media.daum.net/gaia/do/debate/read?bbsId=D115&articleId=610524
16) Park Kyung-sin, "Unconstitutionality of Korea's Temporary Blinds on Internet – "Thou Shall Not Speak for 30 days What Others Do Not Like", Chung-Ang-Bub-Hak (Korean) <http://www.kci.go.kr/kciportal/ci/sereArticleSearch/ciSereArtiView.kci?sereArticleSearchBean.artiId=ART001387276>
17) Constitutional Court 2012.5.31 Decision 2010 Hun-ma 88

proven illegality can form the basis of liability, intermediary or primary. The Korean intermediary liability regime will impose liability for only a provisional illegality if it takes place on the Internet. This constitutes discrimination against the Internet as a medium. Now, it is not a frivolous question how humanity should deal with the special characteristics of the Internet, which calls for more research.

[Note: The National Assembly is currently considering a bill to amend Article 44-2 whereby, if posters demand restoration, the dispute goes into a mandatory mediation, and if the poster receives a favorable mediation decision and the complainant does not object or if the poster receives an unfavorable mediation decision and objects to it by filing a suit, the content is restored. However, the intermediary's initial obligation to temporarily remove all contents identified by complainants remains intact.]

인터넷의 특성과 임시조치 및 저작권 전송중단제도

인터넷의 특성과 임시조치 및 저작권 전송중단제도

박경신
kyungsinpark@korea.ac.kr

인터넷의 생명은 극단적으로 개인화된 소통 방식을 통해 모든 개인을 소통에 참여시킨다는 것이다. 모든 "나"는 누구의 허락과 감시 없이 모두에게 볼수있게 무언가를 올릴 수 있고, 모든 "나"는 누구의 허락과 감시없이 모두의 글을 보거나 다운받을 수 있다. 결국 인터넷은 이를 악용한 불법행위가 일어날 수 밖에 없다. 그러나 인터넷 소통의 공간을 연 사람에게 자신이 모르는 상태에서 일어날 수 있는 모든 침해에 대해 책임을 져야 한다는 생각은 결국 인터넷을 죽일 것이다. .

외국 vs. 한국

- 미국 DMCA Notice-and-Takedown("NTD");
- EU전자상거래지침
- 일본 프로바이더책임제한법

→ "사업자는 몰랐거나 NTD만 하는 한 제3자제공 정보에 대해 책임을 지지 않는다."
→ 불법정보에 대해서도 면책
→ 책임면제조항

- 대한민국 정보통신망법 및 저작권법

→ "사업자는 차단요청이 들어오면 무조건 임시조치/삭제를 할 책임이 있다."
→ 합법정보에 대해서도 삭제/임시조치의무
→ 책임부과조항

현행 규정, 무엇이 문제인가?

정보통신망법 제44조의2(정보의 삭제요청 등) ① 정보통신망을 통하여 일반에게 공개를 목적으로 제공된 정보로 사생활 침해나 명예훼손 등 **타인의 권리가 침해된 경우** 그 침해를 받은 자는 해당 정보를 취급한 정보통신서비스 제공자에게 침해사실을 소명하여 그 정보의 삭제 또는 반박내용의 게재(이하 "삭제등"이라 한다)를 요청할 수 있다.

② 정보통신서비스 제공자는 제1항에 따른 **해당 정보의 삭제등을 요청받으면 지체 없이 삭제·임시조치 등의 필요한 조치를** 하고 즉시 신청인 및 정보게재자에게 알려야 한다. 이 경우 정보통신서비스 제공자는 필요한 조치를 한 사실을 해당 게시판에 공시하는 등의 방법으로 이용자가 알 수 있도록 **하여야 한다**.

④ 정보통신서비스 제공자는 제1항에 따른 정보의 삭제요청에도 불구하고 권리의 침해 여부를 판단하기 어렵거나 이해당사자 간에 다툼이 예상되는 경우에는 해당 정보에 대한 접근을 임시적으로 차단하는 조치(이하 "임시조치"라 한다)를 할 수 있다. 이 경우 임시조치의 기간은 30일 이내로 한다.

⑥ 정보통신서비스 제공자는 자신이 운영·관리하는 정보통신망에 유통되는 정보에 대하여 **제2항에 따른 필요한 조치를 하면 이로 인한 배상책임을 줄이거나 면제받을 수 있다**.

헌법재판소(2012)

합법적인 정보도 요청이 들어오면 임시조치는 해야 한다.

그렇다면 1,2,4항에서 이미 의무로 정한 행위를 했다고 해서 6항에서 면책이라는 혜택을 주는 이유는 무엇인가?

현행 규정, 무엇이 문제인가?

저작권법 제103조 (복제 전송의 중단) (① 온라인서비스제공자(제102조제1항제1호의 경우는 제외한다. 이하 이 조에서 같다)의 서비스를 이용한 저작물등의 복제·전송에 따라 저작권, 그 밖에 이 법에 따라 보호되는 자신의 권리가 침해됨을 주장하는 자(이하 이 조에서 "권리주장자"라 한다)는 그 사실을 소명하여 온라인서비스제공자에게 그 저작물등의 복제·전송을 중단시킬 것을 요구할 수 있다. <개정 2011.6.30.>

② 온라인서비스제공자는 제1항에 따른 **복제·전송의 중단요구를 받은 경우에는 즉시** 그 저작물등의 복제·전송을 중단시키고 권리주장자에게 그 사실을 통보하여야 한다.

⑤온라인서비스제공자가 제4항에 따른 공지를 하고 제2항과 제3항에 따라 그 저작물등의 복제·전송을 중단시키거나 재개시킨 경우에는 다른 사람에 의한 저작권 그 밖에 이 법에 따라 보호되는 권리의 침해에 대한 온라인서비스제공자의 책임 및 복제·전송자에게 발생하는 손해에 대한 **온라인서비스제공자의 책임을 면제한다.**

→?? 2항에서 이미 의무로 정한 것을 해놓았는데 5항에서 책임면제라는 혜택을 주는 이유는??

결과: 사적 검열

- 2012년 100,000건 임시조치 (한국) vs. 2,000 (구글, 세계)
- 서울시장 오세훈의 서울광장 집회불허 비판한 글
- 주영성 의원의 술버릇과 소셜계정 소개한 글
- 서울경찰청장의 동생이 부산에서 불법윤락업소와 연계된 호텔을 운영하다는 텔레비전보도 영상
- 용산참사 희생자를 비하한 정치인 발언을 비난한 글
- 노동자파업에 대해 형사처벌과 손배소를 면할 것을 주장한 글
- 장자연-조선일보 의혹 제기한 야당정치인의 글

Session 1

Safe Harbor (other parts of the world) vs. Limited Liability (Korea)

정보매개자 책임에 대한 이해
(임시조치 등)

Main Speaker / 주제 발표

Urs Gasser
어스 개서

▪ Director of the Berkman Center and
Professor of Practice at Harvard Law School

Urs Gasser is the Executive Director of the Berkman Center for Internet & Society at Harvard University and a Professor of Practice at Harvard Law School. He is a visiting professor at the University of St. Gallen (Switzerland) and at KEIO University (Japan), and he teaches at Fudan University School of Management (China). Urs Gasser serves as a trustee on the board of the NEXA Center for Internet & Society at the University of Torino and on the board of the Research Center for Information Law at the University of St. Gallen, and is a member of the International Advisory Board of the Alexander von Humboldt Institute for Internet and Society in Berlin. He is a Fellow at the Gruter Institute for Law and Behavioral Research. Dr. Gasser has written and edited several books, and published over 100 articles in professional journals. He is the co-author of "Born Digital: Understanding the First Generation of Digital Natives" (Basic Books, 2008, with John Palfrey) that has been translated into 10 languages (including Chinese), and co-author of "Interop: The Promise and Perils of Highly Interconnected Systems" (Basic Books, 2012, with John Palfrey). Urs Gasser's research and teaching activities focus on information law, policy, and society issues. Current projects – several of them in collaboration with leading research institutions in the U.S., Europe, and Asia – explore policy and educational challenges for young Internet users, the regulation of digital technology, ICT interoperability, information quality, the law's impact on innovation and risk in the ICT space, cybersecurity, and alternative governance systems. He graduated from the University of St. Gallen (lic.iur., Dr.iur.) as well as Harvard Law School (LL.M. '03) and received several academic awards and prizes for his research, including Harvard's Landon H. Gammon Fellowship for academic excellence and the "Walther Hug-Preis Schweiz", a prize for the best doctoral theses in law nationwide, among others.

Case Study Speaker/ 특별 토론

Naoko Mizukoshi
나오코 미즈코시

▪ Founder/Partner at Endeavor Law Office

Ms. Mizukoshi is an attorney and Founder/Partner at Endeavour Law Office. Since admitted to practice in Japan in 1995, and in the State of California in 2002, she has been advising a variety of corporate clients from large multi-nationals to small start-ups with her deep expertise in Intellectual Property, Information Technology, and Entertainment. Ms. Mizukoshi possesses a unique combination of experiences both as a partner lawyer at one of the largest law firms in Japan as well as an in-house lawyer at global corporations. Before co-founding Endeavour Law Office in 2010, she was a Partner at TMI Associates. Prior to that, she served as an in-house lawyer at Microsoft, Autodesk, and Nomura Research Institute.

Moderator / 좌장

Park, K.S.
박경신

▪ 1995	J.D. 법학박사	UCLA Law School 미국 UCLA 로스쿨
▪ Present	Professor 교수	Korea University Law School 고려대학교 법학전문대학원
▪ Present	Director 이사	Open Net (사)오픈넷
▪ Present	국제이사 Director of Int'l Relations	Korea Association of Legal Philosophy 한국법철학회
▪ Present	Executive Director 소장	PSPD Law Center 참여연대 공익법센터
▪ Present	Legal Advisor 법률자문위원	Int'l Relations, Korean film Council 한국영화진흥위원회 국제진흥팀

Panelists / 토론자

Kwon, Youngjoon
권영준

▪ 2006	Ph.D. 박사	Graduate School of Law, Seoul National University 서울대학교 법과대학
▪ 2004	LL.M. 법학석사	Harvard Law School 하버드대학교 로스쿨
▪ 2000	M.A. 석사	Graduate School of Law, Seoul National University 서울대학교 법과대학
▪ Present	Professor 교수	Seoul National University Law School 서울대학교 법학전문대학원
▪ Present	Director 센터장	Law and Technology Center, Seoul National University 서울대학교 기술과법 센터
▪ Present	Member 위원	Int'l Trade Law Research Group, Ministry of Justice 법무부 국제거래연구단
▪ Present	Editor of Copyright 편집위원	Korea Copyright Commission 한국저작권위원회

Panelists / 토론자

Kim, Yoo Hyang
김유향

▪ –	Ph.D. 박사	Political Science, Ewha Women's University 이화여자대학교 정치학
▪ Present	Head 팀장	Science, Media and Telecommunications Team, NARS 국회입법조사처 방송통신팀
▪ Present	Adjunct Professor 겸임교수	University of North Korean Studies 북한대학원대학교 IT/경제전공

Panelists / 토론자

Jung, Kyung Oh
정경오

▪ 2011	Graduate 수료	Administrative Law, Chung Aung University Law School 중앙대학교 법학전문대학원 행정법
▪ Present	Attorney at Law 변호사	Hanjung Partners 법무법인 한중
▪ 2008 ~ 2014	Senior Research Fellow 책임연구원	Korea Information Development Institute 정보통신정책연구원
▪ 2008	Advisory Member 전문위원	Korea Communication Standard Commission 방송통신심의위원회
▪ 2005 ~ 2008	Director 심의실장	Korea Internet Safety Commission 정보통신윤리위원회

Main Speaker / 주제발표

Online Intermediaries Project : Findings and Recommendations

Prof. **Urs Gasser**
(Harvard Berkman Center for Internet and Society)

온라인 정보매개자 프로젝트 : 연구결과와 제안

어스 개서 교수 (미 하버드대, 버크맨센터 소장)

Governance of Online Intermediaries: Observations From A Series Of National Case Studies

IV. Role of the Government (p. 9 ~ 14)

The case studies reveal that governments – in addition to technological and market factors – are among the most important forces that shape the online intermediary landscape of a given country. The respective roles government can play are rather diverse and often overlapping, ranging from “governments as users” to “governments as regulators” of intermediaries. Focusing on the latter, the case studies demonstrate that, even within the role of the government as a regulator of online intermediaries, we can find important functional nuances in terms of different manifestations and interpretations of this role. Further, the case studies suggest that different institutions within the government might be involved in the respective online intermediaries governance regime, depending on the underlying regulatory model and strategy (see previous section). In some countries, government agencies are the key regulators; other governance regimes heavily rely on Courts. The analysis also points to structural similarities and differences among the case studies when it comes to the specific approach to compliance and enforcement, ranging from emphasis on

technical means to licensing requirements. The following paragraphs highlight some of the key findings in each of these issue areas.

a Functions

The case study series reveals that governments have varying motives for regulating online intermediaries. In broad terms of regulatory theory,[1] the primary reasons to intervene and regulate might have to do with externalities (e.g. compelling online intermediaries to bear the full costs of service rather than pass on to third parties), can be motivated by the desire to ensure certain levels of "essential" services (e.g. creation of and access to a diverse information ecosystem with multiple sources), or may be aimed at balancing unequal bargaining power (e.g. to protect vulnerable interests or populations, such as children), to name just a few examples. Viewed from a broader functional angle, however, the case studies suggest that the majority of governance models outlined above fall into three in practice overlapping but nonetheless analytically distinct categories: enabling, leveling, or constraining.

The most prominent example where the governance model serves largely the function of an enabler is the U.S. legal framework. As already mentioned above and described in detail in the respective country case study,[2] the U.S. framework is characterized by extensive safe harbors that dramatically limit the liability exposure of online intermediaries. The case study analysis and various other (including empirical) studies suggest that this particular governance arrangement has enabled the flourishing and growth of online intermediaries in the U.S. and, as a result, promoted the functions performed by online intermediaries.[3] While the historic motives for introducing these liability limitations were rather nuanced (in the case of the U.S. Communications Decency Act [CDA], for instance, the lawmaker wanted to enable content self-regulation by online intermediaries without exposing them to liability),[4] contemporary policy debates refer to this enabling function largely in relation to either economic benefits (e.g. incentives to innovate without fear of liability) or in the context of fundamental rights (e.g. elimination of chilling effects).[5]

Another function that online intermediary governance models (in general) and liability regimes (in particular) can perform is the role of a leveler. Traces of such a leveling function can be found in several countries with notice-and-takedown systems where the governance model is targeting online intermediaries as "the in between" to strike a balance between the interests of different parties, for instance between copyright owners and users in the realm of copyright. The CJEU's right to be delisted decision might be seen as another manifestation of such an approach, aimed at leveling the playing field ("fair balance" in the words of the CJEU) between the legitimate interests of the Internet users potentially interested in having access to information and the data subject's fundamental rights. As these two examples indicate, the leveling function of online intermediary governance models can either be implemented through a (generalized) rule such as a DMCA-style notice-and-takedown mechanism, or based on a standard that requires a case-by-case analysis, as in the case of the CJEU's right to be delisted decision.

Third, governance models – especially in the form of liability regimes in the context of this study – typically perform a constraining function by ordering online intermediaries to take specific action or implement certain measures. Even leveling regimes often perform a constraining function, as in the case of notice-and-take-

1) See generally, e.g., Baldwin, Robert, and Martin Cave. Understanding Regulation: Theory, Strategy, and Practice. Oxford: Oxford University Press, 1999.
2) Holland, Adam, Chris Bavitz, Jeff Hermes, Andy Sellars, Ryan Budish, Michael Lambert, and Nick Decoster. "Online Intermediaries Case Studies Series: Intermediary Liability in the United States", The Global Network of Internet & Society Research Centers (2015).
3) See, e.g., Bramble, Nicholas. "Safe Harbors and the National Information Infrastructure." Hastings Law Journal 64, no. 325 (2013). http://www.hastingslawjournal.org/wp-content/uploads/2014/04/Bramble-64.2.pdf.
4) Cannon, Robert. "The Legislative History of Senator Exon's Communications Decency Act: Regulating Barbarians on the Information Superhighway." Federal Communications Law Journal 51 (1996). http://www.cybertelecom.org/cda/cannon2.htm.
5) See, e.g., Bankston, Kevin, David Sohn, and Andrew McDiarmid "Shielding the Messengers: Protecting Platforms for Expression and Innovation." Center For Democracy and Technology. December 2012. https://www.cdt.org/files/pdfs/CDT-Intermediary-Liability-2012.pdf. But see Seltzer, Wendy. "Free Speech Unmoored in Copyright's Safe Harbor: Chilling Effects of the DMCA on the First Amendment." Harvard Journal of Law & Technology 24 (2010): 171. http://jolt.law.harvard.edu/articles/pdf/v24/24HarvJLTech171.pdf.

down regimes where online intermediaries have to meet certain obligations in order to benefit from safe harbor protection. But the case studies have also revealed situations where the constraining effects are more specific or targeted. In the case of Thailand, for instance, the law directly imposes content liability on online intermediaries to preserve the public order (lèse majesté)[6] or enable the control of the flow of information (through censorship and surveillance) under the coup-ruled government. Blocking statutes such as the Turkish Internet Law are highly visible and controversial examples where law serves predominantly a constraining function in the online intermediaries space.[7] The licensing regime in Vietnam imposes hard constraints under which online intermediaries have to operate, to give another example from the case study series.[8]

b Branches

Looking at the role of governments as regulators, the case studies show that different branches of the government may serve as core pillars of a given online intermediary governance system. The series also demonstrates that the basic layout and different degrees of government involvement lead to key questions regarding incentives, legitimacy, accountability, and transparency. In addition to these fundamental issues, the case studies also hint towards a rather underexplored dimension of the governance problem: the role of knowledge when it comes to the regulation of online intermediaries, as such expertise – for instance with respect to the understanding of how different types of intermediaries technically work – might be distributed unequally across the different branches of the government that are involved in the respective governance models.

6) Ramasoota, Pirongrong. "Online Intermediaries Case Studies Series: Online Intermediary Liability in Thailand", The Global Network of Internet & Society Research Centers (2015), 4.
7) Beceni, Yasin and Nilay Erdem. "Online Intermediaries Case Studies Series: Turkey (eBay Case)", The Global Network of Internet & Society Research Centers (2015).
8) Nguyen, Thuy. "Online Intermediaries Case Studies Series: Roles and Liabilities of Online Intermediaries in Vietnam – Regulations in the Mixture of Hope and Fear", The Global Network of Internet & Society Research Centers (2015).

Most of the governance models studied in the context of this research project heavily rely on the Court system to put these models aimed regulating online intermediaries into practice. Until the recent enactment of the Marco Civil, Brazil was among the countries where online intermediary governance almost entirely resided in the realm of Courts. An alternative type of regime puts emphasis on government agencies when it comes to online intermediaries. With respect to non-copyright issues, Korea is an example where a government agency, in form of the Korean Communication Standards Commission, plays an important role within the intermediary governance framework.[9] An extreme version of a government agency-based governance regimes are countries with licensing requirements. In Vietnam, for instance, the providers of online social networking sites and general news websites have to obtain a license from the government before offering such services.[10]

Court-centric regimes are characteristic for democratic countries, while agency-focused intermediary governance frameworks are more prevalent in countries with limited rule of law. The U.S. governance system with its heavy reliance on Courts is at one end of the spectrum in the case study series, while Thailand with its tight control over online intermediaries through the National Council for Peace and Order marks the other.[11] Further, Court-based governance regimes play a particularly important role with respect to copyright issues, as even some countries with relatively strong government agency involvement in non-copyright issues refer to Courts in this area, as the case of Korea illustrates.[12]

9) Park, Kyung-Sin. "Online Intermediaries Case Studies Series: Intermediary Liability – Not Just Backward but Going Back", The Global Network of Internet & Society Research Centers (2015).
10) Nguyen, Thuy. "Online Intermediaries Case Studies Series: Roles and Liabilities of Online Intermediaries in Vietnam – Regulations in the Mixture of Hope and Fear", The Global Network of Internet & Society Research Centers (2015), 3
11) See Holland, Adam, Chris Bavitz, Jeff Hermes, Andy Sellars, Ryan Budish, Michael Lambert, and Nick Decoster. "Online Intermediaries Case Studies Series: Intermediary Liability in the United States", The Global Network of Internet & Society Research Centers (2015); and Ramasoota, Pirongrong. "Online Intermediaries Case Studies Series: Online Intermediary Liability in Thailand", The Global Network of Internet & Society Research Centers (2015).
12) Park, Kyung-Sin. "Online Intermediaries Case Studies Series: Intermediary Liability – Not Just Backward but Going Back", The Global Network of Internet & Society Research Centers (2015).

But even in countries with largely Court-centric regimes lines might be blurring. While U.S. intermediary governance heavily relies on Courts, governmental agencies can play a prominent role at least when it comes enforcement, as the role of state government in the context of Section 230 CDA demonstrates.[13] Similarly, government agencies in the form of data protection authorities are important players in the EU when it comes to online intermediary governance.

c Enforcement

The previous sections already clearly illustrates that governments not only set the general – and at times specific – framework conditions under which online intermediaries operate, but are also instrumental when it comes to the implementation and enforcement of a given governance model. With respect to compliance and enforcement issues, a number of observations gained from the case study series are noteworthy.

At the most abstract level, the comparative analysis of different governance regimes indicates that the incentive structures created by the governments – whether by design or through mere practice – are key in understanding compliance with and enforcement of online intermediary governance frameworks. A key issue identified across the case studies is the question of whether a particular government creates a symmetric or asymmetric incentive structure for online intermediaries to take down content or leave it up in order to avoid liability. In the U.S., for instance, Section 230 CDA provides a symmetric incentive structure in the sense that Courts have been consistent about immunizing online intermediaries from liability as long as they did not author the content in question – whether they take it down, leave it up, or even restore content that was taken down.[14] In contrast, the governance models in India, Korea, and Thailand create asymmetric incentive structures, where intermediaries are incentivized to take down content in order to avoid liability, even if it results in over-compliance.[15]

A second observation related to asymmetric incentives and resulting compliance levels concerns local versus international online intermediaries. The case studies indicate that instances in which licensing requirements apply de facto only to local but not to international intermediaries lead to more compliance, or arguably even over-compliance, with government requests among these local intermediaries. The case study from Thailand is the most prominent example that highlights this asymmetry between local and international players.

Third, the case studies illustrate not only the different enforcement regimes and (e.g. ex post versus ex ante) strategies, including incentives and actors involved, but also indicate the range of enforcement techniques that can be utilized as part of the different governance models. The previous sections have already highlighted the role of licensing requirements as an enforcement tool, particularly in the cases of Turkey and Thailand.[16] Another interesting theme emerging from the case study analysis relates to the role of algorithms in enforcement. The phenomenon of computational compliance has become most visible in the context of the U.S. case study, where software plays a key role in dealing with large-scale problems of copyright infringement over user-created content platforms, specifically YouTube.[17] Algorithms not only play a role in "private ordering" a la YouTube, but also when it comes to government-imposed monitoring and filtering obligations, as the reports

13) Holland, Adam, Chris Bavitz, Jeff Hermes, Andy Sellars, Ryan Budish, Michael Lambert, and Nick Decoster. "Online Intermediaries Case Studies Series: Intermediary Liability in the United States", The Global Network of Internet & Society Research Centers (2015), 6.

14) Holland, Adam, Chris Bavitz, Jeff Hermes, Andy Sellars, Ryan Budish, Michael Lambert, and Nick Decoster. "Online Intermediaries Case Studies Series: Intermediary Liability in the United States", The Global Network of Internet & Society Research Center (2015), 5–7.

15) See Arun, Chinmayi, and Sarvjeet Singh. "Online Intermediaries Case Studies Series: Online Intermediaries in India", The Global Network of Internet & Society Research Centers (2015); and Ramasoota, Pirongrong. "Online Intermediaries Case Studies Series: Online Intermediary Liability in Thailand", The Global Network of Internet & Society Research Centers (2015).

16) See Beceni, Yasin and Nilay Erdem. "Online Intermediaries Case Studies Series: Turkey (eBay Case)", The Global Network of Internet & Society Research Centers(2015); and Ramasoota, Pirongrong. "Online Intermediaries Case Studies Series: Online Intermediary Liability in Thailand", The Global Network of Internet & Society Research Centers (2015).

17) Holland, Adam, Chris Bavitz, Jeff Hermes, Andy Sellars, Ryan Budish, Michael Lambert, and Nick Decoster. "Online Intermediaries Case Studies Series: Intermediary Liability in the United States", The Global Network of Internet & Society Research Centers (2015), 31–34.

from Thailand, Turkey, and India demonstrate.[18]

Finally, and related to the previous issues, the case studies point out the importance of costs, in terms of both money or time, when it comes to compliance and enforcement. Again, the role of cost is multi-faceted and context-specific. For instance, the Turkish case study demonstrates that uncertainties surrounding the notice-and-take-down system and the fact that a criminal proceeding can be launched without costs leads to a preferred activation of the judicial system over private mechanisms.[19] The contrast between automated compliance and enforcement in response to copyright issues on YouTube, versus the human and labor-intense review of takedown requests that attempt to balance user interests under the CJEU's right to be delisted, highlights yet another important dimension of the cost argument when it comes to online intermediary governance.

VI. Conclusion (p.16 ~ 18)

a Summary

A review of online intermediary governance frameworks and issues in Brazil, the European Union, India, South Korea, the United States, Thailand, Turkey, and Vietnam creates a picture full of nuance, whether looking at the genesis of intermediary frameworks, the reasons for intervention, or the specifics of the respective governance models, including strategies, institutions, modalities, and the effects of regulation,

18) See Ramasoota, Pirongrong. "Online Intermediaries Case Studies Series: Online Intermediary Liability in Thailand", The Global Network of Internet & Society Research Centers (2015); and Beceni, Yasin and Nilay Erdem. "Online Intermediaries Case Studies Series: Turkey (eBay Case)", The Global Network of Internet & Society Research Centers (2015); and Arun, Chinmayi, and Sarvjeet Singh. "Online Intermediaries Case Studies Series: Online Intermediaries in India", The Global Network of Internet & Society Research Centers (2015).

19) Beceni, Yasin and Nilay Erdem. "Online Intermediaries Case Studies Series: Turkey (eBay Case)", The Global Network of Internet & Society Research Centers (2015), 13.

among other dimensions. The country case studies both highlight and illustrate the importance of cultural and political context, which is not only reflected in the respective legal norms aimed at regulating intermediaries, but also expressed through different views and perceptions regarding the social function of intermediaries. In some sense, the case studies and the way in which the authors tell the story themselves mirror the same context and diversity. Similarly, the importance of the socioeconomic context has become clearly visible. Many of the features of various intermediary governance models can hardly be understood without considering their economic context, in conjunction with demographic characteristics and shifts.

Despite context-sensitivity, certain categories, clusters, and patterns can be distilled from the various case studies and analyzed. As suggested in this synthesis document, online intermediary frameworks can be grouped and mapped based on a number of core criteria and dimensions. Specifically, and from a conceptual angle, the synthesis shows that there are three basic groups of countries, i.e. countries that lack a specific intermediary governance framework, countries with existing and differentiated specific frameworks, and countries with emerging frameworks. The discussion also reveals patterns with respect to the key drivers and motivations for specific regulations or governance, including "bad headlines", but also forces to be analyzed through the political economic methods. The analysis of the case studies further suggests that the governance models regulating online intermediaries are typically a case of context regulation, particularly when coming in the form of liability regimes. Against this backdrop, the analysis highlights the key role of incentives among the different actors that shape the intermediary landscape, and the interaction among them, when we seek to understand and evaluate the performance of alternative governance models or approaches.

In addition, the case studies have revealed a series of crosscutting and highly dynamic issue-specific challenges, including the problem of definition (what is an online intermediary?), the question of the different types of intermediaries, the design of notice-and-takedown systems, and the cost of compliance and enforcement, among other things. Zooming in on the role of governments, this case study analysis

suggests three basic functions that governments can serve, i.e. an enabling, leveling, or constraining. With a view to the basic institutional set-up of the different governance regimes, the surveyed countries either follow a Court-based system or heavily rely on government agencies in the context of the different regulatory strategies and techniques – with lines between the two models often blurring, depending on the issues at stake. The question of incentives also plays a decisive role when it comes to the analysis of compliance and enforcement issues, including the problem of over-compliance in the case of asymmetric regulation.

b Future Considerations

Both with respect to the conceptual and issue-specific analysis, the mapping exercise summarized in this paper is initially mostly of descriptive value and does not immediately lead to firm normative conclusions or "best practices". That said, a more robust description of the core elements of online intermediary governance frameworks and the various forces at play can lead not only to a deeper phenomenological understanding, but also highlight some of the key considerations and issues to be taken into account when designing, implementing, or reforming governance models for online intermediaries. Such a descriptive map can and must be enriched over time by a growing body of anecdotal, and in some instances even empirical, evidence regarding the performance of varying governance models and their impact on the digital economy and society at large.[20] In that spirit, the synthesis paper and the underlying case studies seek to contribute to a stronger evidence-base that might inform debates about "best practices" regarding online intermediary governance systems by documenting some of the key feature of such regimes.[21]

20) See, e.g., "Closing the Gap: Indian Online Intermediaries and a Liability System Not Yet Fit for Purpose." Accessed December 10, 2014. p. 31–35 https://globalnetworkinitiative.org/content/closing-gap-indian-onlineintermediaries-and-liability-system-not-yet-fit-purpose.

21) In this sense also see "The Manila Principles On Intermediary Liability: Version 0.9," December 1, 2014. https://docs.google.com/document/d/1kAkqgt3cRb65d8ik6vWYgpk6DYpP8ABA43ljgDiGOf8/edit?usp=sharing.

With these caveats in mind, we would like to highlight the following points from the case study analysis for consideration and further deliberation in the debates about the present and future governance of online intermediaries:

1. Understand the function and economics of intermediaries. Online intermediaries are a relatively recent phenomenon, and both a driver and mirror of structural changes in the information ecosystem. Functionally, online intermediaries challenge traditional notions of what qualifies as "intermediary": though online intermediaries are still not the source of content creation, they are increasingly involved in its dissemination, combination, etc. Consequently, much emphasis in legal and policy debates is currently on definitions and categorizations of intermediaries vis-à-vis existing laws and other norms. In addition to these definitional questions, the analysis highlights the importance of a deeper functional understanding of the roles of online intermediaries when seeking adequate regulatory frameworks. The same applies with regard to the economics of intermediaries, given the presence of strong network effects and two sided markets.

2. Emphasize the normative dimension of intermediary regulation. Recently, the interplay between intermediary liability and the digital economy has gained significant attention across jurisdictions. Even architects of systems with rather broad safe harbor regimes seem to be primarily focused on the economic benefit of lean intermediary regulation. While economic arguments are of course important in policy debates, one should equally emphasize the normative dimensions, especially the impact of different governance regimes on Human Rights. That the interest in access to information has no natural "guardian" marks a structural problem in that respect.

3. Analyze and evaluate the full range of regulatory mechanisms. The case studies show that intermediaries are regulated by different mechanisms, directly and indirectly, ex ante and ex post, through "hard" as well as "soft" obligations. Different actors follow different approaches, have different types of resources at their disposal, and show different levels of expertise. In order to analyze, assess, and improve the state of regulation and its effects, it is key to take a holistic view and consider all of

these elements as well as their interplay (or lack thereof). A governance perspective is a helpful lens for such an analysis.

4. Consider the full costs of intermediary regulation. Given the complexity of the digital ecosystem, it is tempting for governments to target intermediaries. At the surface, interventions at the gateways of Internet communication seem to reduce the costs of regulation. The case studies suggest, however, that such a "window" comes with the risk of over-regulation, with a negative impact on users' fundamental rights, as well as on innovation and the digital economy. Research also suggests the importance of taking into account less visible costs of interventions, such as the risk of empowering already powerful intermediaries by forcing them to make content related choices.

5. Strengthen mechanisms of mutual learning. Despite all the nuances, the case studies also reveal commonalities and patterns among different governance regimes. In particular, the study highlights similar challenges among countries with notice-and-takedown systems, with problems like defining the requirements for notices, whether and how to inform the owner of the effected content, regulatory oversight, etc. At least with respect to public policy-makers, the analysis suggests a great potential for transnational learning, complementing the increased sophistication of the operators of intermediaries, who tend to take a global perspective when designing their internal governance regimes.

온라인 매개자 거버넌스: 국가 사례 연구를 통한 조사

Ⅳ. 정부의 역할 (p. 9 ~ 14)

사례연구 결과 기술과 시장 요소뿐 아니라 정부도 해당 국가의 온라인 매개 지형을 형성하는 주요 동력 중 하나라는 사실이 드러났다. "사용자로서의 정부"에서부터 매개자들의 "규제자로서의 정부"에 이르기까지 정부가 할 수 있는 역할은 다양하고 종종 중복된다. 온라인 매개자들의 규제자라는 역할 내에서도 구현과 해석에 따라 다양하고 주요한 기능들이 있다는 점을 사례연구는 보여주었다. 또한, 기본적인 규제 모델과 전략(제3절 참조)에 따라 정부 내 여러 기관들이 각각의 온라인 매개자 거버넌스 체제와 관련이 있음도 제시했다. 일부 국가에서는 정부 기관들이 주요 규제자들인 반면, 여타 거버넌스 체제는 법원에 크게 의존한다. 또한 법준수와 집행에 대한 구체적인 접근방식을 살펴보면 사례연구간에 구조적인 유사성과 차이점도 존재했는데, 기술적 수단을 강조하거나 인허가 요건에 집중하는 방식이 있을 수 있다. 이 같은 사안 분야별 주요 시사점들은 다음과 같다.

a 기능

이번 사례 연구는 정부들이 온라인 매개자들을 규제하는 동기가 다양하다는 사실을 보여준다. 개략적인 규제이론 차원에서 보면,[1] 개입과 규제의 주요 이유는 외부 요인(예: 온라인 매개자들이 전체 서비스 비용을 제3자에게 전가하기보다 책임지도록 하는 것)과 관련이 있거나, 특정 수준의 "필수" 서비스(예: 다양한 정보 생태계 형성 및 접근)를 확보하고자 하는 바람이 원인이 되거나, 불평등한 협상력의 균형을 맞추는(예: 아동과 같은 취약한 집단이나 집단의 이익 보호) 것을 목표로 할 수 있다. 하지만 보다 넓은 기능적 차원에서 들여다보면 이번 사례연구는 앞서 언급된 거버넌스 모델 대부분이 실제로 중복되지만 분석적인 측면에서는 뚜렷하게 구분되는 조력, 균등, 제약이라는 3가지 범주로 구분될 수 있음을 제시한다.

주로 조력자로서의 기능을 담당하는 거버넌스 모델로서 가장 대표적인 사례는 미국의 법률제도이다. 앞서 각 국가별 사례연구에서 구체적으로 설명한 바와 같이[2] 미국의 법률제도는 온라인 매개자들이 법적 책임에 노출되는 것을 극적으로 제한하는 넓은 피난처(safe harbors)로서의 특징을 갖는다. 사례 연구 분석 및 여타 여러 (실증) 연구를 보면 이 특정 거버넌스 제도는 미국에서 온라인 매개자들의 성장과 번영을 가능하게 했으며, 그 결과 온라인 매개자들이 수행하는 기능을 촉진해 왔다.[3] 이러한 법적 책임 제한을 도입한 애초의 동기는 지금과는 다소 달랐는데, 미 통신품위법(CDA)의 경우 의원들은 온라인 매개자들이 법적 책임에 노출되지 않고 컨텐츠를 자체적으로 규제하도록 만들고자 했다.[4] 하지만 오늘날 정책 논쟁에서 이러한 조력 기능은 경제적 효과(예: 법적 책임에 대한 두려움 없이 혁신에 매진하도록 하는 인센티브)나 기본권(예: 사기저하 방지)과 관련해 주로 언급된다.[5]

일반적인 온라인매개 거버넌스 모델과 구체적인 법적책임제도가 수행할 수 있는 또 다른 기능은 균등자로서의 역할이다. 이러한 균등화 기능의 흔적들은 통지 및 삭제(notice-and-takedown) 제도를 갖춘 일부 국가에서 찾을 수 있는데, 이 경우 거버넌스 모델은 저작권 분야에서 저작권자와 저작권 사용자 등 여러 당사자들의 이익간에 균형을 잡는 "중간자" 역할을 하는 온라인 매개자들을 대상으로 한다. 유럽사법재판소(CJEU)의 잊혀질 권리(right to be delisted) 판결은 이러한 접근방식의 또 다른 형태로 볼 수 있으며, 정보에 대한 접근권을 갖는데 관심을 가질 수 있는 인터넷 사용자의 정당한 이익과 정보 대상의 기본권 사이에 공평한 장(CJEU 용어로는 "공평한 균형")을 만드는 것을 목표로 한다. 이러한 두 가지 사례가 보여주듯이 온라인 매개자 거버넌스 모델의 균등화 기능은 미국의 디지털밀레니엄 저작권법(DMCA) 형태의 통지삭제제도 등 일반적인 규정이나 CJEU의 잊혀질 권리 사례와 같이 사례별 분석이 요구되는 기준에 따라 실행될 수 있다.

셋째, 본 연구에서 제시한 법적책임 제도 형태의 거버넌스 모델은 온라인 매개자들에게 특정 행동이나 조치를 취하도록 명령함으로써 통상적으로 제약 기능을 수행한다. 온라인 매개자들이 피난처 보호라는 혜택을 받기 위해 특정 의무를 다해야 하는 통지삭제제도의 경우와 마찬가지로 균등화 제도조차도 제약 기능을 종종 수행한다. 하지만, 제약 효과가 보다 구체적이고 특정된 상황들도 이번 사례연구는 보여준다. 예를 들어 태국 법률의 경우 쿠데타로 통치되는 정부하에 (검열 및 감시를 통해) 정보의 흐름을 통제하거나 공공질서(lèse majesté)를 보호하기 위해[6] 온라인 매개자에 컨텐츠에 대한 법적 책임을 직접 부과한다. 터키 인터넷법 등 차단 법령은 온라인 매개자 영역에서 법이 주로 제약 기능을 수행하는 가장 대표적인 사례로 논란이 되고 있다.[7] 베트남 인허가제도는 온라인 매개자들에게 운영상 엄격한 제약을 부여하는 또 다른 사례이다.[8]

1) 일반적으로 Baldwin, Robert와 Martin Cave 참조. 『규제 이해: 이론, 전략, 실행(Understanding Regulation: Theory, Strategy, and Practice)』, 옥스포드: 옥스포드대학교 출판사, 1999
2) Holland, Adam, Chris Bavitz, Jeff Hermes, Andy Sellars, Ryan Budish, Michael Lambert, Nick Decoster. "온라인 매개자 사례연구: 미국에서 매개자의 법적 책임", The Global Network of Internet & Society Research Centers (2015).
3) Bramble, Nicholas 참조. "피난처 및 국가정보인프라" 『Hastings Law Journal』 64, no. 325 (2013). http://www.hastingslawjournal.org/wp-content/uploads/2014/04/Bramble-64.2.pdf.
4) Cannon, Robert. "Exon 상원의원의 통신품위법 입법 역사: 정보 고속도로에서 야만인 규제하기" 『Federal Communications Law Journal 』51 (1996). http://www.cybertelecom.org/cda/cannon2.htm.
5) Bankston, Kevin, David Sohn, Andrew McDiarmid 참조, "메신저 보호: 표현과 혁신의 기반 보호" Center For Democracy and Technolocy. 2012.12. https://www.cdt.org/files/pdfs/CDT-Intermediary-Liability-2012.pdf, Seltzer, Wendy 참조 "저작권 피난처에서 벗어난 표현의 자유: 수정 제1조에 대한 DMCA의 찬물 끼얹기" 『Harvard Journal of Law & Technology』 24 (2010): 171. http://jolt.law.harvard.edu/articles/pdf/v24/24HarvJLTech171.pdf.
6) Ramasoota, Pirongrong. "온라인 매개자 사례연구: 태국의 온라인 매개자 법적 책임," The Global Network of Internet & Society Research Centers (2015), 4.
7) Beceni, Yasin, Nilay Erdem. "온라인 매개자 사례연구: 터키(이베이 사례)," The Global Network of Internet & Society Research Centers (2015).
8) Nguyen, Thuy. "온라인 매개자 사례연구: 베트남 온라인 매개자의 역할과 책임 – 희망과 공포과 혼재된 규제", The Global Network of Internet & Society Research Centers (2015).

b 정부 부처

규제자로서의 정부 역할을 살펴보면, 여러 정부 부처들이 해당 온라인 매개자 거버넌스 시스템에서 핵심 역할을 수행하는 사례들을 볼 수 있다. 또한 기본적이고 다양한 정부 관여 형태가 인센티브, 합법성, 책임, 투명성에 관련된 주요 문제들로 이어지고 있음을 알 수 있다. 이 같은 기본적인 문제뿐 아니라, 거버넌스 문제에서 다소 덜 다뤄진 측면도 이번 사례에서 드러났는데 온라인 매개자 규제에 있어 지식의 역할이다. 예를 들어 얼마나 다양한 종류의 매개자들이 실제 운영중인지를 이해하는 것과 관련해, 각 거버넌스 모델에 관여하는 정부 부처별로 전문성이 균일하지 않을 수 있다는 것이다.

본 연구에서 조사된 거버넌스 모델 대부분은 규제 대상이 되는 이러한 모델을 실행에 옮기는데 있어 법원 시스템에 크게 의존하고 있다. 최근 마르코 시빌(Marco Civil)법이 제정되기까지 브라질은 온라인 매개자 거버넌스가 거의 전적으로 법원 영역에 맡겨진 국가들 중 하나였다. 또 다른 온라인 매개자 거버넌스 형태로 정부 기관에 의존하는 모델이 있다. 비저작권 사안에 있어서 한국은 정부기관인 방송통신심의의원회가 매개자 거버너스 제도에 있어 주요한 역할을 하는 예이다.[9] 정부 기관에 기반한 거버넌스 제도 중 극단적인 형태는 인허가 요건이 있는 국가들이다. 예를 들어 베트남에서 SNS 및 일반 뉴스 웹사이트 제공업체들은 해당 서비스 제공을 위해 사전에 정부의 인허가를 취득해야 한다.[10]

법원 중심 체제는 민주주의 국가들에서 주로 찾아볼 수 있는 반면, 정부기관 중심 매개자 거버넌스 제도는 제한적인 법치국가들에서 보다 일반적이다. 미국의 거버넌스 체제는 일련의 연구 사례 중 법원에 가장 크게 의존하는 형태이며, 태국의 경우는 국가 평화질서위원회를 통해 온라인 매개자들을 엄격하게 관리하는 형태로 가장 정부기관 중심의 형태를 지니고 있다.[11] 또한, 법원중심 거버넌스 체제는 특히 저작권 문제에 있어 주요한 역할을 하는데 비저작권 문제에 있어 비교적 강력한 정부 기관 개입형태를 보이는 일부 국가들도 이 분야에서는 법원에 의존하며, 이는 한국의 사례에서 보여진다.[12]

9) 박경신. “온라인 매개자 사례연구: 매개자 책임 – 후진이 아닌 후퇴”, The Global Network of Internet & Society Research Centers (2015).
10) Nguyen, Thuy. “온라인 매개자 사례연구: 베트남 온라인 매개자의 역할과 책임 – 희망과 공포과 혼재된 규제”, The Global Network of Internet & Society Research Centers (2015), 3.
11) Holland, Adam, Chris Bavitz, Jeff Hermes, Andy Sellars, Ryan Budish, Michael Lambert, Nick Decoster 참조. “온라인 매개자 사례연구: 미국에서 매개자의 법적 책임,” The Global Network of Internet & Society Research Centers (2015); Ramasoota, Pirongrong. “온라인 매개자 사례연구: 태국 온라인 매개자의 법적 책임,” The Global Network of Internet & Society Research Centers (2015).
12) 박경신. “온라인 매개자 사례연구: 매개자 책임 – 후진이 아닌 후퇴”, The Global Network of Internet & Society Research Centers (2015).

하지만 법원 중심적인 제도를 갖춘 국가들의 경우에도 경계선이 모호할 수 있다. 미국의 매개자 거버넌스는 법원에 크게 의존하지만, CDA제230절의 주정부 역할에서 볼 수 있듯이 정부 기관들이 법집행에서 주요 역할을 수행할 수 있다.[13] 이와 유사하게 EU에서는 데이터 보호 당국 형태의 정부 기관들이 온라인 매개자 거버넌스에 있어 주요한 역할을 하고 있다.

c 법집행

앞서 살펴본 바와 같이 정부들은 온라인 매개자들을 운영하는 일반 혹은 특정 제도의 조건들을 수립할 뿐 아니라 해당 거버넌스 모델의 실행과 법집행에 있어 도구로서의 역할도 수행한다. 제도 준수와 집행문제와 관련하여 사례연구에서 파악된 사실들은 눈여겨볼 가치가 있다.

가장 추상적인 차원에서 다양한 거버넌스 체제의 비교 분석을 보면 정부가 설계나 실행을 통해 마련한 인센티브 구조는 온라인 매개자 거버넌스 제도의 준수와 실행을 이해하는데 있어 핵심이 된다. 사례연구 전반에 걸쳐 파악된 핵심 사안은 해당 정부가 온라인 매개자들이 책임을 피하도록 컨텐츠를 삭제하거나 놔두도록 하는 대칭 혹은 비대칭형 인센티브 구조를 만들었느냐는 것이다. 예를 들어 미국에서 CDA 제 230절은 대칭적인 인센티브 구조를 제공하는데, 법정은 온라인 매개자들이 문제가 되는 컨텐츠를 삭제하거나, 놔두거나, 삭제 후 복원하던지 간에 해당 컨텐츠를 직접 작성하지 않은 한 일관되게 법적 책임을 부과하지 않는다.[14] 이와 대조적으로 인도, 한국, 태국의 거버넌스 모델은 비대칭 인센티브 구조를 취하고 있는데, 과잉 준수가 되더라도 매개자들이 법적책임을 피하기 위해 컨텐츠를 삭제하도록 유인하고 있다.[15]

비대칭 인센티브와 이에 따른 제도 준수 수준에 관한 두 번째 발견 사항은 국내 및 국제 온라인 매개자들과 관련된 것이다. 사례연구를 보면 인허가 요건이 사실상 국제 매개자들을 제외한 국내 매개자들에게만 적용되는 경우 제도 준수 수준이 높거나 심지어 준수

13) Holland, Adam, Chris Bavitz, Jeff Hermes, Andy Sellars, Ryan Budish, Michael Lambert, Nick Decoster. “온라인 매개자 사례연구: 미국에서 매개자의 법적 책임,” The Global Network of Internet & Society Research Centers (2015), 6.
14) Holland, Adam, Chris Bavitz, Jeff Hermes, Andy Sellars, Ryan Budish, Michael Lambert, Nick Decoster. “온라인 매개자 사례연구: 미국 매개자의 법적 책임”, The Global Network of Internet & Society Research Centers (2015), 5–7.
15) Arun, Chinmayi, Sarvjeet Singh 참조. “온라인 매개자 사례연구: 인도의 온라인 매개자”, The Global Network of Internet & Society Research Centers (2015); Ramasoota, Pirongrong. “온라인 매개자 사례연구: 태국 온라인 매개자의 법적 책임”, The Global Network of Internet & Society Research Centers (2015).

과잉으로 이어진다는 것을 알 수 있다. 태국이 국내와 국제 매개자들간의 이 같은 비대칭을 가장 잘 보여주는 사례이다.

셋째, 사례연구를 통해 인센티브와 관련된 행위자 등 여러 실행제도 및 (예: 사후 vs. 사전) 전략 등을 제시됐을 뿐 아니라 다양한 거버넌스 모델의 일환으로 활용될 수 있는 여러 실행 기법도 살펴볼 수 있었다. 앞서 실행 도구로서의 인허가 요건을 살펴봤으며 터키와 태국이 이를 가장 잘 보여주는 사례였다.[16] 또 다른 사례분석을 통해 도출한 흥미로운 주제는 제도 실행에서 알고리즘의 역할에 관한 것이다. 컴퓨터를 통한 제도 준수 현상은 미국 사례에서 가장 잘 나타나는데, 유튜브 등 UCC 컨텐츠 사이트가 저작권을 위반하는 대규모 문제를 처리하는데 있어 소프트웨어가 주요한 역할을 한다.[17] 알고리즘은 유튜브에서 "개별 명령" 역할을 수행할 뿐 아니라 태국, 터키, 인도 사례와 같이 정부가 부과하는 모니터링과 여과 기능도 수행한다.[18]

마지막으로 앞서 언급된 문제와 관련해 사례연구들은 제도의 준수와 실행에 있어 돈과 시간 모두에서 비용의 중요성을 보여준다. 비용의 역할은 다양하며 컨텐츠별로 다르다. 예를 들어 터키 사례를 보면 통지삭제제도를 둘러싼 불확실성과 비용없이 형사소송절차에 착수할 수 있다는 사실은 민간제도보다 사법 제도의 선호로 이어진다는 사실을 알 수 있다.[19] 유튜브상의 저작권 문제에 대한 자동 준수 및 실행방식과 CJEU잊혀질 권리(right to be delisted)하의 사용자 이익의 균형을 맞추고자 많은 인력을 들여 삭제 요청을 검토하는 방식간의 대조는 온라인 매개자 거버넌스에 있어 비용이라는 또 다른 주요한 측면을 강조한다.

16) Beceni, Yasin, Nilay Erdem 참조. "온라인 매개자 사례연구: 터키(이베이 사례)", The Global Network of Internet & Society Research Centers(2015); Ramasoota, Pirongrong. "온라인 매개자 사례연구: 태국 온라인 매개자의 법적 책임", The Global Network of Internet & Society Research Centers (2015).

17) Holland, Adam, Chris Bavitz, Jeff Hermes, Andy Sellars, Ryan Budish, Michael Lambert, Nick Decoster. "온라인 매개자 사례연구: 미국 매개자의 법적 책임," The Global Network of Internet & Society Research Centers (2015), 31–34.

18) Ramasoota, Pirongrong 참조. "온라인 매개자 사례연구: 태국의 온라인 매개자 법적 책임," The Global Network of Internet & Society Research Centers (2015); Beceni, Yasin, Nilay Erdem. "온라인 매개자 사례연구: 터키(이베이 사례)", The Global Network of Internet & Society Research Centers (2015); Arun, Chinmayi, Sarvjeet Singh. "온라인 매개자 사례연구: 인도의 온라인 매개자", The Global Network of Internet & Society Research Centers (2015).

19) Beceni, Yasin, Nilay Erdem. "온라인 매개자 사례연구: 터키(이베이 사례)", The Global Network of Internet & Society Research Centers (2015), 13.

VI. 결론 (p.16 ~ 18)

a 요약

브라질, EU, 인도, 한국, 미국, 태국, 터키, 베트남은 기본제도 수립, 개입 이유 및 전략, 기관, 세부 원칙, 규제 효과 등 기타 거버넌스 모델별 세부사항 등에 있어 다양한 온라인 매개자 거버넌스 제도를 수립했다. 국가별 사례연구를 통해 문화적 정치적 맥락의 중요성을 이해할 수 있었으며, 이러한 요소들은 매개자들을 규제하기 위한 각 법적 기준에 반영되어 있을 뿐 아니라 매개자들의 사회적 기능과 관련해 다양한 견해와 인식을 통해 표현되었다. 어떤 면에서 사례연구와 컨텐츠 작성자들이 말하는 방식은 이와 동일한 맥락과 다양성을 보여준다. 마찬가지로, 사회경제적 맥락의 중요성은 분명하게 드러난다. 다양한 매개자 거버넌스 모델들의 특징 대부분은 인구통계학적 특성 및 변화와 함께 경제적 맥락을 고려하지 않고 이해될 수 없다.

이처럼 맥락이 중요하지만, 다양한 사례연구를 통해 특정한 분류, 군집, 패턴을 도출하고 분석할 수 있었다. 본 종합 논문에서 제시된 바와 같이 온라인 매개자 제도는 다양한 핵심 기준과 요소를 기반으로 분류하고 매핑(mapping)해 볼 수 있다. 보다 구체적으로 개념적인 관점에서 본다면 국가들은 3개의 기본 그룹으로 분류될 수 있다. 즉, 매개자 거버넌스 세부 제도가 없는 국가, 다양하고 구체적인 제도를 갖춘 국가, 제도를 만들어 가는 국가로 나눌 수 있다. 또한, "부정적 보도" 등 구체적인 규제나 거버넌스의 주요 동인과 동기에 있어 일정한 패턴도 파악되었으며, 정치경제적 방법을 통해 분석도 가능하다. 사례연구 분석을 통해 온라인 매개자들을 규제하는 거버넌스 모델은 통상적으로 맥락적인 규제에 해당된다는 점을 알 수 있는데, 이는 책임체제 형태로 구현된다. 이 같은 상황에서 여러 거버넌스 모델이나 접근방식의 성과를 이해하고 평가할 때, 매개자들의 지형을 형성하는 다양한 행위자들간에 인센티브가 하는 주요한 역할과 이들간의 상호작용이 분석을 통해 파악되었다.

또한, '온라인 매개자는 무엇인가'라는 정의의 문제 등 다양한 매개자 종류, 통지삭제 시스템 설계, 제도 준수 및 실행 비용 등 역동적이고 다양한 분야에 걸친 문제별 도전과제도 사례연구를 통해 파악할 수 있었다. 정부 역할을 들여다보면 정부가 할 수 있는 조력, 균등, 제약이라는 세가지 기본 기능을 본 사례연구는 제시한다. 다양한 거버넌스 체제의 기본 제도 수립 측면에서 연구대상 국가들은 여러 규제 전략 및 기법에 따라 법정기반 시스템을 따르

거나 정부 기관에 과도하게 의존하는데, 사안에 따라 이 두 가지 모델간 경계선이 불분명한 경우가 많다. 또한 비대칭 규제의 경우 준수 과잉 등 제도 준수 및 실행 문제에 있어서 인센티브가 결정적인 역할을 한다.

b 향후 고려사항

개념 및 사안별 분석 모두에서 본 논문에 요약된 맵핑 방식은 설명적이며, 확고한 규범적 결론이나 "모범사례"를 즉각 도출하지는 않는다. 온라인 매개자 거버넌스 제도의 핵심 요소와 다양한 작용 동인들을 보다 적극적으로 설명하면 현상을 심도있게 이해할 수 있을 뿐 아니라 온라인 매개자 거버넌스 모델을 설계, 실행, 재편할 때 고려해야 하는 주요 사항과 사안도 확인할 수 있다. 이처럼 설명적인 매핑은 여러 상황을 거쳐 풍부해질 수 있으며, 다양한 거버넌스 모델의 성과와 나아가 디지털 경제와 사회에 미치는 영향에 관한 실증적인 증거도 반영할 수 있다.[20] 이런 측면에서 본 종합 논문과 기본 사례연구는 온라인 매개자 거버넌스 체제의 주요 특징을 문서화하여 "모범 사례"에 대한 정보를 제공할 수 있는 강력한 증거 기반에 기여하고자 한다.[21]

이 같은 사항들을 고려하여 현재 및 향후의 온라인 매개자 거버넌스에 관한 논쟁에서 고려사항 및 추가 도출사항을 다음과 같이 제시하고자 한다.

1. 매개자의 기능과 경제학 이해. 온라인 매개자들은 비교적 최근에 등장한 현상으로, 정보 생태계에서 구조적 변화를 주도하고 동시에 반영한다. 기능적으로 온라인 매개자들은 "매개자"로서의 자질이라는 전통적인 개념에 도전장을 내민다. 온라인 매개자들이 컨텐츠 창작원은 아니지만 컨텐츠의 배포, 통합 등에 갈수록 더 많이 관여한다. 이로 인해 법적 정책적 토론에서 기존 법률과 기타 기준상 매개인들의 정의 및 분류에 많은 중점을 두고 있다. 이러한 정의 문제뿐 아니라 적절한 규제를 마련할 때 온라인 매개자들의 기능을 심도있게 이해하는 것이 중요하다는 것을 사례 분석을 통해 알 수 있다. 강력한 네트워크 효과와 시장의 양면성을 고려할 때 매개자들의 경제학도 이와 마찬가지다.

20) "격차 줄이기: 인도의 온라인 매개자와 책임 제도는 목표 달성에 미흡" 참고, 2014.12.10, p. 31–35 https://globalnetworkinitiative.org/content/closing-gap-indian-onlineintermediaries-and-liability-system-not-yet-fit-purpose.

21) "온라인 매개자에 대한 필리핀의 원칙: 버전 0.9," 2014.12.1. https://docs.google.com/document/d/1kAkqgt3cRb65d8ik6vWYgpk6DYpP8ABA43IjgDiGOf8/edit?usp=sharing.

2. 매개자 규제의 규범적 측면 강조. 최근 매개자의 법적 책임과 디지털 경제사이의 상호작용은 여러 사법 관할권에서 상당한 관심을 끌었다. 광범위한 피난처 체제를 갖춘 시스템은 낮은 매개자 규제를 통해 경제적 효과를 얻는 것에 주로 집중하고 있는 구조를 갖춘 것으로 보인다. 경제적 주장이 정책 논쟁에서 중요하지만, 규범적 측면도 동일하게 강조되어야 하며, 인권에 대한 다양한 거버넌스 체제의 효과에 특히 주목해야 한다. 이런 점에서 정보 접근성에 대한 관심은 자연적인 "후견인"이 없다는 점은 구조적인 문제를 보여준다.

3. 모든 규제 기제의 분석 및 평가. 사례연구를 통해 매개자들이 다양한 제도에 따라 직간접적으로 사전 혹은 사후에 "엄격"하고 "너그러운"의무를 통해 규제를 받는다는 사실을 확인할 수 있었다. 여러 행위자들은 다양한 접근방식을 따르고 다양한 종류의 가용한 자원을 활용하며, 서로 다른 전문성 수준을 보여준다. 규제 현황과 효과를 분석, 평가, 개선하기 위해서는 종합적인 견해를 견지하고 이러한 모든 요소와 상호작용(혹은 상호작용 결여)을 고려하는 것이 핵심이다. 거버넌스 관점은 이러한 분석에 도움이 되는 도구이다.

4. 매개자 규제의 총비용 고려. 디지털 생태계의 복잡성을 고려하면 정부가 매개자들을 목표로 하는 것은 당연하다. 표면적으로 인터넷 통신 게이트웨이에 개입하는 것은 규제 비용을 낮출 수 있을 것으로 보인다. 하지만 사례연구를 보면 이러한 "개입"은 과잉 규제 위험을 수반하고 사용자의 기본권, 혁신, 디지털 경제에 부정적인 영향을 미친다. 또한 기존의 강력한 매개자들에게 컨텐츠 관련 선택을 강요함으로써 더 많은 권한을 주는 위험 등 비가시적인 개입 비용을 고려하는 것도 중요하다는 사실도 이번 연구를 통해 확인되었다.

5. 상호 학습 기제 강화. 여러 거버넌스 체제간 모든 차이에도 불구하고 보편성과 패턴이 존재한다는 것을 사례연구는 제시한다. 특히 통지삭제 시스템을 갖춘 국가들이 직면하고 있는 유사한 난제들도 보여주는데, 효력이 있는 컨텐츠 소유자, 규제 당국 등에 통지를 해야 하는지 여부와 어떻게 해야하는지 등 통지 요건 정의하는데 있어서 문제들이 있다. 적어도 공공 정책 입안자들과 관련해 본 사례분석은 고도의 초국가적인 학습 가능성을 제시하며, 이는 내부 거버넌스 체제를 설계할 때 국제적인 관점을 취하는 매개자 운영자들의 복잡성 증가를 보완한다.

Intermediary Liability Rules in Japan

Ms. **Naoko Mizukoshi**
(Partner, Endeavour Law Office)

일본의 정보매개자 책임 원칙

나오코 미즈코시 변호사 (일본 엔데버 법률사무소)

Case Study: Intermediary Liability Rules in Japan

Case Study: Intermediary Liability Rules in Japan

Naoko Mizukoshi
Endeavour Law Office

May 28, 2015

ENDEAVOUR
LAW OFFICE

Laws and Guidelines in relation to Intermediary Liability in Japan

- Act on the Limitation of Liability for Damages of Specified Telecommunications Service Providers and the Right to Demand Disclosure of Identification Information of the Senders (the "Act") was enacted in 2001
  - Covers all types of infringements, including without limitation, copyright and trademark infringement, defamation, and breach of privacy.
  - Applies to a "specified telecommunications service provider"
    - Including: bulletin board/website administrator, hosting service provider, and access provider
    - Not including: 1:1 communication (email, chat, messenger, etc.) provider
  - Article 3 regulates limitation of ISP's liability for damages (not safe harbor).
  - ISP does not owe liability unless it (i) knew the infringement, or (ii) had knowledge of information distribution and there is a reasonable ground to find that it could know the infringement.
  - Article 4 regulates sender's identification information disclosure requests

Laws and Guidelines in relation to Intermediary Liability in Japan (continued)

- Consultative meetings consisting of representatives from relevant industry associations created following guidelines
  - Guideline regarding Defamation and Breach of Privacy
  - Guideline regarding Copyright Infringement
  - Guideline regarding Trademark Infringement
  - Guideline regarding Sender's Identification Information Disclosure Request
- Guidelines describe the procedure to notify ISPs, the format to be used for notice, and recent ISP's standard practices based on judicial precedents.
- While not required by the Act, ISPs delete illegal information (e.g. obscenity, illegal drugs) subject to another guideline.

Review of Act and its Outcome

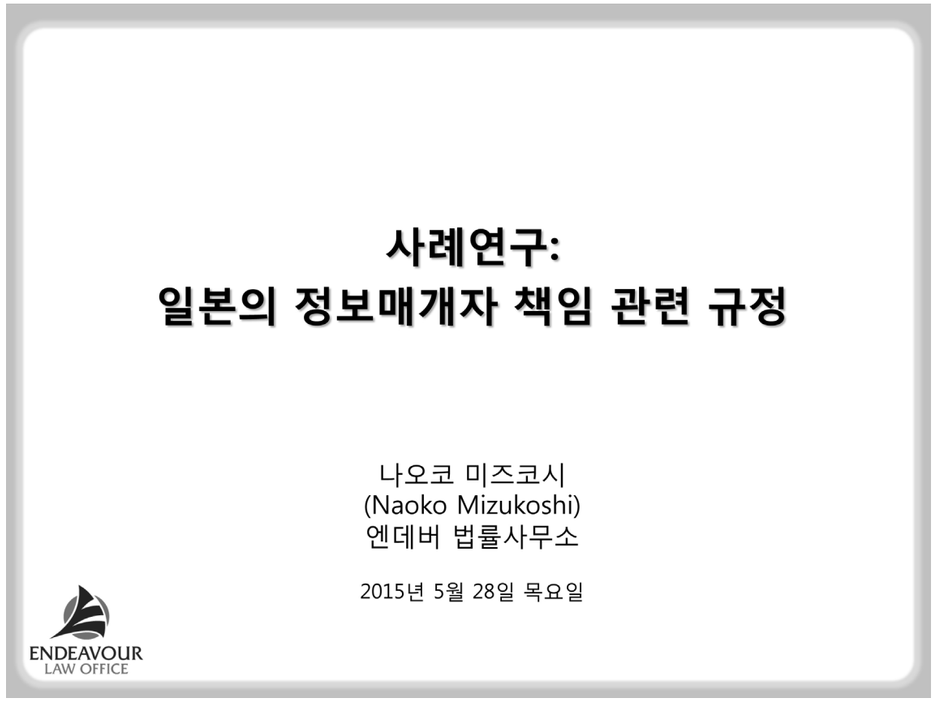
- The Act was reviewed from 2010 through 2011
- Despite many opinions were raised/discussed during the review, the decision was not to amend the Act.

  (examples of topics discussed)
  - Notice and Takedown
  - Three strikes
  - Reasonable measures
  - Monitoring obligation
- Some minor changes were made to the ministerial order to include items subject to the identification disclosure request (e.g., SIM card identification number).
- System in Japan
  - Merit: Stakeholders are collaborating based on guidelines.
  - Demerit: ISPs are at insecure position without safe harbor, i.e. no incentive for expeditious takedown. Copyright takedown could be done faster.

Naoko Mizukoshi
Endeavour Law Office
nmizukoshi@elaw.co.jp
http://english.elaw.co.jp/

ENDEAVOUR
LAW OFFICE

사례연구:
일본의 정보매개자 책임 관련 규정



일본의 정보매개자 책임 관련 법 및 가이드라인

- 특정전기통신역무제공자의 손해배상책임 제한 및 발신자정보의 개시에 관한 법률(이하 본 법)은 2001년에 제정됨
  - 저작권 및 등록상표권 침해, 명예훼손, 사생활 침해 등 모든 유형의 침해를 다룸
  - "특정전기통신역무제공자"에 적용
    - 해당: 게시판, 웹사이트 관리자, 호스팅서비스제공자, 및 접속서비스제공자
    - 제외: 1대1 커뮤니케이션(이메일, 채팅, 메신저 등) 서비스제공자
  - 제3조에서 ISP의 손해배상책임 제한을 규정(면책조항(safe harbor) 아님)
  - ISP는 (1) 침해에 대해 인지하였거나, 혹은 (2) 정보배포에 대한 지식을 갖고 불법성에 대해 알 수 있었을 합리적 근거가 있을 경우를 제외하면 책임이 없음
  - 제4조는 발신자의 신상정보에 대한 개시를 규정

일본의 정보매개자 책임 관련 법 및 가이드라인(이어서)

- 관련 산업계 협회 대표로 이루어진 자문회의에서 다음 가이드라인을 개발
  - 명예훼손 및 사생활침해 관련 가이드라인
  - 저작권 침해 관련 가이드라인
  - 등록상표권 침해 관련 가이드라인
  - 발신자 정보 개시 관련 가이드라인
- 가이드라인에는 ISP 통지 절차, 통지 양식, 판례에 기초한 ISP의 최신 표준관행에 대해 설명
- 본 법에서 요구하지는 않지만 ISP가 여타 가이드라인에 따라 불법정보(예: 음란물, 불법약물)를 삭제함

본 법과 그 성과에 대한 검토

- 2010년에서 2011년까지 개정 여부를 검토
- 검토기간 동안 수많은 의견이 개진/토론되었으나 본 법을 개정하지 않기로 함

  (토론된 주제의 예)
  - 통지 및 삭제 (Notice-and-Takedown)
  - 삼진아웃제(Three strikes)
  - 합리적 조치
  - 모니터링 의무
- 정보 개시 요청에 해당하는 항목을 포함시키기 위해 장관령이 일부 수정됨(예: SIM카드 번호)
- 일본의 제도
  - 장점: 이해관계자들이 가이드라인에 따라 협력
  - 단점: ISP는 면책 규정이 없어 불안정한 위치(신속한 삭제(takedown)에 대한 인센티브 부재) 저작권 침해물 삭제 속도 개선 필요

나오코 미즈코시
(Naoko Mizukoshi)
엔데버 법률사무소
nmizukoshi@elaw.co.jp
http://english.elaw.co.jp/

ENDEAVOUR
LAW OFFICE

Act on the Limitation of Liability for Damages of Specified Telecommunications Service Providers and the Right to Demand Disclosure of Identification Information of the Senders[1)]

(Act No. 137 of November 30, 2001)

Purpose

Article 1 The purpose of this Act is to set forth the limitation of liability for damages of specified telecommunications service providers and the right to demand disclosure of identification information of the senders in case of infringement of the rights through information distribution by specified telecommunications services.

1) http://www.japaneselawtranslation.go.jp/law/detail/?printID=&re=01&dn=1&x=0&y=0&co=1&ia=03&yo=&gn=&sy=&ht=&no=&bu=&ta=&ky=%E7%89%B9%E5%AE%9A%E9%9B%BB%E6%B0%97%E9%80%9A%E4%BF%A1%E5%BD%B9%E5%8B%99%E6%8F%90%E4%BE%9B%E8%80%85%E3%81%AE%E6%90%8D%E5%AE%B3%E8%B3%A0%E5%84%9F%E8%B2%AC%E4%BB%BB%E3%81%AE%E5%88%B6%E9%99%90%E5%8F%8A%E3%81%B3%E7%99%BA%E4%BF%A1%E8%80%85%E6%83%85%E5%A0%B1%E3%81%AE%E9%96%8B%E7%A4%BA%E3%81%AB%E9%96%A2%E3%81%99%E3%82%8B%E6%B3%95%E5%BE%8B&page=1&vm=02

Definitions

Article 2 In this Act, with respect to the meanings of the terms given in the following items, the definition specified in each item shall apply:

(i) The term “specified telecommunications service” means transmission (except transmission of telecommunications (hereinafter in this item only referring to “telecommunications” as defined in Article 2 item (i) of the Telecommunications Business Law (Law No. 86 of December 25, 1984)) with the aim of direct reception thereof by the public) of telecommunications with the aim of reception thereof by unspecified persons.

(ii) The term “specified telecommunications facilities” means telecommunications facilities (referring to “telecommunications facilities” as defined in Article 2 item ii) of the Telecommunications Business Law) being used for the operation of specified telecommunications.

(iii) The term “specified telecommunications service provider” means a person who relays others’ communications with the use of specified telecommunications facilities, or provides specified telecommunications facilities to be used for others’ communications.

(iv) The term “sender” means a person who has recorded information in recording media (limited to such recording media, from which the information recorded therein is to be transmitted to unspecified persons) of specified telecommunications facilities used by a specified telecommunications service provider, or who has input information in the transmission device (limited to such a transmission device, from which the information input therein is to be transmitted to unspecified persons) of such specified telecommunications facilities.

Limitation of Liability for Damages

Article 3 When any right of others is infringed by information distribution via specified telecommunications, the specified telecommunications service provider who uses specified telecommunications facilities for said specified telecommunications (hereinafter in this paragraph referred to as a “relevant service provider”) shall not be liable for any loss incurred from such infringement, unless where it is technically possible to take measures for preventing such information from being transmitted to unspecified persons and such event of infringement falls under any of the following items. However, where said relevant service provider is the sender of said information infringing rights, this shall not apply.

(i) In cases where said relevant service provider knew that the infringement of the rights of others was caused by information distribution via said specified telecommunications.

(ii) In cases where said relevant service provider had knowledge of information distribution by said specified telecommunications, and where there is a reasonable ground to find that said relevant service provider could know the infringement of the rights of others was caused by the information distribution via said specified telecommunications.

(2) When a specified telecommunications service provider has taken measures to block transmission of information via specified telecommunications, said specified telecommunications service provider shall not be liable for any loss incurred by a sender of such information, transmission of which is prevented by said measures, so far as said measures have been taken within the limit necessary for preventing transmission of said information to unspecified persons and said measures fall under any of the following items:

(i) In cases where there was a reasonable ground for said specified telecommunications service provider to believe that the rights of others were infringed without due cause by the information distribution via said specified telecommunications.

(ii) In cases where a person alleging that his right was infringed by distribution of information via a specified telecommunications filed a petition that said specified telecommunications service provider take measures to prevent said information infringing his right (hereinafter referred to as "infringing information") from being transmitted (hereinafter in this item referred to as "transmission prevention measures"), indicating the infringing information and the allegedly infringed right and the reason why said person insists on said infringement (hereinafter in this item referred to as "infringing information, etc.") and where said specified telecommunications service provider provided such infringing information, etc. to the sender of said infringing information and inquired the sender if said sender agrees with implementing said transmission prevention measures, where said specified telecommunications service provider has not received any notice from said sender indicating his disagreement with implementation of said transmission prevention measures after seven days from the day of said inquiry to said sender.

Demand for Disclosure of Identification Information of the Sender, Etc.

Article 4 Any person alleging that his or her rights were infringed by distribution of information via specified telecommunications may, limited to cases when falling under both of the following items, demand a specified telecommunications service provider using specified telecommunications facilities for the operations of said specified telecommunications (hereinafter referred to as a "provider of disclosure-related service") to disclose identification information of the sender pertaining to said infringement of the rights (referring to information, including a name and address, contributing to identifying the sender of the infringing information and which is as stipulated in the applicable MIC ordinance; hereinafter the same shall apply.) possessed by said provider of disclosure-related service:

(i) Where there is evidence that the rights of a person demanding said disclosure were infringed by the distribution of the infringing information.

(ii) Where said identification information of the sender is necessary for the person demanding said disclosure to exercise his or her rights to claim damages and where there is justifiable ground for said person to receive disclosed identification information of the sender.

(2) When the provider of disclosure-related service receives such demand as stipulated in the preceding paragraph, said provider shall hear the opinion of the sender of the infringing information pertaining to said demand for disclosure on whether said sender consents to the disclosure of his or her identification information, except where said provider is unable to contact said sender or where there are special circumstances.

(3) Any person to whom the identification information of the sender has been disclosed in accordance with the provisions of paragraph (1) must not use the identification information of the sender without due cause, unjustly damaging the reputation or disturbing the peaceful existence of the sender.

(4) The provider of disclosure-related service shall not be liable for any loss incurred by the person who demanded for said disclosure in accordance with the provisions of paragraph (1) arising from said provider's refusal of said demand, unless there is any willful act or gross negligence on the part of said provider. However, where said provider of disclosure-related service is the sender of infringing information pertaining to said demand for disclosure, this shall not apply.

特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律

(平成十三年十一月三十日法律第百三十七号)

趣旨

第一条　この法律は、特定電気通信による情報の流通によって権利の侵害があった場合について、特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示を請求する権利につき定めるものとする。

定義

第二条　この法律において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

一　特定電気通信　不特定の者によって受信されることを目的とする電気通信（電気通信事業法（昭和五十九年法律第八十六号）第二条第一号に規定する電気通信をいう。以下この号におい

て同じ。）の送信（公衆によって直接受信されることを目的とする電気通信の送信を除く。）をいう。

二　特定電気通信設備　特定電気通信の用に供される電気通信設備（電気通信事業法第二条第二号 に規定する電気通信設備をいう。）をいう。

三　特定電気通信役務提供者　特定電気通信設備を用いて他人の通信を媒介し、その他特定電気通信設備を他人の通信の用に供する者をいう。

四　発信者　特定電気通信役務提供者の用いる特定電気通信設備の記録媒体（当該記録媒体に記録された情報が不特定の者に送信されるものに限る。）に情報を記録し、又は当該特定電気通信設備の送信装置（当該送信装置に入力された情報が不特定の者に送信されるものに限る。）に情報を入力した者をいう。

損害賠償責任の制限

第三条　特定電気通信による情報の流通により他人の権利が侵害されたときは、当該特定電気通信の用に供される特定電気通信設備を用いる特定電気通信役務提供者（以下この項において「関係役務提供者」という。）は、これによって生じた損害については、権利を侵害した情報の不特定の者に対する送信を防止する措置を講ずることが技術的に可能な場合であって、次の各号のいずれかに該当するときでなければ、賠償の責めに任じない。ただし、当該関係役務提供者が当該権利を侵害した情報の発信者である場合は、この限りでない。

一 当該関係役務提供者が当該特定電気通信による情報の流通によって他人の権利が侵害されていることを知っていたとき。

二　当該関係役務提供者が、当該特定電気通信による情報の流通を知っていた場合であって、当該特定電気通信による情報の流通によって他人の権利が侵害されていることを知ることができたと認めるに足りる相当の理由があるとき。

２　特定電気通信役務提供者は、 特定電気通信による情報の送信を防止する措置を講じた場合において、 当該措置により送信を防止された情報の発信者に生じた損害については、当該措置が当該情報の不特定の者に対する送信を防止するために必要な限度において行われたものである場合であって、次の各号のいずれかに該当するときは、賠償の責めに任じない。

一　当該特定電気通信役務提供者が当該特定電気通信による情報の流通によって他人の権利が不当に侵害されていると信じるに足りる相当の理由があったとき。

二　特定電気通信による情報の流通によって自己の権利を侵害されたとする者から、当該権利を侵害したとする情報（以下この号及び第四条において「侵害情報」という。）、侵害されたとする権利及び権利が侵害されたとする理由（以下この号において「侵害情報等」という。）を示して当該特定電気通信役務提供者に対し侵害情報の送信を防止する措置（以下この号において「送信防止措置」という。）を講ずるよう申出があった場合に、当該特定電気通信役務提供者が、当該侵害情報の発信者に対し当該侵害情報等を示して当該送信防止措置を講ずることに同意するかどうかを照会した場合において、当該発信者が当該照会を受けた日から七日を経過しても当該発信者から当該送信防止措置を講ずることに同意しない旨の申出がなかったとき。

公職の候補者等に係る特例

第三条の二　前条第二項の場合のほか、特定電気通信役務提供者は、特定電気通信による情報（選挙運動の期間中に頒布された文書図画に係る情報に限る。以下この条において同じ。）の送信を防止する措置を講じた場合において、当該措置により送信を防止された情報の発信者に生じた損害については、当該措置が当該情報の不特定の者に対する送信を防止するために必要な限度において行われたものである場合であって、次の各号のいずれかに該当するときは、賠償の責めに任じない。

一　特定電気通信による情報であって、 選挙運動のために使用し、 又は当選を得させないための活動に使用する文書図画（以下「特定文書図画」という。）に係るものの流通によって自己の名誉を侵害されたとする公職の候補者等（公職の候補者又は候補者届出政党（公職選挙法　（昭和二十五年法律第百号）第八十六条第一項 又は第八項 の規定による届出をした政党その他の政治団体をいう。）若しくは衆議院名簿届出政党等（同法第八十六条の二第一項　の規定による届出をした政党その他の政治団体をいう。）若しくは参議院名簿届出政党等（同法第八十六条の三第一項　の規定による届出をした政党その他の政治団体をいう。）をいう。以下同じ。）から、当該名

誉を侵害したとする情報（以下「名誉侵害情報」という。）、名誉が侵害された旨、名誉が侵害されたとする理由及び当該名誉侵害情報が特定文書図画に係るものである旨（以下「名誉侵害情報等」という。）を示して当該特定電気通信役務提供者に対し名誉侵害情報の送信を防止する措置（以下「名誉侵害情報送信防止措置」という。）を講ずるよう申出があった場合に、当該特定電気通信役務提供者が、当該名誉侵害情報の発信者に対し当該名誉侵害情報等を示して当該名誉侵害情報送信防止措置を講ずることに同意するかどうかを照会した場合において、当該発信者が当該照会を受けた日から二日を経過しても当該発信者から当該名誉侵害情報送信防止措置を講ずることに同意しない旨の申出がなかったとき。

二　特定電気通信による情報であって、特定文書図画に係るものの流通によって自己の名誉を侵害されたとする公職の候補者等から、名誉侵害情報等及び名誉侵害情報の発信者の電子メールアドレス等（公職選挙法第百四十二条の三第三項　に規定する電子メールアドレス等をいう。以下同じ。）が同項 又は同法第百四十二条の五第一項 の規定に違反して表示されていない旨を示して当該特定電気通信役務提供者に対し名誉侵害情報送信防止措置を講ずるよう申出があった場合であって、当該情報の発信者の電子メールアドレス等が当該情報に係る特定電気通信の受信をする者が使用する通信端末機器（入出力装置を含む。）の映像面に正しく表示されていないとき。

発信者情報の開示請求等

第四条　特定電気通信による情報の流通によって自己の権利を侵害されたとする者は、次の各号のいずれにも該当するときに限り、当該特定電気通信の用に供される特定電気通信設備を用いる特定電気通信役務提供者（以下「開示関係役務提供者」という。）に対し、当該開示関係役務提供者が保有する当該権利の侵害に係る発信者情報（氏名、住所その他の侵害情報の発信者の特定に資する情報であって総務省令で定めるものをいう。以下同じ。）の開示を請求することができる。

一　侵害情報の流通によって当該開示の請求をする者の権利が侵害されたことが明らかであるとき。

二　当該発信者情報が当該開示の請求をする者の損害賠償請求権の行使のために必要である場合その他発信者情報の開示を受けるべき正当な理由があるとき。

2　開示関係役務提供者は、前項の規定による開示の請求を受けたときは、当該開示の請求に係る侵害情報の発信者と連絡することができない場合その他特別の事情がある場合を除き、開示するかどうかについて当該発信者の意見を聴かなければならない。

3　第一項の規定により発信者情報の開示を受けた者は、当該発信者情報をみだりに用いて、不当に当該発信者の名誉又は生活の平穏を害する行為をしてはならない。

4　開示関係役務提供者は、第一項の規定による開示の請求に応じないことにより当該開示の請求をした者に生じた損害については、故意又は重大な過失がある場合でなければ、賠償の責めに任じない。ただし、当該開示関係役務提供者が当該開示の請求に係る侵害情報の発信者である場合は、この限りでない。

Session 2

Intermediary Liability and Digital Ecosystem

정보매개자 책임과
ICT 생태계

Main Speaker / 주제 발표

Anupam Chander
아누팜 챈더

▪ Professor of Law at UC Davis

Anupam Chander is Director of the California International Law Center and Professor of Law at the University of California, Davis, where he is a Martin Luther King, Jr. Hall Research Scholar. He has been a visiting professor at Yale Law School, the University of Chicago Law School, Stanford Law School, and Cornell Law School. He has published widely in the nation's leading law journals, including the Yale Law Journal, the NYU Law Journal, the University of Chicago Law Review, the Texas Law Review, and the California Law Review.

A graduate of Harvard College and Yale Law School, he clerked for Chief Judge Jon O. Newman of the Second Circuit Court of Appeals and Judge William A. Norris of the Ninth Circuit Court of Appeals. He practiced law in New York and Hong Kong with Cleary, Gottlieb, Steen & Hamilton.

Main Speaker / 주제 발표

Oliver Süme
올리버 쥬메

▪ EuroISPA President

Oliver J. Süme is President of EuroisPA, the worlds largest ISP Associaion, representing more than 2300 Internet Service Providers across the EU and EFTA Countries. He is also deputy chair of the board of the German Internet Industry Association (eco) since 2000. There, he oversees the activities of the Political and Legal Affairs Department, which includes responsibility for representing the political interests of the association and its over 800 member companies. Süme is also a trained lawyer and partner at the Hamburg–based law firm of Richter Süme, where he has worked since 1997, primarily as an advocate for companies in the Internet and IT sectors. Süme is a certified IT–Lawyer and member of the IT Law Committee of the Hanseatic Bar Association. He is co–founder and CEO of Hamburg Top–Level–Domain, the registry for the new Top–Level–Domain ".hamburg".

Moderator / 좌장

Kim, Jewan
김제완

▪ 1998	Ph.D. 박사	Graduate School of Law, Korea University 고려대학교 법과대학
▪ 1994	M.A. 석사	Graduate School of Law, Korea University 고려대학교 법과대학
▪ present	Professor 교수	Korea University Law School 고려대학교 법학전문대학원
▪ present	President 원장	Legal Research Institute, Korea University 고려대학교 법학연구원
▪ present	Member 위원	Bar Reform Committee, Ministry of Justice 법무부 변호사제도개선위원회 위원
▪ present	Member 자체평가위원	Fair Trade Commission 공정거래위원회
▪ present	Member 실행위원	PSPD Judicial Watch Center 참여연대 사법감시센터

Panelists / 토론자

Kim, Minjeong
김민정

▪ –	Ph.D. 박사	School of Journalism and Mass Communication, University of North Carolina 미국 노스캐롤라이나대학교 저널리즘&매스컴
▪ –	M.A. 석사	School of Journalism and Mass Communication, University of North Carolina 미국 노스캐롤라이나대학교 저널리즘&매스컴
▪ –	M.A. 석사	Dept. of Mass Communication, Hankuk University of Foreign Studies 한국외국어대학교 신문방송학과
▪ Present	Associate Professor 부교수	Division of Media and Communication, Hankuk University of Foreign Studies 한국외국어대학교 사회과학대학 미디어커뮤니케이션학부
▪ Present	Director of Research 연구이사	Korean Society for Media Law, Ethics and Policy Research 한국언론법학회
▪ 2012 ~ 2013	Associate Professor 부교수	Colorado State University 미국 콜로라도 주립대학교

Panelists / 토론자

Lee, Inho
이인호

▪ –	Ph.D. 박사	Graduate School of Law, Chung-Ang University 중앙대학교 대학원 법학
▪ Present	Professor 교수	Chung-Ang University Law School 중앙대학교 법학전문대학원
▪ Present	Co-President 공동회장	Korea Association For Informedia Law 한국정보법학회
▪ Present	Commissioner 위원(비상임)	Central Administrative Appeals Commission 중앙행정심판위원회
▪ Present	Member 위원	Legislation Support Committee of the National Assembly Secretariat 국회사무처 입법지원위원회
▪ Present	Vice President 부회장	Korean Society for Media Law, Ethics and Policy Research 한국언론법학회

Panelists / 토론자

Yoon, Jongsoo
윤종수

▪ 1989	M.A. 석사	Graduate School of Law, University of Seoul 서울시립대학교 법과대학
▪ Present	Partner 파트너 변호사	Shin&Kim 법무법인 세종
▪ Present	Chairperson 위원장	Advisory Board for Development of Internet Search Service 인터넷 검색 서비스 발전을 위한 자문위원회
▪ Present	Vice President 부회장	Korea Association For Informedia Law 한국정보법학회
▪ Present	Member 위원	Korea Copyright Commission 한국저작권위원회
▪ present	Board Member 이사	Creative Commons 크리에이티브 커먼스

Main Speaker / 주제발표

The "Electronic Silk Road" and Intermediary Liability

Prof. **Anupam Chander**
(UC Davis School of Law)

"e-실크로드"와
정보매개자 책임

아누팜 챈더 교수 (미 UC데이비스 로스쿨)

The Electronic Silk Road and Information Intermediaries

Nearly every company set up in a garage in Silicon Valley hopes to take over the world. There is reason for such optimism. Again and again, Silicon Valley firms have become the world's leading providers of Internet services. How did Silicon Valley become the world's leading supplier of Internet services?

Popular explanations for Silicon Valley's recent success revolve around two features. First, Silicon Valley bestrides the great academic centers of Stanford University and the University of California, Berkeley, and sits near the artistic and intellectual hub of San Francisco. Second, the center of venture capital in the United States also happens to be in Menlo Park, California, allowing both industries to profit from each other in a symbiotic relationship. But education and money coincide in other parts of the United States as well. Why did those parts not prosper in the manner of Silicon Valley? More fundamentally, did not the Internet make geography irrelevant? Scholars answer that Silicon Valley's advantage lies in the economies of agglomeration. Ronald Gilson argued that California's advantage was its labor law, which he believes encourages "knowledge spillovers" and agglomeration economies by facilitating employee mobility. While these standard accounts do much to explain the dynamism of Silicon Valley relative to other parts of the United States, they do not explain the relative absence of such Internet innovation hubs outside the United States, or the success of Silicon Valley enterprises across the world.

Law played a far more significant role in Silicon Valley's rise and its global success than has been previously understood. It enabled the rise of Silicon Valley while simultaneously disabling the rise of competitors across the world. In this Article, I will argue that Silicon Valley's success in the Internet era has been due to key substantive reforms to American copyright and tort law that dramatically reduced the risks faced by Silicon Valley's new breed of global traders. Specifically, legal innovations in the 1990s that reduced liability concerns for Internet intermediaries, coupled with low privacy protections, created a legal ecosystem that proved fertile for the new enterprises of what came to be known as Web 2.0. I will argue that this solicitude was not accidental—but rather a kind of cobbled industrial policy favoring Internet entrepreneurs. In a companion paper, Uyên Lê and I show that these aspects of copyright and tort law were not driven by commercial considerations alone, but were undergirded in large part by a constitutional commitment to free speech. As we argue there, a First Amendment-infused legal culture that prizes speech offered an ideal environment in which to build the speech platforms that make up Web 2.0.

I will compare the legal regimes not between Silicon Valley and Boston's Route 128, but between the United States and key technological competitors across the globe. The indulgence of American law for Internet enterprise appears in sharper relief when contrasted with the legal regimes faced by web entrepreneurs elsewhere. In Europe, concerns about copyright violations and strict privacy protections hobbled Internet startups. Asian web enterprises faced not only copyright and privacy constraints, but also strict intermediary liability rules. I will contrast the leading cyberlaw statutes and cases in the United States, with their explicit embrace of commerce and speech, with those from Europe and Asia, which are more attendant to the risks of this new medium for existing interests. I will show that Google and Yahoo were so worried that Japanese copyright law would make search engines illegal that they placed their search servers offshore. A Japanese computer science professor advised his students to publish their software outside Japan. British Prime Minister David Cameron suggested that Google's search engine might have been illegal under English copyright law.

This Article upends the conventional wisdom, which sees strong intellectual property protections as the key to innovation—what the World Intellectual Property Organization calls a "power tool" for growth. Understanding the reasons for Silicon Valley's global success is of more than historical interest. Governments across the world, from Chile to Kenya to Russia, seek to incubate the next Silicon Valley. My review suggests that overly rigid intellectual property laws can prove a major hurdle to Internet innovations, which rely fundamentally on empowering individuals to share with each other. This study helps make clear what is at stake in debates over new laws such as the Stop Online Piracy Act (SOPA) and its relatives, highlighting the effect of these laws on Silicon Valley's capacity for innovation. I show that government has the power to enable, or disable, a new industry. The power to make in this case implies the power to break.

Innovation scholars worry about the "valley of death," the stage between start-up idea and successful commercialization, in which most start-up enterprises founder. Cyber scholars fond of citing Joseph Schumpeter's "creative destruction" need to attend to his focus as well on the finance needed by innovators.

Imagine the boardroom in a Silicon Valley venture capital firm, circa 2005. A start-up less than a year old has already attracted millions of users. Now that start-up, which is bleeding money, needs an infusion of cash to survive and scale up. The start-up lets people share text, photos, and videos, and includes the ability to readily share text, pictures, and videos posted by one's friends. If that start-up can be accused of abetting copyright infringement on a massive scale, or must police its content like a traditional publishing house lest it face damages claims or an injunction, your hundred-million-dollar investment might simply vanish to plaintiffs' lawyers in damages and fees. An injunction might stop the site from continuing without extensive human monitoring that could not be justified by potential revenues. Because of the insulation brought by U.S. law reforms in the 1990s, American start-ups did not fear a mortal legal blow. The legal privileges granted to Internet enterprises in the United States helped start-ups bridge the valley of death.

Let me anticipate criticism. First, legal realists might object that I have spoken about law on the books. What about law in action? I demonstrate through actual cases the practical importance of the liberal American law and the strict European and Asian laws. Second, some might seek to trivialize my thesis: law always matters to the success of an enterprise because it could have made that enterprise illegal, but did not. That is not my claim; rather, my claim is that U.S. authorities (but not those in other technologically advanced states) acted with deliberation to encourage new Internet enterprises by both reducing the legal risks they faced and largely refraining from regulating the new risks they introduced. Third, some will insist that if law was relevant, it was only because it got out of the way. After all, the last person hired at a Silicon Valley start-up is the lawyer. I show that the story of Silicon Valley is not only a story of brilliant programmers in their garages, but also a legal environment specifically shaped to accommodate their creations.

My claim may resonate with students of American legal history. Morton Horwitz famously argued that nineteenth-century American courts modified liability rules to favor the coming of industrialization. I suggest an even more widespread effort, with the Executive, Congress, and the Courts, each in their own way promoting Internet enterprise. Horwitz decried the nineteenth-century's laws' implicit subsidy to industrialists, which he saw as being borne on the backs of society's least fortunate. The limitations on Internet intermediary liability and the lack of omnibus privacy protections beyond those that are promised contractually by websites mean that there is a price to be paid for the amazing innovation of the past two decades. Even while we celebrate innovation, we must recognize its costs.

But the benefits have been enormous, not only in the economic impact of the information that is being shared, but also in the radical democratization of the freedom of speech.

In the United States, Congress and the courts recognized that broad liabilities on Internet intermediaries would impinge on the speech of ordinary persons. Free speech depends on a free press. Today, Internet intermediaries are increasingly replacing the press of old, just as radio and television replaced print in earlier eras. Where early interpretations of the First Amendment had focused on direct governmental regulation, beginning with New York Times v. Sullivan, the U.S. Supreme Court recognized that speech could be burdened indirectly, by delegating the right to sanction speech to private parties.

When it comes to speech, Internet intermediaries are likely to be ensnared, caught in the middle of the worldwide war fueled by copyright interests, users' privacy, and governments' desire to control what is said and to listen in on what people are saying. Internet intermediaries are often the most vulnerable and effective points of control for any government keen on controlling speech.

The First Amendment reveals itself as the industrial policy for an information age. In an information age, free speech greases the economic engine. By revealing the free speech foundations of American cyberlaw, I hope to encourage other countries around the world eager to incubate the next Silicon Valley to embrace free speech. Governments from Brazil to India to Russia to South Korea, seeking to incubate their own Silicon Valleys, must recognize the vital role that free speech plays in enabling Internet enterprise.

e-실크로드와 정보매개자

실리콘 밸리의 차고에서 시작하는 대부분의 회사들은 세계 정복을 꿈꾼다. 이러한 낙관론에는 이유가 있다. 실리콘밸리 기업들이 계속해서 세계 유수의 인터넷 서비스 제공업체로 자리매김하고 있기 때문이다. 그렇다면 실리콘밸리는 어떻게 세계적인 인터넷 서비스 제공지가 되었는가?

실리콘밸리의 최근 성공 비결에는 두 가지 요소가 있다는 것이 일반적인 견해이다. 첫째, 스텐포드대학교와 캘리포니아대학교 버클리캠퍼스라는 위대한 학문의 전당 사이에 위치한 실리콘밸리는 샌프란시스코의 예술과 지식의 허브 인근에 자리하고 있다는 점이다. 둘째, 미국 벤처금융 중심이 캘리포니아 멘로공원(Menlo Park)에 있기 때문에, 실리콘밸리와 벤처금융은 공생관계를 통해 상호 이익을 거둘 수 있다. 하지만 교육과 자금이라는 요소는 미국 다른 지역에서도 공존하고 있는데, 왜 이러한 지역들은 실리콘밸리와 같은 방식으로 번영하지 않는 것일까? 보다 근본적인 질문은 인터넷으로 인해 지역적인 요소는 무의미해지지 않았는가? 학자들은 실리콘밸리의 장점은 집합 경제학에 있다고 답한다. Ronald Gilson은 캘리포니아의 장점은 노동법으로 종업원들의 이동을 조장함으로써 집합 경제와 "지식의 전이(knowledge spillover)"를 촉진한다고 주장했다. 이 같은 일반적인 설명은 미국내 타 지역 대비 실리콘밸리의 역동성을 잘 설명해 주지만, 이러한 인터넷 혁신이 타국에서 찾아보기 힘들다는 점이나 실리콘밸리 기업들이 거둔 세계적인 성공을 설명해주기에는 부족하다.

실리콘밸리의 부상과 세계적인 성공에 있어 법은 지금까지의 인식보다 훨씬 더 중요한 역할을 했다. 법은 실리콘밸리의 부상을 가능하게 했을 뿐 아니라 동시에 세계적으로 경쟁자들의 부상을 막기도 했다. 본 논문에서 인터넷 시대에 실리콘밸리의 성공은 미국의 저작권

불법행위법(copyright and tort law)에 대한 주요 개혁에서 기인하며, 이러한 개혁으로 인해 실리콘밸리의 신생 국제 무역업체들이 직면할 수 있는 위험부담이 극적으로 줄어들었다고 필자는 주장한다. 보다 구체적으로, 낮은 수준의 개인정보 보호 정책들과 아울러 인터넷 정보매개자들의 법적 책임 우려를 낮춘 1990년대 법적 혁신을 통해 웹2.0으로 알려진 신생 기업들에게 비옥한 토대를 제공한 법적 생태계를 마련한 것이다. 이 같은 배려들은 우연의 산물이 아니라 인터넷 기업들을 위해 마련된 산업정책이었음을 본 논문에서 밝히고자 한다. 다른 논문에서 필자와 Uyên Lê는 이러한 저작권 불법행위법의 이러한 측면들이 상업적인 고려사항만으로 추진된 것이 아니라 주로 표현의 자유에 대한 헌법적 약속에 의해 뒷받침되었음을 제시했다. 해당 논문에서 주장한 바와 같이 수정 제1조는 표현의 자유를 소중하게 여기는 법적 문화를 조성했고, 웹2.0을 구성하는 표현의 기반이 구축될 수 있는 이상적인 환경을 제공했다.

본 논문에서는 실리콘밸리와 보스턴의 128번 도로가 사이가 아니라 미국과 세계적인 주요 기술 경쟁자들간의 법적 체제를 비교하고자 한다. 인터넷 기업을 위한 미국법의 관대함은 다른 나라에서 인터넷 기업들이 직면하고 있는 법적 체제와 대조될 때 보다 뚜렷이 부각된다. 유럽에서 저작권 위반에 대한 우려와 엄격한 개인정보 보호 정책들은 신생 인터넷 기업에게 장애물로 작용했다. 아시아의 온라인 기업들은 저작권과 개인정보 제약뿐 아니라 엄격한 매개자 책임 규정에 직면했다. 본 논문에서 미국과 유럽의 대표적인 사이버 법령과 사례들을 대조해볼 예정인데, 미국은 상업과 표현의 자유를 공개적으로 반영한 반면, 유럽은 기존의 이익을 보호하기 새로운 인터넷이라는 매체의 위험에 보다 집중했다. 구글과 야후가 일본 저작권법이 검색엔진을 불법화할 것이라고 우려한 나머지 검색 서버를 해외에 두기로 결정한 사례도 제시할 것이다. 한 일본 컴퓨터공학과 교수는 제자들에게 소프트웨어를 일본이 아닌 타국에서 출시하라고 조언하기도 했다. 데이비드 캐머론 영국 총리는 구글 검색엔진이 영국저작권법에 따르면 불법이었을 것이라고 주장했다.

본 논문은 세계지적재산권기구(WIPO)가 성장의 "강력한 도구"라고 부르는 강력한 지적재산권 보호를 혁신의 핵심으로 간주하는 기존의 통념을 뒤집는다. 실리콘밸리의 세계적인 성공 원인을 이해하는 것은 역사적 차원을 넘어서는 일이다. 칠레에서 케냐, 러시아에 이르기까지 세계 모든 정부는 제2의 실리콘밸리를 만들고자 한다. 필자는 과도하게 엄격한 지재권법이 인터넷 혁신에 주요한 장애가 될 수 있다고 주장하는데, 인터넷의 혁신은 근본적으로 개인들이 서로 정보를 공유하도록 권한을 주는데 기반하고 있기 때문이다. 본 연구는 '온라인 저작권 침해 금지 법안(SOPA)'와 관련 법안 등 신규 법률에 관한 논쟁에 걸린 문제들을 명확히 파악하는데 도움이 되며, 이러한 법들이 실리콘밸리의 혁신 역량에 미치는 영향을 중점적으로 분석하고자 한다. 정부가 신규 산업의 성패를 결정할 수 있는 능력이 있다는 사실도 본 논문에서 제시될 예정이다. 여기에서 성공하게 만드는 능력은 곧 실패하게 만드는 능력인 것이다.

혁신 학자들은 창업 아이디어와 성공적인 상업화 중간 단계인 "죽음의 계곡(valley of death)"에 대해 우려를 표명하는데, 대부분의 스타트업 창업자들이 여기에 위치해있다. Joseph Schumpeter의 "창의적 파괴"를 즐겨 인용하는 사이버 학자들은 혁신가들이 필요한 자금뿐 아니라 Schumpeter의 핵심 주장에도 주의를 기울일 필요가 있다.

2005년경 실리콘 밸리의 한 벤처금융 기업의 이사회실을 상상해 보자. 설립된 지 채 1년이 되지 않은 이 스타트업은 이미 수백만 명의 사용자들을 모았다. 현재 적자상태인 이 기업은 생존과 확장을 위해 현금 수혈이 필요하다. 이 기업은 사용자들이 문자, 사진, 영상을 올리고 친구들이 올린 문자, 사진, 영상도 즉시 공유할 수 있는 기능을 제공한다. 만약 이 회사가 대규모 저작권 침해를 방조한다는 혐의로 고소되거나 손해배상이나 명령을 받지 않기 위해 기존 출판사처럼 컨텐츠를 감시해야 한다면, 수억 달러의 투자금이 원고측 변호사의 손해배상액과 수수료로 사라질 수 있다. 법원 명령을 통해 해당 사이트는 잠재적인 수입으로는 감당하기 어려운 수준의 대규모 인적 모니터링 없이는 운영을 중단해야 할 수도 있다. 1990년대 미국법 개혁으로 인한 법적 보호로 인해 미국 스타트업들은 치명적인 법적 처벌을 두려워하지 않게 되었다. 미국 인터넷 기업들에 부여된 법적 특권은 스타트업들이 이 죽음의 계곡을 건널 수 있도록 도왔다.

이 같은 주장에 대해 다음과 같은 비판이 제기될 수 있다. 첫째, 법적 현실주의자들은 필자가 교과서상의 법에 대해 말하고 있다고 반론을 펼칠 수 있을 것이다. 그렇다면 실제 실행되고 있는 법은 어떠한가? 본 논문에서는 실제 사례를 통해 자유로운 미국법과 엄격한 유럽 및 아시아 법들의 실용적인 중요성을 제시하고자 한다. 둘째, 법은 기업을 불법화할 수 있기 때문에 기업의 성공에 있어 항상 중요하지만 실제로 불법화지 않았다는 필자의 이론을 일축하고자 할 수 있다. 이는 필자의 주장이 아니다. 오히려 미 당국(다른 기술적으로

앞선 국가들의 당국이 아닌)은 신생 인터넷 기업들이 직면했던 법적 위험을 낮추고 이들이 가져오는 새로운 위험을 규제하지 않음으로써 이러한 기업들을 장려하기 위한 의도적인 행동을 취했다는 것이 필자의 주장이다. 셋째, 만약 법적인 연관성이 있다면 이는 법이 단지 방해하지 않았기 때문이라고 주장할 수도 있다. 결국 실리콘밸리의 스타트업은 변호사를 절대 고용하지 않을 것이다. 실리콘밸리의 이야기는 차고에서 일하는 뛰어난 프로그래머들의 이야기일 뿐 아니라 이들의 창업에 부응하도록 특별히 고안된 법적 환경에 관한 이야기임을 본 논문에서 제시하고자 한다.

필자의 주장은 미국법 역사 학도의 공감을 얻을 수 있을 것이다. Morton Horwitz 는 잘 알려진 바와 같이 19세기 미국 법원이 산업화 도래에 우호적인 방향으로 법적 책임 규정을 수정했다고 주장했다. 필자는 행정부, 의회, 법정이 각각의 방식을 통해 인터넷 기업을 촉진하기 위해 보다 방대한 노력을 기울였다고 주장한다. Horwitz는 19세기 법이 경영주들에게 은밀히 보조금을 제공했다고 주장했는데 이는 사회에서 가장 불운한 사람들을 등에 업고 탄생한 제도라고 그는 생각했다. 인터넷 정보매개자들의 책임에 대한 제한과 웹사이트가 계약을 통해 약속한 수준을 넘어선 일괄적인 개인정보 보호의 부재는 지난 20년간의 놀라운 혁신에 대해 지불해야 할 가격이 있다는 것을 의미한다. 혁신을 축하할 때에도 이 비용은 인정되어야 한다.

하지만 공유되는 정보의 경제적 효과뿐 아니라 표현의 자유의 급진적인 보편화가 가져온 혜택은 막대했다.

미국에서 의회와 법정은 인터넷 정보매개자에 대한 광범위한 법적 책임이 일반인들의 표현의 자유를 침해할 수 있다고 인정했다. 표현의 자유는 언론의 자유에 달려있다. 과거 라디오와 TV가 인쇄매체를 대체했듯이 오늘날 인터넷 정보매개자들은 갈수록 기존 언론을 대체하고 있다. 수정 제1조의 초창기 해석은 New York Times v. Sullivan사건을 비롯해 직접적인 정부 규제에 초점을 뒀지만, 미대법원은 언론을 제재할 권리를 민간 당사자들에게 이양하게 되면 표현의 자유에 간접적으로 부담을 줄 수 있다고 인정했다.

표현의 자유에 있어 인터넷 정보매개자들은 저작권 이해, 사용자 개인정보, 여론을 통제하고 파악하고자 하는 정부의 바램에 의해 펼쳐지는 세계적인 전쟁 한가운데서 사면초가 상황에 빠질 수 있다. 인터넷 정보매개자들은 언론을 통제하고자 하는 정부에 있어 가장 손쉽고 효과적인 통제 포인트이다.

수정 제1조는 정보화 시대를 위한 상업 정책이라는 점이 자명하다. 정보화 시대에 표현의 자유는 경제라는 엔진의 윤활유 역할을 한다. 미국 사이버법의 표현의 자유라는 토대를 제시함으로써 필자는 제2의 실리콘밸리의 주인공이 되고자 열망하는 세계 다른 국가들이 표현의 자유를 포용하도록 장려하기를 희망한다. 브라질에서 인도, 러시아, 한국에 이르기까지 제2의 실리콘밸리를 만들고자 하는 정부들은 표현의 자유가 인터넷 기업을 장려함에 있어 수행하는 핵심 역할을 수행한다고 인정해야 할 것이다.

Main Speaker / 주제발표

E-Commerce Directive and Experience of European ISPs

Mr. **Oliver Süme**
(President, EuroISPA)

EU 전자상거래지침과
유럽 ISP의 경험

올리버 쥬메 회장 (유럽ISP협회)

Intermediary Liability in Europe : The Electronic-Commerce-Directive

1. Article 14: “Actual Knowledge”

The “actual knowledge” requirement has proven to be a cornerstone of the safer-harbor regime for both caching and hosting providers. The general wording introduced in the Directive was elaborated on purpose to ensure that the decision on the legality of a given piece of content would only be taken by a court or an administrative authority with trained personnel able to make balanced assessments. This approach proved to be useful in the prevention of active monitoring of allegedly illegal activities in compliance with the “no general monitoring obligation” in Article 15.

However, the lack of a specific definition of “actual knowledge” gave rise to interpretative problems at national level concerning the exact conditions under which a service provider was effectively acquiring such knowledge. In some cases, it is unclear if the intermediary acquires actual knowledge when a user is simply making a complaint or flagging a content deemed inappropriate, as opposed to a court order or decision establishing that a piece of content is effectively illegal.

In this context several questions arise:

- What kind of information is necessary in order to provide actual knowledge to the intermediary?
- How detailed must this information be?
- Can this information be provided by any third party or is it necessary that it is provided by the affected party?
- Concerning the actual knowledge about the illegality of content, does the intermediary need to carry out a legal analysis or must such illegality be apparent for everyone?

In order to cope with such concerns and minimize the risks related to hypothesis of ignorance, purposefully disinformation or inadvertency, the provider has been generally deemed having actual knowledge of the illegal deeds once a competent authority has declared the content illegal and has ordered its withdrawal, limitation to its access or declared the existence of damages, and the service provider knew about such decision.

Similar objective facts have been established, for example, by a detailed notice from a copyright owner. This, sometimes, requires service providers to address complex issues, such as whether particular acts that have been notified, such as terrorism or hate speeches allegations, are illegal or not, whether a product has been "put on the market" in the EU, is second-hand, is a tester, etc.

Actual knowledge, therefore, needs to be linked to a notification which fulfills certain minimum requirements such as:

- the notification should be in writing;
- the complainant should provide adequate identification of the specific item of content alleged to be infringing (a general description of the type of content, that requires the intermediary to investigate to discover which particular items match that description, is not sufficient);
- the notification should be sent to an e-mail address reserved for this purpose by the service provider;
- it should clearly specify which information or activity the complaint relates to;
- it should provide evidence that the complainant possesses the rights which he claims to be violated;
- it should include an assertion that the publisher or person making the work available is infringing their rights and does not have a lawful basis for publishing the work or making it available (whether by means of a license or by operation of law);
- it should include details of the unlawful nature of the activity or information in question;
- it should contain an assertion of truthfulness and accuracy of the above and include an admission of liability for action taken in reliance on the same.

It is noteworthy an Italian recent case where an ISP had "actual knowledge" from a third party warning alleging infringement of copyright by the ISP's users, through a notification meeting the above minimum requirements.

The Court stated that the ISP only obligation was to foreword to the competent authorities (i.e. Public Prosecutor's office and Ministry of Communications) all the information relating to the alleged infringements of copyright contained into the warning (order of Tribunal of Rome no. 415 of 2010).

2. Voluntary industry agreements

The above does not prejudice procedures of detection and content removal that service providers might implement under voluntary agreements and other means of actual knowledge that may be established. Such procedures are voluntary mechanisms for cooperation set forth in the ECD, through which the interested party can report the existence of an alleged illegal activity to an ISP with a view to the ISP reviewing the purportedly content and, as the case may be, assessing the advisability of removing or disabling access to it.

However, EuroISPA believes that there are a number of requirements and conditions that must be considered when setting up voluntary industry agreements.

The aim should also be to reinforce legal certainty for ISPs and their liability limitations, and create the context for a true collaboration with parties to the agreement. In principle Articles 12 – 15 should not be affected by voluntary industry agreements. In particular it must be excluded that any voluntary agreements give rise to a presumption of actual knowledge that would expose the service provider to liability.

3. Article 14: "Expeditiously"

Service providers must expeditiously remove, or block access to, information once they are aware of their illegal nature. The Directive does not define this requirement and leaves to Member States to "[establish] specific requirements which must be fulfilled expeditiously prior to the removal or disabling of information" (Recital 46).

Generally speaking, the term "expeditious" offers the necessary flexibility for case-by-case assessments. It cannot be laid down without the individual circumstances of the particular case.

If the expeditious action of a provider is due when the notice is coming from a court, a different assessment should be done in case of voluntary mechanisms. Indeed, while in the former case the intermediary has legal certainty, in the latter it could be required to act as soon as it is put on notice regardless of whether it has all the elements and the level of certainty needed to make a decision about the illegality of the content to be removed or disabled. Calling for expeditious removal in these cases, could result in the disabling access to sites or content that are not illegal, with far reaching consequences for the person unduly affected.

4. Article 14: notice and take-down

The notification procedure of allegedly illegal material for hosting providers in Article 14 ECD does not clearly define the mechanism to adopt in order to establish "actual knowledge" or "awareness of facts or circumstances". As consequence, diverging approaches have been adopted across Member States which could be gathered in the following categories:

- a A formal, official notification by a competent judicial authority (notice and take down): this option ensures the actual knowledge and provide legal certainty for intermediaries.
- b Simple notification determining actual knowledge: several shortcomings can be easily identified with the fact that the notice could come from official as well as unofficial sources; the burden of proving the illegality would stay with the provider (i.e. obvious crime vs complex query); the risk of such a system is to have the notice and take down applied consistently by the intermediary on all notifications and without proper legal assessment in order to escape liability. As mentioned above, it is of key importance to clarify and define minimum requirements as to when a provider has "actual knowledge" to reduce legal uncertainties for all parties involved. The UK law has laid down requirements similar to those listed under Question 53.
- c Statutory requirements: some countries do not provide a formal or simple notification procedure but set specific requirements to be observed by courts (i.e. location of the information, nature, contact details of the sender, etc.).

EuroISPA believes that the establishment of notice and stay down or notice and notice procedures should be evaluated comprehensively. We have reservations that the establishment of these procedures will have additional value. In principle, disputes should be solved directly between the parties concerned. ISPs, in their role of intermediaries, are an uninvolved third party. EuroISPA questions the practicability

of these procedures that could lead to legal uncertainty and impose obligations that will undermine the established liability regime. Moreover, it must be safeguarded and ensured that ISPs, in their role of intermediaries, do not become judges of the illegality of content.

4-1. Notice and notice

EuroISPA believes that an additional notification procedure maybe an option that could resolve disputes amicably and put the liability where it should lie, i.e. in the hands of parties disagreeing on the legality of a given piece of content. Such a system could come into consideration exclusively for hosting providers and limited to the forwarding of a notification. Privacy laws and the secrecy of telecommunications should be respected, and fundamental freedoms must be strictly adhered to.

Furthermore, it has to be taken into account that any notification procedure, like the notice and notice, is based on the general assumption that:

- intermediaries are exempted from liability;
- the general no-monitoring obligation is preserved;
- a penalty against a claimant that files a wrongful notice is introduced.

4-2. Notice and stay down

EuroISPA believes that such a system raises legal uncertainty, turns ISP in judges of the illegality of the content and imposes ongoing filtering or monitoring on users' communications while completely by-passing the judge intervention.

Such filtering or monitoring methods are not only costly to implement and present a risk for users' fundamental rights, but they also have no proven effectiveness.

In practice, "notice and stay down" is incompatible with the principle in Article 15, "no duty to monitor" as in order to discharge a requirement that certain material stay down a hosting provider would have to constantly monitor their service for the reappearance of the notified material. Moreover, unless the notification was extremely narrowly construed to refer to exact digital copies of the same file, notice and stay down would be impossible to implement (for example, a notice demanding the removal and continued suppression of libelous content could not be considered to cover a repetition of the same libelous assertion in different words).

5. Filtering measures

The discussions on filtering should in no case be limited to technical feasibility and the preliminary question one may expect from the European Commission is whether it is desirable, in line with Europe's values and economic interest, to even consider filtering methods. Such methods are difficult to be efficiently implemented in a resilient environment like the Internet that was designed to avoid barriers and blocks and find alternative ways to deliver information. This is particularly true in situations where the telecommunications providers' role is only a "mere conduit" of real-time transmissions, for example in peer-to-peer networks. The impracticability

of such measures is grounded on several reasons:

Form a technological point of view: an effective filtering is not possible. Easy to circumvent, all content is affected (particularly legal content). There are an impact and adverse effects on the network resilience, security and efficiency of the infrastructure. All content has to be transported/checked by a centralized filtering infrastructure in the ISP network. The risk is high for a general monitoring of content/users to have collateral damages such as hypothesis of over-blocking.

From a broader perspective:

- Filtering measures bring with obvious implications with regard to the violation of fundamental freedoms;
- not for-profit providers cannot be expected to put in place filtering technologies;
- the needed economic investments in infrastructures and personnel are burdensome for providers and would significantly and durably impact the development of the European Information Society in a negative way. It also exists a risk of "mission creep", i.e. start addressing a specific issue and then enlarge the monitoring to other issues as well;
- it exists a risk of "technology creep", i.e. the need to constantly up-to-date the filter in accordance to the technological evolution of the Internet communications (ex: encryption). Filtering leads to the development of encrypted protocols and never ending investments to catch up with illegitimate uses and services (as oppose to deal with the problem at its source), resulting in costly and ineffective measures.

Additionally, if an Internet access provider has to actively roll out a filtering technology with regard to (part of) the data transmitted on its network, it could be argued that it would have the unintended consequence of neutralising the application of Article 12 of the Directive which exempts the access provider from any liability regarding the information transmitted via its network on condition that it does not select or modify the information contained in the transmission. However, if one considers that filters do not imply the selection of the information contained in the transmission as they consist of "mere technical instruments", then the liability exemption would be lifted with the consequence that the provider risks to be held liable for the malfunctioning of the filtering technology on its network causing, for instance, illegal content not being intercepted. In other words, the ISP characterization as "mere conduit" could be jeopardized with serious consequences for the provider, its customers and the respect of Fundamental Rights.

As established in the context of the **Belgian Scarlet-SABAM** case, where the technical solution "Audible Magic" was proposed as a possible filter for peer-to-peer traffic, the Belgian court acknowledged that it well might not be effective or scalable. Indeed, it seems impossible that a technology could make a waterproof distinction on the basis of the legal/illegal nature of the communication or even the identification of what is in a file. Indeed, this depends on specific considerations not directly related to the filter technology but, for instance, to the authorization or concrete license terms granted by the author or the collecting society and on the possible interference of statutory exceptions to copyright.

6. Proportionality

As mentioned, there is considerable doubt as to whether existing network filtering technologies would be effective in achieving their stated goal, particularly as users can be expected to use relatively simple encryption techniques to remain "one step ahead" of the technology. Encryption of peer-to-peer traffic is already happening at an increasing rate; filtering measures are likely to serve only to encourage universal adoption of encryption to avoid detection. At the same time, filtering can be expected to result in a risk of degradation of network services, of user experience and in the inadvertent blocking of access to legitimate content. Additionally, the increased costs such technology bring with would contribute creating a further barrier to address the digital divide.

As detailed in the WIPO Conventions and the Copyright in the Information Society Directive (2001/29/EC), exemptions to copyright for legitimate, agreed purposes are recognized and uncontroversial parts of intellectual property legislation. It is entirely possible for users to wish to exchange files which do not breach copyright but which, nonetheless, would risk being "filtered" by network filtering technologies that only allow "approved" files to get through. Both the EU and Council of Europe have had a global leadership position for many years in promoting free speech and access to information. There is simply no existing filtering technology that would allow full use of current technologies while ensuring that legitimate users' behaviours are not restricted.

To what extent can it be considered proportionate or even desirable at any level that intermediaries, which do not benefit in any way from the alleged illegal activity, should finance, or be obliged to finance network filtering technologies?

How much less acceptable does this approach seem when we consider that there is widespread agreement that these technologies offer no answer, or expectation of an answer, to the issue of encrypted files, meaning that an ISP investing heavily in such technology would see the investment rendered meaningless in a short space of time?

On a wider scale, imposing filtering in a way which is likely either to result in legal content being made inaccessible or results in cross-border effects (where legal material becomes unavailable because it is illegal in another country, for example) has international legal implications. The UN Covenant on Civil and Political Rights (Article 19) states that "everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice". A similar provision also appears in the European Convention on Human Rights.

The general obligation under Article 15 ECD proved to be sufficiently flexible and well drafted as to allow public authorities to put additional obligations on ISPs. Indeed, if the "general" monitoring obligation is forbidden, Member States are not prevented from imposing "specific, limited and clear" obligations on ISPs for individual cases. This interpretation is confirmed by Recital 47 of the directive which adds that courts can still request an ISP, even if not liable for the infringement, to terminate or prevent it through injunctions. However, when imposing specific obligations, a public authority should carefully assess the scope of it to avoid that the measure produces effects equivalent to a generalized monitoring.

* * *

ANNEX:

Relevant articles from the E-Commerce directive:

Section 4: Liability of intermediary service providers

Article 12

"Mere conduit"

1. Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network, Member States shall ensure that the service provider is not liable for the information transmitted, on condition that the provider:

a does not initiate the transmission;

b does not select the receiver of the transmission; and

c does not select or modify the information contained in the transmission.

2. The acts of transmission and of provision of access referred to in paragraph 1 include the automatic, intermediate and transient storage of the information transmitted in so far as this takes place for the sole purpose of carrying out the transmission in the communication network, and provided that the information is not stored for any period longer than is reasonably necessary for the transmission.

3. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement.

Article 13
"Caching"

1. Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request, on condition that:

- a the provider does not modify the information;
- b the provider complies with conditions on access to the information;
- c the provider complies with rules regarding the updating of the information, specified in a manner widely recognised and used by industry;
- d the provider does not interfere with the lawful use of technology, widely recognised and used by industry, to obtain data on the use of the information; and
- e the provider acts expeditiously to remove or to disable access to the information it has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement.

2. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement.

Article 14
Hosting

1. Where an information society service is provided that consists of the storage of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the information stored at the request of a recipient of the service, on condition that:

- a the provider does not have **actual knowledge** of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or
- b the provider, upon obtaining such knowledge or awareness, acts **expeditiously** to remove or to disable access to the information.

2. Paragraph 1 shall not apply when the recipient of the service is acting under the authority or the control of the provider.

3. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement, nor does it affect the possibility for Member States of establishing procedures governing the removal or disabling of access to information.

Article 15

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.

유럽의 정보매개자 책임: 전자상거래 지침을 중심으로

1. 제14조: “실질적 인식”

“실질적 인식(actual knowledge)” 요건은 캐싱 및 호스팅 서비스 제공자의 면책 체제에 있어 결정적인 계기임이 입증되었다. 지침이 제시한 총칙은 특정 콘텐츠의 합법성에 대한 결정은 균형잡힌 평가가 가능한 전문적 훈련을 받은 인력을 보유 법정이나 행정당국에 의해서만 내려지도록 정교하게 의도된 것이다. 이러한 접근법은 제15조 “일반적 모니터링 의무 금지” 조항에 따라 불법이라고 주장된 활동에 대한 적극적 감시를 예방하는 데에 유용한 것으로 판명되었다.

하지만 “실질적 인식”에 대한 구체적인 정의가 없어 각국 수준에서 서비스 제공업체가 실제로 이와 같은 지식을 습득하는 정확한 요건들과 관련한 해석의 문제가 발생했다. 사건에 따라 정보매개자가 법원의 명령 혹은 결정으로 콘텐츠가 실제로 불법이라고 판명된 것이 아니라 이용자가 단순히 불만을 신고하거나 부적절하다고 판단한 콘텐츠에 표시했을 때 실질적으로 인식하였는가가 불분명한 경우도 있다.

이러한 맥락에서 다음의 몇 가지 의문이 생긴다.

- 정보매개자에게 실질적 인식을 제공하기 위해 필요한 정보의 종류는 무엇인가?
- 해당 정보는 얼마나 상세해야 하는가?
- 해당 정보가 제3자에 의해 제공될 수 있는가 아니면 당사자에 의해서만 제공되어야 있는가?
- 콘텐츠의 불법성에 관련한 실질적 인식에 대해, 정보매개자가 법적 분석을 수행할 필요가 있는가 또는 이러한 불법성은 만인에게 명백해야 하는가?

이와 같은 우려를 해소하고 부지, 의도적 왜곡 또는 태만의 가정과 관련된 리스크를 최소화하기 위해 통상 서비스 제공자는 관할 기관이 해당 콘텐츠가 불법이라고 선언하고, 그 삭제, 접근의 제한을 명하거나, 피해가 있는 것으로 결정하며, 제공자가 이러한 결정을 알고 있을 때, 불법성에 대한 실질적 인식을 갖고 있는 것으로 여겼다.

그 동안 저작권 소유자로부터의 상세한 통지에 의해서도 유사한 객관적 사실이 성립되었다. 이 경우, 서비스제공자는 테러행위나 혐오발언 혐의 등 통지된 특정의 행위의 불법성 여부, 유럽연합 "시장에 출시된" 제품이 중고 또는 시험용 제품인지 여부와 같이 복잡한 문제에 대응해야 할 때가 있다.

따라서 실질적 인식은 다음과 같은 최소 요건을 충족하는 통지와 관련되어야 한다.

- 통지는 서면으로 이루어져야 한다.
- 통지자는 불법 혐의가 있는 콘텐츠의 구체적 항목에 대해 충분히 적시해야 한다(콘텐츠 유형에 대한 일반 설명, 즉 정보매개자가 해당 설명에 맞는 특정 항목을 찾기 위해 별도로 조사해야 하는 설명으로는 불충분함).
- 통지는 서비스제공자가 본 목적을 위해 개설한 별도 이메일 주소로 발송되어야 한다.
- 통지에는 문제되는 정보나 행위가 분명하게 명시되어야 한다.
- 통지에는 통지자가 침해 받았다고 주장하는 권리의 소유주임을 증명하는 증거가 제공되어야 한다.

- 통지에는 발행인 또는 저작물을 시중에 공개한 자가 자신의 권리를 침해하고 있으며 저작물의 발행 또는 공개의 법적 근거가 없다는 주장(라이선스나 법적용을 통해)을 포함해야 한다.
- 통지에는 관련 행위 또는 정보의 불법적 성격의 상세한 내용을 포함해야 한다.
- 통지에는 이상의 내용에 대한 사실성 및 정확성에 대한 주장과 이와 관련하여 취한 행동에 대해 책임을 인정한다는 주장이 포함되어야 한다.

이상의 최소 요건을 충족하는 통지를 통해, 이용자들의 저작권 침해를 주장하는 제3자의 경고에 의해 ISP가 "실질적 인식"을 갖게 되었다고 본 최근의 이탈리아 판례는 주목할 만하다.

법원은 ISP의 유일한 의무는 경고장에 포함된 저작권 침해 주장과 관련된 모든 정보를 관할 기관(즉 검찰 및 통신부)에 전달하는 것이라고 판결했다(2010년 로마지방법원 명령 no.415).

2. 자발적 업계 협약

이상의 내용은 서비스제공업체가 자율 협약과 성립될 수 있는 기타 실질적 인지수단들에 따라 수행할 수 있는 적발과 콘텐츠 삭제의 절차를 침해하지 않는다. 이러한 절차는 유럽 공동체 지침에 명시된 협조의 자발적 메커니즘이며 이를 통해 이해당사자가 불법이라고 주장된 행동이 있음을 ISP가 불법이라고 알려진 콘텐츠를 검토하고 필요에 따라 이를 삭제 또는 그 접근을 제한할 타당성을 평가하게 만들 목적으로 ISP에게 보고할 수 있다.

그럼에도 불구하고 EuroISPA는 자발적 업계 협약 체결 시, 몇몇 요건이 고려되어야 한다고 믿는다.

이는 ISP와 그 책임의 제한과 관련한 합법적 확실성을 강화하고, 협약 당사자들과 함께 진정한 협력에 이르는 바탕을 마련하기 위한 목적도 있다. 원칙적으로 제12~15조는 자발적 업계 협약으로 영향을 받아서는 안 된다. 특히 어떤 자발적 협약도 실질적 인식에 대한 추정을 일으켜 서비스제공자가 책임에 노출되도록 하는 일은 없어야 한다.

3. 제14조: “신속하게”

서비스제공업체는 정보의 불법성을 인지한 즉시 이를 신속하게 삭제하거나 접근을 막아야 한다. 지침은 이 요건을 정의하고 있지 않으며 “정보의 삭제 또는 제한을 두기에 앞서 신속하게 충족시켜야 하는 구체적 요건[을 설립]”(제정취지recital 46)하는 것을 회원국의 몫으로 둔다.

일반적으로 “신속하게”라는 개념 때문에 사건 별로 평가하기 위해 필요한 유연성이 제공된다. 특정 사건의 개별 상황과 무관하게 규정할 수는 없다.

자발적 메커니즘의 경우, 법원으로부터 통보를 받아 서비스제공자의 신속한 행위가 필요할 경우에는 별도의 평가가 필요하다. 전자의 사건에서는 정보매재자에게 합법적 확실성이 존재하나, 후자의 경우에는 정보매재자가 삭제 혹은 제한을 두기로 한 콘텐츠의 불법성 여부를 결정하기 위해 필요한 확실성의 모든 요소나 수준을 갖추고 있는가와 상관없이 신고 받은 즉시 행동을 취해야 할 수 있다. 이러한 경우, 신속한 삭제를 요구한다면 필요이상으로 피해 받는 사람에게 지대한 영향을 미쳐 불법이 아닌 웹사이트나 콘텐츠에 대한 접근 제한을 초래할 수 있다.

4. 제14조: 통지 및 삭제(notice-and-takedown)

지침 제14조의 불법이라고 주장된 콘텐츠 관련 호스팅서비스제공자에 대한 신고 절차는 “실질적 인식” 또는 “사실이나 정황에 대한 인지”를 성립시키기 위해 채택해야 할 메커니즘을 명확하게 정의하고 있지 않다. 그 결과 그 동안 회원국 별로 다양한 방법이 채택되었고 이를 다음과 같이 분류할 수 있다.

a 관할 사법당국에 의한 공식 통보(통지삭제): 이 방법은 실질적 인식을 확보하고 정보매개자에게 합법적 확실성을 제공한다.

b 실질적 인식을 결정하는 간단한 통지: 해당 통지가 공식 혹은 비공식 경로로 내려질 수 있다는 사실로부터 몇 가지 단점을 지적할 수 있음; 불법성의 입증은 제공자의 책임(즉 명백한 불법 vs 복잡한 문의절차); 이러한 시스템의 리스크는 정보매재자가 책임을 면하기 위해 제대로 된 합법성에 대한 평가 없이 모든 통지에 대해 통지삭제를 적용하는 것이다. 앞서 언급한대로 관련된 모든 이해당사자들에게 법적 불확실성을 줄이기 위해 서비스제공자가 언제 “실질적 인식”을 하였는가와 관련해 최소한의 요건을 명확하게 정의하는 것은 매우 중요하다. 영국법은 Question 53에 나열된 바와 유사한 요건을 규정하고 있다.

c 제정법상의 요건: 일부 국가는 공식 혹은 단순 통지 절차를 제공하고 있지 않으며 법원이 준수해야 하는 일련의 특정 요건을 정하고 있다(정보의 위치, 특성, 발신자의 상세 연락처 등).

EuroISPA는 통지 및 차단유지(notice and stay down) 또는 이중 통지(notice and notice) 절차의 도입은 종합적으로 평가되어야 한다고 믿는다. 이러한 절차의 성립이 부가적 가치를 가질 것이라고는 생각하지 않는다. 원칙적으로 법적 분쟁은 이해당사자간에 직접적으로 해결되어야 한다. 정보매재자 역할을 하는 ISP는 관련되지 않은 제3자이다. EuroISPA는 성립된 책임 체계를 약화시킬 의무를 부과하고 법적 불확실성을 일으킬 수 있는 이러한 절차의 실효성에 의문을 갖고 있다. 나아가 ISP가 정보매재자 역할에 있어 불법 콘텐츠를 판별하는 법관이 되지 않도록 확실한 안전장치가 필요하다.

4-1. 이중 통지(notice and notice)

EuroISPA는 추가적인 통지 절차가 분쟁의 원만한 해결과 정당한 책임 분배(해당 콘텐츠의 합법성에 대해 이견을 가진 양당사자에게 책임)의 방법이 될 수 있다고 믿는다. 이와 같은 시스템은 호스팅서비스제공자의 경우에만 고려할 수 있으며 통지의 전달에 국한된다. 프라이버시법과 통신비밀은 존중되어야 하며 기본권도 엄격하게 존중되어야 한다.

나아가 2차에 걸친 통지와 같은 모든 통지 절차는 다음과 같은 일반 가정에 기반하여 고려해야 한다.

- 정보매재자 면책
- 일반적 감시의무 금지 원칙 유지
- 잘못 통지한 자에 대한 제재의 도임

4-2. 통지 및 차단유지(notice and stay down)

EuroISPA는 이러한 시스템은 법적 불확실성을 높이고 ISP가 콘텐츠의 불법성을 결정하는 판결자로 만들며, 이용자간 커뮤니케이션에 지속적인 필터링과 모니터링을 강요하는 동시에 판사의 개입을 완전히 우회하게 만든다고 믿는다.

이와 같은 필터링 및 모니터링 방법은 이행에 큰 비용이 들고 이용자의 근본적인 권리를 침해할 위험이 있을 뿐만 아니라 그 효과가 검증되지도 않았다.

실제로 “통지 및 차단유지”는 특정 콘텐츠의 삭제요청을 처리하기 위해서 호스팅업체는 지속적으로 자사 서비스를 모니터링해 신고된 내용물의 재등록을 감시해야 하기 때문에 제15조의 “감시 의무 금지” 원칙과 양립될 수 없다. 또한 동일 파일에 대한 정확한 디지털 복사본을 지목할 정도로 통지 내용의 범위가 극히 좁지 않는 한 통지 및 차단유지는 이행이 불가능하다(예를 들면 명예훼손적 콘텐츠의 삭제 및 지속적인 통제는 동일한 주장이 다른 문구로 반복하여 재등장하는 것까지 포함한다고 할 수 없다).

5. 필터링 조치

필터링에 대한 논의는 어떠한 경우에도 기술적 타당성에 국한되어서는 안되며 유럽연합 집행위원회로부터 기대할 수 있는 가장 중요한 질문은 유럽의 가치와 경제적 이해에 비추어 필터링 방법을 논하는 것 자체가 바람직한가 이다. 이와 같은 방법은 장벽과 차단장치를 피해 정보전달의 다른 경로를 찾도록 설계된 인터넷과 같이 복원력이 큰 환경에 효과적으로 시행하기 어렵다. 정보통신제공업체의 역할이 p2p 네트워크 등과 같이 실시간 전송의 “단순도관(mere conduit)”에 불과한 상황에서는 더더욱 그러하다. 이러한 조치의 실행 불가능한 측면은 다음과 같은 이유에 근거한다.

기술적 시각: 효과적인 필터링이 불가능. 우회가 쉬우며 모든 콘텐츠가 영향을 받는다(특히 합법적 콘텐츠). 네트워크 복원력, 보안, 인프라의 효율성에 대한 충격과 역효과를 미친다. 모든 콘텐츠는 ISP 네트워크의 중앙집중화된 필터링 인프라로 이동시켜 검사를 거쳐야 한다. 콘텐츠와 이용자에 대한 통상적인 모니터링은 과도한 차단의 가능성과 같은 부수적인 피해에 대한 리스크가 크다.

보다 광의의 시각:

- 필터링 조치는 기본권의 침해와 관련해 뻔한 결과를 초래할 것임.
- 비상업적인 정보서비스제공자가 필터링 기술을 운영할 것으로 기대할 수 없음.
- 서비스제공자에게 인프라와 인력에 대한 소요되는 투자는 부담이 되며, 유럽 정보사회 발전에 상당하고 지속적으로 부정적인 영향을 줄 것임. “임무 과잉”의 리스크, 즉 특정 이슈에 대응하는 것으로 시작해 모니터링을 다른 이슈들로 확대할 위험도 있으며;
- “기술 과잉”의 리스크, 즉 인터넷 통신의 기술발전(암호화 등)에 발맞춰 필터를 지속적으로 업데이트해야 할 위험이 있다. 필터링은 암호화된 프로토콜의 개발과 위법한 사용 및 서비스에 대응하기 위한 끝없는 투자로 이어져(문제의 근본원인에 대처하는 대신에) 결국 고비용의 효과 없는 조치가 될 것이다.

또한 인터넷 접속서비스제공자가 자사 네트워크로 전송되는 데이터(혹은 그 일부)와 관련하여 적극적으로 필터링 기술을 출시해야 한다면 이는 의도하지 않게 접속서비스제공자가 자사 네트워크로 전송된 정보와 관련하여 전송된 정보를 선택 또는 수정하지 않는 한 모든 책임을 면책하는 지침 제12조의 적용을 무력화시키는 결과를 초래한다는 주장이 제기될 수 있다. 하지만 필터가 “단순한 기술적 도구”라는 이유로 전송된 정보의 선택을 시사하지는 않는다고 한다면 면책이 해지되어 결과적으로 서비스제공자는 자사 네트워크에 사용된 필터 기술의, 예를 들어 불법 콘텐츠를 차단하지 못하는 등의 결함에 대해 책임을 져야 할 위험에 처한다. 다시 말해, ISP를 “단순도관”으로 특징짓는 것은 서비스업체, 그 고객, 그리고 기본권에 대한 존중 모두에 심각한 결과를 초래하는 등 위태로울 수 있다.

기술솔루션 “Audible Magic”이 p2p 트래픽에 대한 필터 기술 후보로 제안된 벨기에의 Scarlet-SABAM 건의 판례 맥락에서 보듯이, 벨기에 법원은 필터링이 효과는 물론 대규

모 확장성도 없다고 봐도 무방하다고 인정했다. 물론 한 기술로 커뮤니케이션의 합법/불법성에 기초해 이를 완벽하게 구분한다거나 심지어 파일 내 내용을 알아내는 것조차 불가능해 보인다. 필터 기술과 직접적 관련이 없으나 예를 들면 저자 또는 저작권 협회에 의한 허가 또는 구체적인 라이선스 조건과 관련된 구체적 내용, 그리고 저작권에 대한 법적 예외에 의한 간섭 가능성에 따라 달라질 수 있다.

6. 비례성

앞서 언급한 바와 같이, 기존 네트워크 필터링 기술이 당초 목적달성에 효과적일 것인가에 대해 상당히 회의적인 시각이 있으며, 특히 해당 기술보다 "한발 앞서기" 위해 이용자들은 상대적으로 단순한 암호화 기법을 사용하기만 해도 되기에 더더욱 회의적이다. p2p 트래픽의 암호화는 이미 빠르게 이루어지고 있으며, 필터링 조치도 결국 검사를 피하기 위한 암호화 기술의 보편적 사용을 장려하게 될 뿐이다. 동시에 필터링은 네트워크 서비스, 이용자 경험의 품질저하, 그리고 합법적 콘텐츠에 대해 의도하지 않은 접근차단을 초래할 위험이 있다. 또한 이와 같은 기술로 증가된 비용은 디지털 불평등 해소에 더 큰 장벽을 만들게 할 것이다.

세계지적재산권기구(WIPO) 협정과 정보사회의 저작권 지침(2001/29/EC)에 상세히 명시된 바와 같이, 정당하고 합의된 목적을 위한 저작권 예외는 지적재산권법 제정에서 인정되고 이견이 없는 부분이다. 사용자가 저작권을 침해하지는 않지만 "승인된" 파일만 통과시키는 네트워크 필터링 기술로 "걸러질" 위험이 있는 파일들을 교환하는 것이 얼마든지 가능하다. 그 동안 EU와 유럽 평의회는 지난 수년간 전세계에서 발언과 정보접근의 자유를 전파하기 위한 선도적 지위에 있었다. 현 기술의 활용을 극대화하는 동시에 정당한 이용자들의 행태가 제한되지 않도록 보장할 현존하는 필터링 기술은 없다.

불법이라고 주장된 활동으로 어떠한 형태의 이익도 취하지 않는 정보매개자가 어느 수준까지 네트워크 필터링 기술에 투자하거나 투자해야 할 때, 비례성에 맞거나 적어도 바람직하다고 여길 수 있을까?

위 기술이 암호화된 파일 문제에 대해 해법이 될 수 없으며, 해법을 기대할 수도 없다는, 즉 ISP가 이러한 기술에 많은 투자를 해도 단기적으로 무의미한 투자였음을 알게 될 것이라는 광범위한 합의가 있다는 점을 고려할 때, 이러한 방법은 얼마다 더 용인하기 힘들게 될까?

더 크게 보면, 합법적 콘텐츠에 접근이 차단되거나 크로스보더 효과가 발생(예를 들어, 합법적인 콘텐츠가 다른 국가에서 불법이라는 이유로 접근 불가하게 되는)하도록 필터링을 적용하는 것은 국제적인 법적 결과를 초래하게 된다. 시민적 및 정치적 권리에 관한 UN 규약(제19조)은 "모든 사람은 표현의 자유를 가지며; 여기에는 국경과 관계없이 구두, 서면, 혹은 인쇄로, 예술의 형태 또는 선택가능 한 모든 매체를 통해 모든 유형의 정보와 아이디어를 탐구, 수령, 전파하는 자유가 포함된다"고 명시하고 있다. 유럽 인권협약에도 유사한 문구가 있다.

유럽 공동체 지침 제15조에 따른 일반적 의무 조항은 충분히 유연하고 잘 명시되어 공공 당국이 ISP에 추가적인 의무부과가 가능한 것으로 입증되었다. 실제로 "일반적인" 모니터링 의무가 금지된다고 해도 회원국은 ISP에 대해 사건 별로 "특정되고, 한정되며, 분명한" 의무를 부과할 수 있다. 이러한 해석은 법원이 불법행위에 대한 법적 책임이 없는 ISP에게도 여전히 명령을 통해 침해의 중단 또는 예방을 요구할 수 있다고 추가적으로 명시하고 있는 지침의 개정설명 47조에 의해서도 확인되고 있다. 그럼에도 불구하고 특정된 의무를 부과할 때, 공공기관은 해당 조치가 일반적 모니터링에 준하는 효과를 일으키는 것을 방지하기 위해 그 범위에 대해 세심한 검토가 있어야 한다.

* * *

전자상거래 지침 관련조항:

제4부 정보매개서비스제공자의 책임

제12조
"단순도관(Mere conduit)"

1. 통신망에서 서비스 수혜자에 의한 정보의 전송 또는 통신망으로의 접속 제공을 포함한 정보사회 서비스가 제공되는 경우, 회원국은 해당 서비스제공자가 다음의 조건에 해당하는 한, 전송된 정보에 대해 서비스제공자의 면책을 보장해야 한다.

a 전송을 개시하지 않을 것
b 전송의 수신자를 선택하지 않을 것
c 전송에 포함된 정보를 선택 또는 수정하지 않을 것

2. 제1항의 전송 및 접속제공 행위에는 통신망에서 전송을 실행할 목적으로만 발생하고, 해당 정보가 전송에 합리적으로 필요한 기간보다 초과하여 저장되지 아니하는 한, 송신된 정보의 자동적이고, 매개적이며, 임시적인 저장이 포함된다.

3. 본 조는 법원 또는 행정당국이 회원국의 법체계에 따라 서비스제공자에게 침해의 중단 혹은 예방을 요구할 가능성에 영향을 주지 않는다.

제13조
"캐싱(Caching)"

1. 정보통신망에서 서비스 수혜자에 의한 정보의 전송을 포함한 정보사회 서비스가 제공되는 경우, 회원국은 다른 서비스 수혜자의 요청에 의한 그 수혜자에 대해 이루어지는 정보의 계속적 전송을 더 효율화하기 위한 목적으로만 실행된 정보의 자동적이고, 매개적이며, 임시적인 저장에 대해 다음의 조건 하에서 서비스제공자의 면책을 보장해야 한다.

a 제공자가 해당 정보를 수정하지 않을 것;
b 제공자가 해당 정보에 대한 접근 요건을 준수할 것;
c 제공자가 업계에서 폭넓게 인정되고 사용되는 방식으로 명시된 정보의 갱신에 관한 규칙을 준수할 것;
d 제공자가 해당 정보의 이용에 대한 자료 취득에 있어 업계에서 폭넓게 인정되고 사용되는 기술의 합법적 이용에 개입하지 않을 것; 그리고
e 제공자가 전송의 원천에 있는 정보가 통신망에서 삭제 또는 접근 제한되었거나 법원 또는 행정당국이 이와 같은 삭제 또는 제한을 명령했다는 사실에 대해 실질적으로 인지한 즉시 저장한 해당 정보를 신속하게 삭제 또는 제한할 것

2. 본 조는 법원 또는 행정당국이 회원국의 법체계에 따라 서비스제공자에게 침해의 중단 혹은 예방을 요구할 가능성에 영향을 주지 않는다.

제14조:
호스팅(Hosting)

1. 서비스 수혜자가 제공한 정보의 저장으로 구성된 정보사회 서비스가 제공되는 경우, 회원국은 서비스 수혜자의 요청에 의해 저장된 정보에 대해 다음의 조건 하에서 서비스제공자의 면책을 보장해야 한다.

a 제공자가 불법 행위나 불법 정보에 대해 **실질적 인식(actual knowledge)**이 없으며, 손해배상 청구와 관련하여 불법 행위 또는 불법 정보가 명백하게 드러난 사실 또는 정황을 인지하지 못할 것; 또는

b 제공자가 이와 같은 인식 또는 인지가 있을 경우 **신속하게** 해당 정보를 삭제하거나 그 접근을 금지했을 것

2. 제1항은 서비스수혜자가 제공자의 권한 또는 통제 하에 행동하는 경우에는 적용되지 않는다.

3. 본 조는 법원 또는 행정당국이 회원국의 법체계에 따라 서비스제공자에게 침해의 중단 혹은 예방을 요구할 가능성에 영향을 미치지 않으며, 회원국이 정보의 삭제 또는 그 접근의 금지를 규정하는 절차를 수립할 가능성에도 영향을 미치지 않는다.

제15조
일반적 모니터링 의무 금지

1. 회원국은 제12, 13, 14조가 적용되는 서비스의 제공 시, 서비스제공자가 자신이 전송 또는 저장하는 정보를 모니터링할 일반적 의무를 부과해서는 안되며, 불법 행위임을 드러내는 사실 또는 정황을 적극적으로 조사할 일반적 의무도 부과해서는 안 된다.

2. 회원국은 정보사회 서비스제공자에게 자사 서비스 수혜자에 의해 행하여진 불법이라고 주장되는 행위 또는 이들이 제공한 정보에 대해 관할 당국에 지체 없이 알려야 할 의무 또는 서비스제공자가 저장계약을 맺은 자사 서비스 수혜자의 신상을 파악할 수 있는 정보를 관할 당국의 요청에 따라 제공할 의무를 규정할 수 있다.

Session 3

Intermediary Liability and Copyright

정보매개자 책임과
저작권 제도

Main Speaker / 주제 발표

Eric Goldman
에릭 골드먼

▪ Professor of Law at Santa Clara University School of Law

Eric Goldman is a Professor of Law at Santa Clara University School of Law. He also directs the school's High Tech Law Institute. Before joining the SCU faculty in 2006, he was an Assistant Professor at Marquette University Law School, General Counsel of Epinions.com, and an Internet transactional attorney at Coley Godward LLP.

Eric teaches and publishes in the areas of Internet Law, Intellectual Property and Advertising & Marketing Law. He blogs on these topics at the Technology & Marketing Law Blog, which has been named to the ABA Journal Blawg 100 every year since 2009, and the Tertium Quid blog at Forbes. Since 2002, he has made over 280 public presentations and over 1,600 media appearances. In 2011, the California State Bar's IP Section named him the "IP Vanguard" award winner (in the academic/public policy category), and in 2012 and 2013, Managing IP magazine named him to a shortlist of "IP Thought Leaders" in North America.

Eric received his BA, summa cum laude and Phi Beta Kappa, in Economics/ Business from UCLA in 1988. He received his JD from UCLA in 1994, where he was a member of the UCLA Law Review, and concurrently received his MBA from the Anderson School at UCLA.

Main Speaker / 주제 발표

Rebecca Giblin
레베카 깁린

▪ Senior Lecturer at Monash University Faculty of Law

Informed by her early career as an information technology consultant, Rebecca's research focuses primarily on copyright law and the regulation of the internet and emerging technologies. Her book Code Wars (Edward Elgar, 2011, www.codewarsbook.com) recounts the legal and technological history of the first decade of the P2P file sharing era, focusing on the innovative and anarchic ways in which P2P technologies evolved in response to decisions reached by courts with regard to their predecessors. Rebecca's recent major research paper 'Evaluating Graduated Response' critically evaluates the extent to which the big claims that are being made about the success and efficacy of global graduated responses are supported by the available evidence.

Current research interests include exploring the elusive notion of 'the public interest' in copyright, working towards a new flexible exceptions framework in Australia, further developing her work on anti–regulatory code and understanding the regulatory challenges posed to libraries as they shift to elending. Rebecca is a Senior Lecturer within Monash University's law faculty and sits on the Board of the Australian Digital Alliance. During 2011 Rebecca was the Kernochan Visiting International Intellectual Property Scholar at Columbia Law School in New York, and in 2013 a Senior Visiting Scholar in residence at Berkeley Law School. During 2013 and 2014 her work was partly funded by the Monash University Research Accelerator Program.

Moderator / 좌장

Park, Deok-Young
박덕영

▪ –	LL.M. 법학석사	University of Cambridge 영국 캠브리지대학교
▪ –	Ph.D. 박사	Graduate School of Law, Yonsei University 연세대학교 대학원 법학
▪ –	M.A. 석사	Graduate School of Law, Yonsei University 연세대학교 대학원 법학
▪ Present	Associate Professor 부교수	Yonsei University Law School 연세대학교 법학전문대학원
▪ Present	Head 센터장	EU Law Center, Yonsei University 연세대학교 EU법센터
▪ 2012	President 회장	Korean Society of International Economic Law 한국국제경제법학회

Panelists / 토론자

Lee, Kyuhong
이규홍

▪ 2009	Ph.D 박사	Graduate School of Law, Yonsei University (copyright law) 연세대학교 일반대학원 (저작권법)
▪ Present	Presiding judge 부장판사	Seoul Central District Court, specialized at IP 서울중앙지방법원 지재전담
▪ 2013	Presiding Judge 부장판사	Uijeongbu District Court, Goyang branch 의정부지방법원 고양지원
▪ 2011	Professor 교수	Judicial Research and Training Institute 사법연수원
▪ 2010	Presiding Judge 부장판사	Daejon District Court 대전지방법원
▪ 2009	Judge 판사	Seoul High Court, specialized at IP 서울고등법원 (지적재산권 전담부)

Panelists / 토론자

Jung, Pilwoon
정필운

▪ –	Ph.D. 박사	Graduate School of Law, Yonsei University 연세대학교 대학원 법학
▪ Present	Professor 교수	Korea National University of Education 한국교원대학교
▪ Present	Director of General Affairs 총무이사	Korea Internet Law Association 한국인터넷법학회
▪ Present	Director 이사	Korean Constitutional Law Association 한국헌법학회
▪ Present	Director of General Affairs 총무이사	Association of Korea Constitutional Case Law Studies 한국헌법판례연구학회
▪ Present	Director of Planning 기획이사	Korean Society of Media Law, Ethics and Policy Research 한국언론법학회

Panelists / 토론자

Choe, Kyong-Soo
최경수

▪ 1992	Ph.D. 박사	Graduate School of Law, Korea University (International Economic Law) 고려대학교 일반대학원 법학
▪ 1987	LL.M. 법학석사	School of Law, University of Dundee 영국 던디대학교 법과대학
▪ 1984	M.A. 석사	Graduate School of Law, Korea University 고려대학교 일반대학원 법학
▪ Present	Chief Senior Researcher 수석연구위원	Korea Copyright Commission 한국저작권위원회
▪ 2011 ~ 2015	Director General 실장	Copyright Research Office, Korea Copyright Commission 한국저작권위원회 정책연구실
▪ 2007	Vice President 부회장	Korea Copyright Law Association 한국저작권법학회
▪ 2006 ~ 2007	Government delegate 한국정부대표	Korea-U.S. and Korea-EU FTA IPR Negotiations 한미, 한EU FTA 지적재산권 분야

Main Speaker / 주제발표

ISP Liability under DMCA

Prof. **Eric Goldman**
(Santa Clara University School of Law)

미국 디지털밀레니엄저작권법(DMCA)상
ISP의 책임

에릭 골드먼 교수 (미 산타클라라대 로스쿨)

How the DMCA's Online Copyright Safe Harbor Failed

DOI: 10.6521/NTUTJIPLM.2014.3(2).10

Quick View

Ⅰ. Introduction

In 1998, Congress enacted the Digital Millennium Copyright Act ("DMCA"). One of its provisions, 17 U.S.C. § 512, gave online service providers a safe harbor from liability for user-caused copyright infringements. The web hosting safe harbor's structure was relatively simple: copyright owners assume the burden of notifying service providers when their users are committing copyright infringement, at which point the service providers are expected to intervene if they want to avoid being liable. This system, called "notice-and-takedown," has served the Internet well enough to create many interesting and important user-generated content websites.

Unfortunately, 15 years of relentless litigation by the copyright industry has created a number of cracks in the notice-and-takedown system. As a result, the notice-and-takedown system is failing as a safe harbor, progressively undermining

the safe harbor's ability to foster entrepreneurship in the user-generated content industry. This Essay explains how cracks in the safe harbor are rendering it useless.

Ⅱ. Background

Copyright law is a strict liability tort. That means a person is liable for copyright infringement if their actions violate a copyright owner's rights, even if they had no idea they were doing so. In the mid-1990s, a few cases suggested that online service providers could be strictly liable for user-caused copyright infringement, even if the service providers didn't know that its users were doing so.[1]

These cases prompted the DMCA safe harbor codified in 17 U.S.C. § 512(c), which created the notice-and-takedown system. Its key innovation is that online service providers aren't strictly liable for user-caused copyright infringement; service providers should be liable only if they get a takedown notice from copyright owners and then fail to respond quickly. Indeed, the statute spells out what information needs to be in a takedown notice before it creates the obligation for service providers to act.[2] Thus, it's clear Congress wanted to override copyright law's strict liability default rule for online service providers and require copyright owners to take affirmative steps outside the courtroom before they ran to the courtroom to sue user-generated content websites.

From the beginning, copyright owners quickly realized that sending takedown notices was a chore.[3] As a result, copyright owners have repeatedly sued service providers for user-caused copyright infringement even where the copyright owners haven't sent takedown notices.[4] Naturally, if copyright owners could establish service provider liability without the need to send takedown notices, it would effectively render Section 512(c)'s notice-and-takedown scheme moot.

Ⅳ. Undermining the Safe Harbor

Through aggressive litigation in court, copyright owners have made substantial progress in eviscerating the notice-and-takedown system, especially in the past two years or so. Some of the ways they have done so:

1 Pre-1972 Sound Recordings

In the GrooveShark case,[5] the court held that pre-1972 sound recordings-which are governed by state copyright law, not federal copyright law-are not covered by the notice-and-takedown scheme. Because a service provider allowing users to post sound recordings has no reliable automated way of distinguishing pre- and post-1972 works, service providers cannot rely on the notice-and-takedown for any sound recordings.[6]

2 Knowledge Requirement

Courts have established two ways that service providers can "know" about their users' infringing behavior even if copyright owners don't send takedown notices.

1) Professor of Law and Co-Director of the High Tech Law Institute, Santa Clara University School of Law; J.D./M.B.A., University of California, Los Angeles; B.A., University of California, Los Angeles. Contact email: egoldman@gmail.com. This article (without footnotes) was originally published at http://blog.ericgoldman.org/archives/2014/06/how-the-dmcas-online-copyright-safe-harbor-failed.htm.
2) See, e.g., Playboy Enterprises, Inc. v. Frena, 839 F. Supp. 1552 (M.D. Fla. 1993); Playboy Enterprises, Inc. v. Russ Hardenburgh, 982 F. Supp. 503 (N.D. Ohio 1997).
3) 17 U.S.C. § 512(c)(3).
4) See, e.g., ALS Scan v. Remarq Communities, Inc., 239 F.3d 619 (4th Cir. 2001)
5) See, e.g., UMG Recordings, Inc. v. Shelter Capital Partners LLC, 667 F.3d 1022 (9th Cir. 2011); Viacom Int'l Inc. v. YouTube, Inc., 676 F.3d 19 (2d Cir. 2012) (Viacom sued YouTube even though Viacom waited some time to send 100,000 takedown notices and YouTube immediately processed them).
6) UMG Recordings, Inc. v. Escape Media Group, Inc., 107 A.D.3d 51, 964 N.Y.S.2d 106 (N.Y.A.D. 1 Dept. 2013).

First, courts have added a new safe harbor exclusion called "willful blindness."[7] This exclusion doesn't have a rigorous definition–courts are still trying to figure out what it means[8]–and the courts created this exclusion even though the statute specifically described what types of information about user conduct could foreclose the safe harbor.

Second, the courts have said that "inducing" infringement also likely forecloses the safe harbor.[9] We have clearer definitions of what constitutes inducement, though inducement arguments have rarely succeeded outside the peer-to-peer file sharing context. Nevertheless, lawsuits against user-generated content websites routinely allege inducement, consuming substantial litigation expenses for both parties.

3 Investors' Liability

Courts have indicated that investors in online service providers aren't covered by Section 512[10]–leading the potentially anomalous conclusion that investors may be liable for copyright infringement even when the companies they've invested in aren't. Naturally, exposing investors to personal risk for making investments in user-generate content websites is a pretty effective way of discouraging those investments.

* * *

These three exclusions undermine the safe harbor in two ways. First, they prevent user-generated content websites from relying on the notice-and-takedown system. Simply responding to copyright owner takedown notices isn't enough to keep a service provider out of court.

Second, more problematically, copyright owners can drain defendants' coffers of lots of money seeking evidence to support these exceptions,[11] even if the copyright owners ultimately lose in court. This ensures that well-funded copyright owners can drive entrepreneurs out of business simply through aggressive litigation, regardless of the merits;[12] and it substantially raises the amount of cash required to enter the user-generated content business, as a portion (effectively, the first funds raised) must be set aside for the seemingly inevitable and quite expensive ligation that will surely ensue.

Ⅳ. Implications

For all of the angst about SOPA's evisceration of notice-and-takedown,[13] it's clear that the notice-and-takedown system is dying without any legislative intervention. Congress attempted to articulate a pretty clear rule: users who upload infringing files are liable; their web hosts aren't unless they ignore takedown notices. Somehow, the courts have gotten far enough away from this basic proposition that now copyright owners have plenty of leverage over user-generated content websites without ever sending them takedown notices at all. Perhaps Section 512's failure isn't surprising; in retrospect, it's pretty clear Congress misarchitected Section 512.[14] Despite that, Congress isn't likely to consider meaningful defendant-favorable reform any time soon.

7) See Eric Goldman, More Evidence That Congress Misaligned the DMCA Online Copyright Safe Harbors (UMG v. Grooveshark), http://www.forbes.com/sites/ericgoldman/2013/04/24/more-evidence-that-congress-misaligned-its-online-copyright-safe-harbors-umg-v-grooveshark/ (last visited Dec. 2, 2014).
8) See Viacom Int'l Inc. v. YouTube, Inc., 676 F.3d 19 (2d Cir. 2012); UMG Recordings, Inc. v. Shelter Capital Partners LLC, 718 F.3d 1006 (9th Cir. 2013).
9) See, e.g., the Ninth Circuit's baffling quadruple-negative articulation of the doctrine: "the DMCA recognizes that service providers who do not locate and remove infringing materials they do not specifically know of should not suffer the loss of safe harbor protection." UMG Recordings, Inc. v. Shelter Capital Partners LLC, 718 F.3d 1006 (9th Cir. 2013).
10) Columbia Pictures Industries, Inc. v. Fung, 710 F.3d 1020 (9th Cir. 2013).
11) UMG Recordings, Inc. v. Shelter Capital Partners LLC, 718 F.3d 1006 (9th Cir. 2013).
12) For example, YouTube spent $100M just to file its summary judgment motion in the Viacom case. Erick Schonfeld, Google Spent $100 Million Defending Against Viacom's $1 Billion Lawsuit, http://techcrunch.com/2010/07/15/google-viacom-100-million-lawsuit/ (last visited Dec. 2, 2014).
13) The most obvious example is Veoh, which won its Ninth Circuit case after it had gone bankrupt. Eric Goldman, UMG v. Shelter Capital: A Cautionary Tale of Rightsowner Overzealousness, http://blog.ericgoldman.org/archives/2011/12/umg_v_shelter_c.htm (last visited Dec. 2, 2014).
14) See Eric Goldman, Celebrating (?) the Six-Month Anniversary of SOPA's Demise, http://www.forbes.com/sites/ericgoldman/2012/07/18/celebrating-the-six-month-anniversary-of-sopa-demise/ (last visited Dec. 2, 2014).

Cited as

Bluebook. Style: Eric Goldman, How the DMCA 's Online Copyright Safe Harbor Failed, 3 NTUT J. OF INTELL. PROP. L. & MGMT. 195 {2014).

APA Style: Goldman, E. (2014). How the DMCA's online copyright safe harbor failed. NTUT Journal of Intellectual Property Law & Management, 3(2), 195-198.

OSCOLA Style: E Goldman, 'How the DMCA's Online Copyright Safe Harbor Failed' (2014) 3 NTUT Journal of Intellectual Property Law & Management 195.

DMCA의 온라인 저작권 피난처는 어떻게 실패했나

DOI: 10.6521/NTUTJIPLM.2014.3(2).10

간략보기

Ⅰ. 도입

1998년 미 의회는 디지털 밀레니엄 저작권법(이하 "DMCA")을 제정했다. 이 중 17 U.S.C. §512 조항은 온라인 서비스 제공자들에 사용자가 유발하는 저작권 침해 책임으로부터 피난처(safe harbor)를 제공한다. 웹 호스팅 피난처 구조는 비교적 단순한데, 저작권자들은 사용자들이 저작권을 침해할 때 서비스 제공자들에 이를 알리는 책임을 맡게 되며, 이때 서비스 제공자들은 책임을 지지 않으려면 개입해야 한다. "통지 및 삭제(notice-and-takedown)"이라 불리는 이 제도는 여러 흥미롭고 중요한 UCC 웹사이트가 탄생될 수 있도록 인터넷의 성장에 기여해 왔다.

불행히도 지난 15년간 저작권 산업계의 끊임없는 소송은 이 통지삭제 제도에 많은 균열을 가져왔다. 그 결과 이 제도는 피난처로서의 역할을 하지 못하고 UCC 산업에서 기업가정신을 촉진하는 피난처의 능력도 점차 줄어들게 되었다. 본 자료를 통해 균열로 인해 어떻게 피난처가 기능을 잃게 되었는지에 대해 설명하고자 한다.

Ⅱ. 배경

저작권법은 불법행위에 대해 엄격책임을 묻는다. 이는 한 개인이 모른 채 저작권자의 권리를 침해하는 경우에도 저작권 침해에 대한 책임을 져야 한다는 의미이다. 1990년대 중반 몇 가지 사례를 보면 온라인 서비스 제공자들은 사용자들이 저지른 저작권 침해에 대해 몰랐다고 할지라도 엄격책임을 져야 했다.[1)]

이러한 사례들로 인해 DMCA 피난처가 17 U.S.C. §512에 성문화되었고, 통지삭제 제도가 탄생했다. 가장 핵심적인 변화는 사용자들의 저작권 침해로 인해 온라인 서비스 제공자들에 엄격한 책임을 지우지 않는다는 점이다. 서비스 제공자들은 저작권자들로부터 통지를 받고도 즉각적인 조치를 취하지 않은 경우에만 책임을 지게 된다. 사실상 법률은 서비스 제공자가 취해야 할 조치를 명시하기 전에 어떠한 정보가 삭제통지서에 포함돼야 하는지 명시하고 있다.[2)] 따라서 의회는 온라인 서비스 제공자들을 위해 저작권법의 엄격책임 기본 규정을 무효화 하고, 저작권자들이 UCC 웹사이트에 대한 소송을 제기하고자 법원으로 달려가기 전에 법정 밖에서 시정 조치를 취하기를 원한 것이다.

처음부터 저작권자들은 삭제통지서를 보내는 것이 귀찮은 일이라는 사실을 즉시 깨달았다.[3)] 그 결과 저작권자들은 사용자들의 저작권 침해에 대해 삭제통지서를 송부하지 않았을 때조차 서비스 제공자들을 상대로 계속 소송을 제기했다.[4)] 저작권자들이 삭제통지서를 발송할 필요 없이 서비스 제공자의 법적 책임을 물을 수 있다면, 제512(c)절의 통지삭제 제도에 관한 논란은 야기될 수 밖에 없을 것이다.

1) 산타클라라대학교 법대, 법학과 교수 및 첨단법률협회 공동 소장; 로스엔젤레스 캘리포니아대학교 법학박사/M.B.A; 로스엔젤레스 캘리포니아대학교 학사. 연락처: egoldman@gmail.com. 본 논문(각주 제외)은 http://blog.ericgoldman.org/archives/2014/06/how-the-dmcas-online-copyright-safe-harbor-failed.htm에 최초 게재됨.
2) Playboy Enterprise, Inc. v. Frena 사건 참조, 839 F. Supp. 1552 (M.D. Fla. 1993); Playboy Enterprise, Inc. v. Russ Hardenburgh, 982 F. Supp. 503 (N.D. Ohio 1997)
3) 17 U.S.C. §512(c)(3)
4) ALS Scan v. Remarq Communities, Inc. 참조, 239 F.3d 619 (제4순회재판소, 2001)

Ⅲ. 피난처 침해

특히 지난 2년여간 법정에서 공격적인 소송을 통해 저작권자들은 통지삭제 제도를 무효화하는데 상당한 진전을 거뒀다. 이들이 사용한 방식은 다음과 같다.

1 1972년 이전 음원

GrooveShark 사건[5)]의 경우 법원은 연방 저작권법이 아닌 주 저작권법의 지배를 받는 1972년 이전 음원은 통지삭제제도의 대상이 아니라고 판결했다. 사용자들이 음원을 게시하도록 허용하는 서비스 제공자들이 1972년 이전과 이후 창작물을 자동으로 구분할 수 있는 신뢰할만한 방법이 없기 때문에 서비스 제공자들은 모든 음원에 대해 통지삭제 방식을 신뢰할 수 없다.[6)]

2 인지 요건

법원은 저작권자들이 삭제통지서를 발송하지 않더라도 서비스 제공업체들이 사용자들의 침해 행위에 대해 "알 수"있는 두 가지 방식을 규정했다. 첫째, 법원이 피난처에서 배제한다고 새롭게 추가한 것은 "의도적인 간과(willful blindness)"[7)]라고 불리는 것이다. 이에 대한 명확한 정의가 없고 법원은 여전히 의미를 파악하고자 노력하고 있으며,[8)] 법률이 사용자 행위에 대한 어떤 종류의 정보가 피난처를 박탈하는지 구체적으로 규정하고 있음에도 불구하고 법원은 이 같은 배제를 설정했다.

5) UMG Recordings, Inc. v. Shelter Capital Partners LLC, 667 F.3d 1022 (제9순회재판소, 2011); Viacom Int'l Inc. v. YouTube, Inc., 676 F.3d 19 (제2순회재판소, 2012) (바이어컴은 10만건의 삭제통지서를 발송하기 위해 기다리고 유튜브는 이들을 처리했지만 바이어컴은 유튜브를 상대로 소송을 제기했다)
6) UMG Recordings, Inc. v. Escape Media Group, Inc., 107 A.D.3d 51, 964 N.Y.S.2d 106 (N.Y.A.D. 1 Dept. 2013)
7) Eric Goldman, 『의회가 DMCA 온라인저작권 피난처를 잘못 설정했다는 추가 증거(UMG v. Grooveshark)』, http://www.forbes.com/sites/ericgoldman/2013/04/24/more-evidence-that-congress-misaligned-online -copyright-safe-harvors-umg-v-grooveshark/ (최종 수정 2014.12.2)
8) Viacom Int'l Inc. v. YouTube, Inc., 676 F.3d 19 (제2순회재판소, 2012); UMG Recordings, Inc. v. Shelter Capital Partners LLC, 718 F.3d 1006 (제9순회재판소, 2013)

둘째, 법원은 침해를 "유도하는(inducing)" 것도 피난처에서 배제된다고 판결했다.[9] 유도(inducement)라는 주장은 P2P 파일 공유 이외에 거의 성립된 적은 없지만 어떤 것이 유도에 해당되는지에 대한 보다 명확한 정의는 있다. 그럼에도 불구하고 UCC 웹사이트에 대한 소송에서 유도의 주장이 꾸준히 제기되고 있으며, 양 당사자 모두 이로 인해 상당한 소송 비용을 낭비하고 있다.

3 투자자 책임

법원이 온라인서비스 제공업체에 대한 투자자들은 제512절에 해당되지 않는다고 선고함으로써,[10] 투자를 받은 기업들이 책임이 없는 경우에도 투자자들은 저작권 침해에 대한 책임이 있을 수 있다는 이례적인 결론으로 이어졌다. 자연히 UCC 웹사이트에 투자함으로써 개인적인 위험에 노출되는 것은 이들 투자자들의 투자를 크게 감소시킬 수 있다.

* * *

이상의 3가지 배제는 두 가지 측면에서 피난처를 저해한다. 첫째, UCC 웹사이트가 통지삭제제도를 신뢰하지 못하게 만든다. 저작권자의 삭제통지에 대응하는 것만으로는 서비스 제공자들이 소송을 피할 수 없기 때문이다.

둘째, 더 큰 문제는 저작권자들이 결국 패소한다 할지라도 이러한 배제를 뒷받침하는 증거를 찾기 위해 피고인으로 하여금 막대한 소송 비용을 지불하게 할 수 있다는 것이다.[11] 이 경우 자금력이 좋은 저작권자들은 사건의 시시비비와 관계없이[12] 공격적인 소송을 통해 기업 파산도 야기할 수 있다. 또한, UCC 사업을 시작하는데 필요한 충분한 현금을 확보할 때 1차 모금액 등 일부는 반드시 발생하게 될 불가피하고 막대한 비용이 소요되는 소송을 위해 따로 비축해둬야 하는 상황이 발생된다.

9) 제9순회재판소의 이 정책에 대한 4중 부정 판결 참조: "DMCA는 서비스제공업체들이 구체적으로 알지 못하는 저작권 침해 자료의 위치를 파악하지 못하고 삭제하지 않은 경우 피난처 보호에서 배제되지 않는다고 인정한다"
10) Columbia Pictures Industries, Inc. v. Fung. 710 F.3d 1020 (제9순회재판소, 2013)
11) UMG Recordings, Inc. v. Shelter Capital Partners LLC. 718 F.3d 1006 (제9순회재판소, 2013)
12) 예를 들어 유튜브는 바이어콤과의 소송에서 약식판결 청구에만 1억을 사용했다. Google의 Erick Schonfeld는 바이어콤의 10억 달러 소송에서 변호에 1억 달러를 썼다. http://techchrunch.com/2010/07/15/google-viacom-100millionlawsuit (최종 수정 2014.12.2)

Ⅳ. 시사점

SOPA의 통지삭제 무효화에 대한 불안으로 인해[13] 통지삭제 제도가 입법부의 아무런 개입 없이 사장되어가고 있다는 점은 분명하다. 의회는 저작권 침해 파일을 올리는 사용자들에게 책임이 있고 삭제통지서에 대해 아무런 조치를 하지 않는 경우가 아닌 한 웹 호스트들은 책임이 없다는 상당히 분명한 규정을 만들고자 노력했다. 법원은 이러한 기본 명제로부터 크게 멀어져 이제 저작권자들이 삭제통지서를 발송하지 않고도 UCC 웹사이트에 대한 상당한 영향력을 발휘할 수 있게 됐다. 제512절의 실패는 그다지 놀랍지 않다. 돌이켜보면 의회가 제512절을 잘못 구성한 것이 자명하기 때문이다.[14] 그럼에도 불구하고 의회는 가까운 시일 내에 피고인들에게 우호적인 의미있는 개정을 고려할 것 같지는 않다.

인용방식

Bluebook 스타일: Eric Goldman, 『DMCA의 온라인 저작권 피난처는 어떻게 실패했나』, 3 NTUT J. INTELL. PROP. L. & MGMT. 195 (2014).

APA 스타일: Goldman, E.. (2014). DMCA의 온라인 저작권 피난처는 어떻게 실패했나, 『NTUT 저작권법 & 관리 저널』, 3(2), 195-198

OSCOLA 스타일: E Goldman, 'DMCA의 온라인 저작권 피난처는 어떻게 실패했나' (2014) 3 『NTUT 저작권법 & 관리 저널』 195

13) 가장 대표적인 사례가 베오(Veoh)로 파산 후 제9순회재판소 소송에서 승소했다. Eric Goldman, 『UMG v. Shelter Capital: 저작권자의 지나친 투기에 대한 경고 이야기』, http://blog.ericgoldman.org/archives/2011/12/umg v shelter c.htm (최종 수정 2014.12.2)
14) Eric Goldman, 『SOPA 서거 6개월 기념 축하(?)』, http://www.forbes.com/sites/ericgoldman/2012/07/18 / celebrating-the-six-month-anniversary-of-sopas-demise/ (최종 수정 2014.12.2)

Main Speaker / 주제발표

Evaluating Graduated Response

Dr. **Rebecca Giblin**
(Monash University Faculty of Law)

삼진아웃제에 대한
비교법적 평가

레베카 깁린 교수 (호주 모나쉬대)

Precis of Research Findings - Evaluating Graduated Response

This is a précis of the research results and ideas that will be presented by Dr Rebecca Giblin on 28 May 2015. Full results and citations are available in the accompanying peer-reviewed research paper: "Evaluating Graduated Response" (2014) 37 Columbia Journal of Law & the Arts 147-209.

RESEARCH PROJECT AND METHODOLOGY

The research results discussed in this document are drawn from an extensive study, conducted over 18 months, and examining each international jurisdiction that had a 'graduated response' copyright enforcement arrangement in its public law as of September 2013. It also examined two jurisdictions featuring equivalent private arrangements. The study sought to ascertain the extent to which claims that had been made regarding the efficacy of these schemes were supported by the available evidence. Its methodology involved evaluating, for each jurisdiction, the extent to which such arrangements had been demonstrated to:

a reduce copyright infringement;
b increase legitimate markets, and
c encourage the creation and dissemination of a variety of creative and cultural content.

The analysis discovered serious problems with the evidence in support of these schemes. This précis explains the main deficiencies and makes some suggestions about what that data might mean for the future.

DEFICIENCIES IN THE EVIDENCE

'Correlation' does not equal 'causation'

When two trends head in the same direction, people are sometimes confused into believing that one must cause the other. For example, when polio was endemic in the first half of the 20th century, children were widely warned against eating ice-cream. It had been observed that occurrence of polio increased in line with ice-cream sales, and that led to a belief that ice-cream was a cause of the disease. It was later established that, although there was indeed a correlation between polio outbreaks and ice-cream consumption, the one was not caused by the other. Instead, the correlation was explainable with reference to a third factor: polio outbreaks and icecream consumption both increased during warmer months. This story is a reminder that, just because there are two trends going in the same direction does not mean that one of them causes the other. At best, it means that one of them may cause the other. Further investigation is then required to confirm or disaffirm that connection.

Many of the claims about the efficacy of graduated response regimes suffer from the same confusion that created that fear of ice-cream, ie, they inaccurately equate correlation with causation. This is particularly apparent in claims that have been made internationally about the South Korean experience with graduated response.

South Korea has been commendably successful in reducing copyright infringement over the last few years. Lobbyists for additional copyright enforcement have sometimes made an argument that goes like this: 'South Korea has reduced piracy. South Korea has graduated response. Therefore, graduated response reduces piracy.' That is, they make the basic error of confusing correlation with causation. This simplistic analysis ignores the fact that there are a vast many other factors at play that might alternatively explain the reduction in infringement levels in South Korea, including increased education, the tremendous successes of local music, TV and movie industries, increased availability of legitimate access and regulatory enforcement measures other than graduated response. Despite exhaustive investigation, my research was unable to find any credible causal link between the introduction of a graduated response regime and reduced infringement in South Korea or any other jurisdiction. In a number of countries the picture is complicated further by considerable evidence of individuals switching to alternative sources of infringement in an attempt to avoid detection, rather than by forsaking infringement altogether. The most that can be said is that there may sometimes be a correlation, with further investigation necessary to determine any closer relationship.

The notice volume data fallacy

Graduated responses generally require several warnings to be issued before any punitive action is taken. Data regarding the relative number of first to second notices, and second to third notices, is commonly pointed to as evidence of the efficacy of such schemes. The reasoning goes that, if there are less second notices issued than first notices, and less third notices than second notices, that is evidence that the scheme is reducing infringement.

Such arguments are made particularly often in the case of the French law, which is known as Hadopi. Representatives of the recording industry have used the fact that 'as many as 95% of first notices from Hadopi do not give rise to a second notice [and] 92% of second notices do not give rise to a third' as evidence of reduced infringement. According to Hadopi, The International Federation of the Phonographic Industry ('IFPI') has similarly noted with approval that 'Hadopi has now sent more

than one million notices, with only 8 per cent of infringers receiving a second warning.' In the same vein, the President of the Commission in charge of the French scheme has said, '[t]he less third warnings we send . . . the more the law will have proven effective.'

Since notice volume data is used as evidence of the efficacy of graduated response so often and with such authority, it is worth specifically identifying the fallacies in the reasoning. In my analysis, I use the notice volume data from the French scheme as of July 2013 [inset below] to highlight three reasons why such claims are nonsense.

> *Hadopi notice volume data, July 2013:*
> *2,004,847 first notices had been issued (the issuance of first notices is a largely automatic process)*
> *201,288 second notices had been issued (the issuance of second notice is also a largely automatic process)*
> *710 'délibérations', or investigations, had been reported (during which human investigators consider whether subscribers who have received a third allegation should be referred to prosecutors)*

Reason 1:
failure to account for factors arising from the design of the scheme

First, a higher number of earlier than later notices will always be reflected in published figures because, by definition, subsequent notices cannot be issued to subscribers until after they have been issued with earlier ones. This creates an unavoidable time lag. Some idea about the extent of that lag can be gleaned from the Hadopi Commission's own figures, which show that no second notices were issued until five months after the issue of the earliest first notices, and no délibérations (ie, the human investigations which occur at the third stage) were undertaken until five months after the earliest second notices were sent. This suggests it is reasonable to

expect that users who have received an earlier notice will not receive a subsequent one for at least five months. This needs to be accounted for in comparing the number of notices issued at different stages. In the case of the French law, one way of doing so would be by comparing the number of first notices issued at any point in time with the number of second notices issued five months after that point.

Another explanation for the higher number of earlier notices than later ones is that, under the French scheme, a second notice can only be issued to any given subscriber if a second allegation is made within six months of the first. After that period expires, Hadopi can only respond to an allegation of infringement by issuing a new 'first' notice. Similarly, a third 'strike' can only arise within a year of the second. Thus it is entirely plausible that, over the thirty-four months of operation covered by the figures, some users received more than one 'first' or 'second' notice, causing an over-representation of those numbers without actually suggesting any reduction of infringement. As Hadopi has not released information detailing how many subscribers received more than one first or second notice on more than, this factor cannot be accounted for on the available data.

Reason 2:
mathematical probability

The second reason why this notice volume data says nothing about the efficacy of graduated response is because, under the French system, not every allegation necessarily gives rise to any notice at all. Though Hadopi does not publicly report on the number of infringement allegations it receives, publicly available court documents confirm that it acts on only a small percentage of allegations. Consistent with the available information, I conservatively assume that 12% of allegations actually gave rise to notices being issued. If that is the case, a person who receives a first notice has an exponentially lower chance of receiving a second notice, and a correspondingly lower chance of receiving a third one, even if they do not change their behaviour at all. That's because, if there is no behavioural change, the chance of an individual receiving a subsequent notice is entirely independent of whether or not he or she had

received one previously. Imagine a fisherman practising catch-and-release with 100 fish swimming in a pool. Given a 10% chance of being caught, 10 of those 100 fish will be captured and then thrown back into the water. In the next round, each fish has again the same 10% chance of being caught. The next 100 fish out of the water won't be exactly the same ones that were caught the first time: only a few will be unlucky enough to be hooked twice. On average, there should actually only be 1 fish being caught twice (being 10% of 10%). Similarly, if an infringing individual has a 12% chance of receiving a first notice, they have just a 12% of 12% (0.122, or 1.44%) chance of receiving a second notice. And they will have just a 12% of 12% of 12% (0.123, or 0.1728%) chance of proceeding to the third stage. As a result, based on the 2,004,847 first notices that were issued by July 2013, we could reasonably expect there to have been 240,581 second notices to be issued (or 191,982 if we also control for the estimated 5 month time lag between stages). In fact, 201,288 were actually issued. This suggests little correlation between receipt of notice and reduced infringement (or possibly even an inverse correlation, since more notices than we might expect were actually received once the time lag had been accounted for).

There is a much stronger correlation between the number of second notices issued and third stage investigations. Based on this probability calculus, we could have expected 24,155 third stage proceedings to have been initiated, or 16,674 if the time lag is controlled for. In fact, only 710 'délibérations' were reported. However, the relatively small number of enforcement actions cannot be taken in and of itself as saying anything meaningful about the effect of notices in impacting infringement. That would be like police claiming the fact of few arrests in and of itself as evidence that crime is low. In both scenarios we would need more information, such as: how many allegations are being made? How many are being acted upon? How many give rise to an investigation? How long is the backlog before the commencement of an investigation? In Hadopi's case, the circumstances suggest a number of factors which might explain the low number of investigations independent of changed user behavior, mostly relating to its lack of investigative resources. Recall that the third stage of the process requires significant human input. At the time of the study, Hadopi had never processed more than 64 third stage investigations in a single month. In August 2011 and 2012, the traditional French vacation month, it issued none at all (although it did

issue big numbers of automated first and second notices). In these circumstances, the number of délibérations cannot credibly be claimed to say anything about whether infringement was reduced.

Reason 3:
correlation and causation again..!

Though claims are repeatedly made that notice volume data proves the efficacy of graduated response, they cannot be given credibility if they do not control for any of the above factors.

If those factors were taken into account, it is possible that the data might show a correlation between receipt of notices and a reduction of infringement. Alternatively, as we see from the above model, it may show a correlation between receipt of notices and increased infringement. No matter which way the correlation flows however, that would not be enough in and of itself to support a claim that the receipt of notices increases or decreases infringement, because of course, correlation ≠ causation. Further investigation would be needed to ascertain whether there was any causal relationship between the issuance of notices and the achievement of any of graduated response's aims, using, for example, the methodology of a controlled experiment. My research was unable to discover any evidence of such a link.

Reliance on non-credible data

In addition to the scientific and logical fallacies that undermine the evidence in support of the efficacy of graduated responses, it is further damaged by a more general lack of scientific credibility. The vast majority of studies put forward as evidence of the efficacy of graduated responses worldwide:

1. have never been subject to peer review – the globally accepted measure of scientific rigour, accuracy and credibility; and/or
2. are funded by the same organisations lobbying for the wider global rollout of graduated response, or organisations with a strong vested interest in their widespread adoption (for example, companies whose business model is to issue the infringement allegations on which such systems are based); and/or
3. have non-transparent methodologies (ie only the 'final numbers' or 'summary of results' are provided, with no way of ascertaining how they were determined) and are not available to researchers or the public for review.

In fact, my research identified only two significant studies worldwide which had been submitted to peer review, had not been conducted or funded by graduated response lobbyists, and had transparent methodologies.

In the first, New Zealand researchers measured P2P traffic before and after the NZ graduated response law came into effect, observing a reduction of more than half. They also noticed that use of technologies which could be used to circumvent the scheme jumped significantly. A year later, a follow-up found some recovery in the amount of P2P traffic, though it was still less than before the scheme came into operation. They also found a further massive increase in the amount of HTTPs traffic. The researchers theorized that this was caused by a further shift to non-P2P infringement, which falls outside the NZ enforcement scheme. While this work is clearly of far greater scientific credibility than almost every other piece of 'evidence' used in support of the efficacy of graduated response, it still has significant limitations. It was based on very limited data points, and the researchers said they would need to examine the traffic mixes from all ISPs within and outside NZ before they could even consider claiming causation between the change and the new law. The study also did not control for the new services which started operating in NZ around the same time as the law came into operation, doubling the existing legal music offerings.

The second example, the Danaher study, is the only serious attempt to claim a link between graduated response and increased legitimate markets. It did this by graphing weekly iTunes sales data for France and a control group of other European countries against Google Trends data showing French searches for 'HADOPI' over the same period. Over this time period, French sales diverged from and remain above those of the control group. This study, known as the 'Danaher study', was another welcome addition to the evidence. Notably however, the effect it identified has never been replicated in the broader recorded music market. It was also contradicted by the Lescure Report, a comprehensive study commissioned by the French Government to evaluate Hadopi's effects. After considering all relevant evidence, including the Danaher study, the Lescure Report concluded that, even if Hadopi had caused some reduction in P2P infringement, it had overwhelmingly caused traffic to be diverted to other infringing sources rather than to legitimate markets.

With the exception of these two limited studies, the general quality of evidence relied upon in support of claims that graduated responses were effective was extremely poor.

LESSONS THAT MIGHT BE DRAWN FROM THESE RESULTS

My study has demonstrated that, while the well-resourced organisations advocating for the adoption and continuance of graduated response schemes have made big claims about their efficacy, those claims are not supported by the evidence.

When the theory that ISP enforcement was the key to improving outcomes for copyright industries first started being made, there was no data to confirm or disprove it. Now that some countries have experimented with the introduction of such schemes however, we have a much clearer picture of how the theory matches up with results. After a number of years, there is no clear causal link in any jurisdiction between

graduated response and reduced infringement, increased legitimate markets or more widespread production and dissemination of content.

In these circumstances, it is no surprise that regulators around the world seem to be looking for solutions elsewhere. No graduated response scheme has been enacted in the public law of any nation since 2011, and France has partially repealed its own scheme. In the absence of any credible evidence of benefit, and given the sizeable investments required to maintain them, those who have already enacted graduated responses might take this opportunity to consider the desirability of retention. Governments might also consider asking stakeholders to do more to help demonstrate that they are indeed achieving their aims. For example, rightholders are often in possession of data that might enable more scientifically rigorous evaluation of the impacts of such laws; perhaps they may be required to provide it to independent researchers. If graduated response schemes really do work as well as is often claimed, surely their proponents would welcome such analysis. At the very least, it is time to ask lobbyists to do more to justify the big claims that they make in order to ensure that law and policy are in line with the evidence.

삼진아웃제 평가

본 자료는 레베카 깁린(Rebecca Giblin) 박사가 2015년 5월 28일 발표할 연구 결과와 견해 개요이다. 전체 결과와 인용은 첨부된 상호 심사 연구 논문을 참조하면 된다: "Evaluating Graduated Response" (2014) 37 Columbia Journal of Law & the Arts 147-209.

연구 프로젝트 및 방법

본 자료는 18개월에 걸친 방대한 연구를 통해 도출한 결과물로 2013년 9월 기준 공법상 누적대응 방식인 저작권 "삼진아웃제(graduated response)"를 갖춘 국제 관할권을 모두 연구했다. 또한, 이에 상응하는 사법 제도를 도입한 관할권 2곳도 검토했다. 연구 목적은 이러한 제도의 효율성이 기존 증거에 의해 어느 정도 뒷받침되는지 파악하는 것이었다. 이를 위해 각 관할권별로 다음과 같은 효과가 어느 정도 달성됐는지 평가하는 방법을 사용했다.

- a 저작권 침해 감소
- b 합법 시장 증가
- c 다양하고 창의적인 문화 컨텐츠 창작 및 보급 장려

이 같은 분석을 통해 삼진아웃제를 뒷받침하는 증거에 심각한 문제가 있음을 발견했다. 본 발췌문은 증거의 주요 결함을 설명하고 향후 시사점을 제시하고자 한다.

증거 부족

‘상호연관성’은 ‘인과관계’와 동일하지 않다.

두 개의 현상이 동일한 추세를 보이면 이들간에 인과관계가 성립된다고 종종 오인되기도 한다. 예를 들어 소아마비가 만연했던 20세기 전반 아동들의 아이스크림 섭취 위험성에 대해 대대적인 경고가 내려졌었다. 소아마비 발병건수와 아이스크림 판매가 함께 증가한다고 보고되자 아이스크림이 소아마비의 원인이라고 결론을 내린 것이다. 차후에 소아마비 발병과 아이스크림 섭취는 ‘상관관계’가 있지만 ‘인과관계’는 아니라고 규명되었다. 이 둘의 상관관계는 세 번째 요소로 설명이 가능했는데, 소아마비 발병 건수와 아이스크림 섭취는 모두 날씨가 더울 때 증가했다. 이는 두 가지 현상이 동일한 흐름으로 진행된다고 해도 반드시 인과관계에 있는 것은 아니라는 사실을 보여주는 사례이다. 이들 현상간에 인과관계가 존재할 가능성은 있지만, 원인과 결과를 확인하려면 추가적인 연구가 필요하다.

아이스크림에 대한 공포와 마찬가지로 누적대응 즉 삼진아웃제의 효과에 관한 대부분의 주장들도 오인에서 기인한다. 즉, 상관관계와 인과관계를 동일시하는 오류를 범하는 것이다. 이는 한국의 삼진아웃제 시행에 관한 국제적인 주장에서 특히 명확하게 드러난다. 한국은 지난 몇 년간 저작권 침해 건수를 줄이는데 성공했다. 저작권 집행 강화를 목표로 하는 로비스트들은 “한국은 불법 다운로드를 줄였다. 한국은 삼진아웃제를 두고 있다. 따라서 삼진아웃제는 불법 다운로드를 줄인다”라고 식의 주장을 한다. 이는 ‘상관관계’를 ‘인과관계’로 오인하는 기초적인 오류를 범한 것이다. 이 같이 지나치게 단순화된 분석 방식은 삼진아웃제 이외에 교육 확대, 국내 음악과 TV, 영화 산업의 대대적인 성공, 합법 다운로드 경로 증가, 규제집행 조치 등 여타 여러 요소들이 작용하고 있으며, 이러한 요소들이 저작권 침해 수준 감소도 설명할 수 있다는 사실을 간과한 것이다. 철저한 조사에도 불구하고 본 연구에서 삼진아웃제 도입과 한국 등 여러 사법 관할권의 저작권 침해 감소간에 신뢰할 수 있는 인과관계를 찾을 수는 없었다. 많은 국가에서 이들의 관계는 더 복잡하게 나타났는데, 개인들이 저작권 침해를 그만두기 보다 적발을 피할 수 있는 경로로 이동했다는 증거가 상당했기 때문이다. 따라서 상관관계가 일부 존재한다고 볼 수 있지만 보다 긴밀한 연관성을 파악하기 위해서는 추가 연구가 필요하다.

통지서 수량 자료 오류

삼진아웃제는 일반적으로 몇 차례 경고 후 처벌 조치를 취하도록 되어 있다. 1차와 2차, 2차와 3차 통지서 수량 차이에 관한 자료가 삼진아웃제의 효율성을 보여주는 증거로 주로 사용된다. 1차보다 2차 통지서 수량이, 2차보다 3차 통지서 수량이 적다면 해당 제도가 저작권 침해 건수를 줄인다는 증거라고 주장하는 것이다.

이 같은 주장은 아도피(Hadopi)라고 불리는 프랑스 법률 사례에서 특히 자주 볼 수 있다. 음반 산업 대표자들은 “Hadopi의 1차 경고 중 최대 95%가 2차 경고로 이어지지 않으며, 2차 경고의 92%가 3차 경고로 이어지지 않는다”는 사실을 저작권 위반 감소의 증거로 든다. 비슷하게는 국제음반산업협회(IFPI)가 “Hadopi가 발송하는 백만건 이상의 통지서 강운데 단지 8%만이 2차 통지서를 받는다”라고 언급했다. 이와 마찬가지로, Hadopi를 담당하는 위원회 의장은 “3차 통지서 발송수량이 적을수록 Hadopi 법의 효율성이 입증될 것”이라고 말한 바 있다.

통지서 수량 자료가 삼진아웃제 효과성의 증거라고 당국들이 빈번하게 인용하고 있기 때문에, 이 같은 논리의 오류를 구체적으로 살펴볼 가치가 있다. 2013년 7월 기준 프랑스 Hadopi 제도에 따른 통지서 발송 자료[아래 참조]를 분석해 앞서 주장이 허위인 3가지 이유를 제시하고자 한다.

Hadopi 통지서 수량 자료, 2013년 7월 기준
1차 통지서 2,004,847건 발송 (1차 통지서는 대부분 자동 발송)
2차 통지서 201,288건 발송 (2차 통지서도 대부분 자동 발송)
“심사” 또는 조사 710건 보고 (대인 조사관이 3차 혐의가 제기된 통지서 수령자가 검찰에 송부돼야 한다고 간주한 경우)

이유 1:
제도 설계상 발생되는 요인들을 설명하지 못함

첫째, 발표된 수치에 2, 3차 통지서 수보다 '항상' 더 높은 1, 2차 통지서 수가 반영되는 이유는 2, 3차 통지서는 1, 2차 통지서가 발송된 이후에만 발송이 가능하기 때문이다. 이로 인해 불가피하게 시차가 발생한다. Hadopi 위원회 자체 자료를 통해 파악한 시차 정도를 살펴보면, 1차 통지서로부터 5개월 이후에 2차 통지서가 발송되고, 심사(3단계 대인 조사)는 앞서 2차 통지서 발송 5개월 후 시작된다. 즉, 통지서 수령자들은 적어도 5개월 이내에 추가 경고 통지를 받지 않는다고 기대하는 것이 합리적이라는 것이다. 따라서, 단계별 통지서 수량을 비교할 때 이점이 반영돼야 한다. 프랑스 Hadopi법의 경우, 1차 통지서 발송 수량과 그로부터 5개월 후 발송된 2차 통지서 수량과 비교하는 것이 한가지 방안이 될 수 있다.

Hadopi 제도에 따른 통지서 발송 수량이 단계가 지날수록 줄어드는 또 다른 이유는 2차 저작권 위반 혐의가 1차 혐의 시점으로부터 6개월 내 제기될 때만 2차 통지서가 해당 수령자에게 발송될 수 있다는 사실이다. 이 기간이 지나면, Hadopi제도는 위반 혐의에 대해 신규 '1차' 통지서만 발송하도록 하고 있다. 이와 마찬가지로, 3단계 '처벌'은 2차 혐의로부터 1년 내에 발생될 때만 진행될 수 있다. 따라서 앞서34개월 운영 기간을 다룬 수치에는 '1차'나 '2차' 통지서를 2회 이상 수령한 경우도 포함돼 수치가 과도하게 반영됨에 따라 사실상 저작권 위반 감소로 볼 수 없다고 해석하는 것이 전적으로 타당하다. Hadopi는 1차나 2차 통지서 2회이상 수령자 수에 관한 정보를 공개하지 않았기 때문에 이 요소는 기존 자료만으로는 설명이 불가능 하다.

이유2:
수학적 확률

앞서 통지서 발송 수량 자료가 삼진아웃제의 효과에 대해 어떠한 것도 말해주지 않는다는 두 번째 이유는 Hadopi 제도 하에서 모든 위반 혐의가 반드시 통지로 이어지지는 않기 때문이다. Hadopi가 접수하는 저작권 위반 혐의수는 공개되지 않지만, 공개된 법정 자료를 보면 접수된 혐의 중 소수만 처리되는 것을 알 수 있다. 이 자료에 따라 접수된 혐의 중 12%만이 실제 통지서 발송으로 이어진다고 보수적으로 가정해 보면, 1차 통지서 수령자가 위반 행위를 시정하지 않더라도 2차 통지서를 받을 확률은 기하급수적으로 낮아지며, 3차 통지서를 받을 확률 또한 매우 낮다. 행위의 시정이 없다 해도 추가 통지서를 받을 확률은 사전에 통지서를 받았는지 여부와는 전혀 무관하기 때문이다. 예를 들어 물고기 100마리가 있는 낚시터에서 물고기를 잡고 놔주는 연습을 하는 어부가 있다고 생각해보자. 잡힐 확률이 10%라면, 100마리 중 10마리가 잡힌 후 물에 다시 돌아가게 된다. 다음 단계에서 각 물고기가 잡힐 확률은 모두 10%로 동일하다. 두 번째 잡힌 물고기들은 처음 잡혔던 물고기들과 똑같지는 않고, 운 없는 일부 물고기만 두 번 잡히게 될 것이다. 평균적으로 봤을 때 1마리는 두 번 잡히게 된다(10%의 10%). 이와 유사하게 저작권을 위반한 개인이 1차 통지서를 받을 확률이 12%라면, 2차 통지를 받을 확률은 12%의 12% (0.122, or 1.44%)가 된다. 3차 통지서를 받을 확률은 12%의 12%의 12%(0.123, or 0.1728%)가 된다. 이를 2013년 7월에 발송된 2,004,847건의 1차 통지서에 대입해 보면, 2차 통지서는 240,581건(5개월 시차를 적용하면 191,982건)이 발송될 것이라고 합리적으로 예측할 수 있다. 실제로 201,288건이 발송됐다. 이는 통지서 수령과 위반 감소 사이에 상관관계가 거의 없다는 점을 보여준다(시차를 적용하면 기대치보다 더 많은 통지서가 실제로 발송됐기 때문에 역 상관관계 가능성 조차 있음).

2차 통지서 발송수와 3단계 조사간에는 더 강한 상관관계가 있다. 확률 계산에 따라 24,155건, 혹은 시차 요인을 통제하면 16,674건의 3단계 조사건이 시작될 것으로 예측되었다. 그러나 실제로는 단지 710건의 "심사"만 보고됐다. 하지만, 비교적 소수인 법집행 조치가 통지서가 저작권 침해에 미치는 영향에 관한 유의미한 자료로서 고려되어야 한다고 볼 수는 없다. 이는 마치 낮은 체포 수가 낮은 범죄율의 증거라고 경찰이 주장하는 것과 같다. 두 가지 경우 모두 얼마나 많은 혐의가 제기됐는지, 얼마나 많은 조치가 취해졌는지, 얼마나 많은 사례가 조사로 이어졌는지, 조사 대기 건은 몇 건인지 등 더 많은 정보가 필요하다. Hadopi 사례를 보면 정황상 주로 조사자원 부족과 관련된 여러 요소들로 인해 사용자 행위 변화와 관계없이 조사건수가 줄어든 것으로 보인다. 3단계 절차는 상당한 인력 투입이 필요하다는 점을 생각하면 된다. 연구 당시 Hadopi가 한달 동안 진행한 3단계 조사는 최대 64건이었다. 프랑스인들의 통상적인 휴가철인 2011년과 2012년 8월에는 3단계 통지서가 전혀 발송되지 않았다(하지만 대량의 1차와 2차 통지서가 자동 발송됐다). 이러한 상황에서 조사건수와 저작권 위반 감소간에 어떠한 관계가 있다는 주장은 신뢰할 수 없다.

이유 3:
상관관계과 인과관계

통지서 발송 수량 자료가 삼진아웃제의 효과를 입증한다는 주장이 반복적으로 제기되지만, 상기 요인들이 통제되지 않는다면 이러한 주장은 신뢰성을 줄 수 없다.

이러한 요인들이 고려했을 때 통지서 자료가 통지서 수령과 저작권 위반 감소간에 상관관계를 보여줄 수도 있을 것이다. 역으로 상기 모델을 통해 제시했듯이 통지서 수령과 위반 증가간에 상관관계가 존재할 수도 있다. 하지만 어느 방향의 상관관계이던지 간에 해당 자료는 통지서 수령이 위반을 증가시키거나 감소시킨다는 주장을 뒷받침하기에는 충분하지 않는데 이는 당연히 상관관계와 인과관계가 동일하지 않기 때문이다. 통지서 발송과 삼진아웃제 목표 달성에 인과관계가 있는지 확인하기 위해서는 통제 실험 방법 등을 사용한 추가 조사가 필요하다. 본 연구에서는 이러한 인과관계가 있다는 증거를 전혀 발견하지 못했다.

신뢰할 수 없는 자료에 의존

삼진아웃제 효과를 뒷받침하는 증거는 이러한 과학적 논리적 오류뿐 아니라 과학적 신뢰성 자체가 결여되었다는 점에서 더욱 문제가 된다. 세계적으로 삼진아웃제 효과의 증거로서 제시된 연구 대부분은 다음 중 하나에 해당된다.

1. 국제적으로 용인되는 과학적 엄격성, 정확성, 신뢰성을 갖춘 평가 방식인 상호 검토를 받은 적이 없음
2. 삼진아웃제의 세계적인 확산을 위해 로비하는 기관이나 삼진아웃제의 광범위한 도입으로 인해 막강한 이권을 갖는 기관(예: 저작권 침해 의혹을 사업모델을 갖고 있는 기업)에게 자금을 지원 받음
3. 불투명한 방법 (예: '최종 수치' 혹은 '결과 요약'만 제공돼 결론 도출을 확인할 방법이 없는 경우)을 사용하고 연구자들이나 대중의 검토를 위해 공개되지 않음

실제로 세계적으로 단지 2가지 주요 연구만이 상호 검토를 위해 제출되었고, 삼진아웃제 로비스트에 의해 실시되거나 자금을 지원받지 않았으며, 투명한 방법을 사용한 것으로 본 연구 결과 파악되었다.

첫번째 사례는 뉴질랜드 연구자들이 뉴질랜드 삼진아웃제 법안 발효 전후 P2P 트래픽을 측정한 것으로, 50% 이상의 트래픽 감소가 관찰되었다. 또한, 삼진아웃제도를 우회할 수 있는 기술 사용도 크게 증가한 것을 발견했다. 1년 후 진행된 후속 연구에서 P2P 트래픽양이 일부 회복됐음을 발견했지만 여전히 삼진아웃제 시행 전보다는 낮은 수준이었다. 또한, HTTP 트래픽도 크게 증가했음을 발견했다. 연구자들은 뉴질랜드 법 제도에서 벗어난 P2P이외 저작권 위반형태로 사용자들이 이동함으로써 이 같은 현상이 발생됐다는 이론을 제시했다. 이 연구가 삼진아웃제 효과를 뒷받침하는데 사용되는 다른 '증거'보다 과학적 신뢰성은 훨씬 높지만 여전히 주요한 한계가 있다. 제한된 자료에 기반하고 있으며, 연구자들은 트래픽 변화와 신규 법률간에 인과관계를 주장하기 전에 뉴질랜드 내외부 모든 ISP로부터 트래픽 믹스를 조사할 필요가 있다고 말했다. 또한 삼진아웃제 시행으로 기존의 합법적 음악 서비스가 2배로 증가했는데 이 연구는 당시 뉴질랜드에서 새롭게 운영되기 시작한 신규 서비스를 통제하지 않았다.

두 번째는 다나허(Danaher) 연구로 삼진아웃제와 합법적 시장 증가간 연관성을 주장하기 위해 진행된 유일하고 심도 깊은 사례이다. 프랑스와 다른 유럽 국가로 구성된 통제 집단간 아이튠스(iTunes) 주간 판매량 자료와 동기간 프랑스인들의 '아도피(HADOPI)' 구글 검색 자료를 비교하는 방법을 사용했다. 이 기간 중 아이튠스 프랑스 판매량은 통제 집단과 다른 형태를 보이며 더 높은 수준을 유지했다. 'Danaher 연구'로 알려진 이 연구는 삼진아웃제를 뒷받침하는 증거로서 환영받았다. 하지만 주목할 만한 사실은 이러한 효과가 더 넓은 음반 시장에서는 나타나지 않는다는 점이다. 또한 프랑스 정부가 Hadopi효과를 평가하기 위해 의뢰한 종합 연구인 레스뀌르(Lescure) 보고서와도 상충된다. Danaher 연구 등 모든 관련 증거를 검토한 후 Lescure 보고서는 Hadopi가 P2P 저작권 침해 감소를 일부 야기했다고 할지라도, 트래픽이 합법적인 시장이 아닌 또 다른 저작권 위반 경로들로 이동하는 결과를 낳았다고 결론을 내렸다.

상기 두 가지 제한된 연구를 제외하고 삼진아웃제의 효과적이었다는 주장을 뒤받침한다고 인용되는 증거들의 전반적인 수준은 매우 낮다.

이러한 결과로부터 도출할 수 있는 교훈

본 연구는 삼진아웃제 도입과 유지를 지지하는 재원이 두둑한 기관들이 삼진아웃제 효과에 관해 강력한 주장을 하지만 뒷받침할 만한 증거가 없다는 사실을 증명했다.

ISP 실행이 저작권 산업 결과를 개선하는데 있어 핵심이라는 이론이 처음 제기됐을 때 이를 수긍하거나 반박할 수 있는 자료가 없었다. 하지만 일부 국가들이 삼진아웃제 도입을 실험해 옴으로써, 이 이론과 결과가 어떻게 연결되는지 더 잘 이해할 수 있게 되었다. 수년이 흘렀지만 삼진아웃제와 저작권 위반 감소, 합법적 시장 증가 혹은 보다 광범위한 콘텐츠 생산과 배포간의 명확한 인과관계를 어느 국가에서도 찾아볼 수 없었다.

이러한 상황에서 전세계 규제자들이 다른 곳에서 해결방안을 찾고 있는 것은 전혀 놀라운 일이 아니다. 2011년 이후 삼진아웃제가 공법으로 제정된 적이 없고, 프랑스는 자체 제도를 일부 무효화하기도 했다. 제도의 효과에 대한 신뢰할만한 증거가 전혀 없고, 유지에 필요한 대규모 투자를 고려할 때 기존에 삼진아웃제를 제정한 국가들은 이번 기회를 활용해 유지하는 것이 과연 바람직한 것인지 검토해볼 수도 있을 것이다. 정부 차원에서는 이해관계자들에게 삼진아웃제 목표가 달성되고 있음을 보여줄 수 있도록 더 많은 노력을 기울여달라고 요청하는 방안도 생각해 볼 수 있다. 예를 들어 저작권자들은 해당 법의 효과를 과학적으로 보다 엄격하게 평가할 수 있는 자료를 보유하고 있는 경우가 많다. 아마도 이러한 자료를 독립 연구자들에게 제공하도록 요청할 수 있을 것이다. 만약 삼진아웃제도가 주장처럼 효과가 있다면, 삼진아웃제 지지자들은 이 같은 분석을 환영할 것이 분명하다. 마지막으로 로비스트들에게 법과 정책이 증거와 일치하도록 자신들의 주장을 정당화할 수 있는 노력을 더 많이 기울여달라고 촉구해야 할 것이다.