

정보매개자책임의 국제적 흐름

이용자 권리 보호와 ICT 산업 발전을 위한 플랫폼사업자의 책임원칙

# 정보매개자책임의 국제적 흐름

Open Net - Harvard Berkman Center Seminar on Intermediary Liability



## 정보매개자책임의 국제적 흐름

이용자 권리 보호와 ICT 산업 발전을 위한 플랫폼사업자의 책임원칙

Open Net-Harvard Berkman Center Seminar on Intermediary Liability

일자 2015년 5월 28일 (목)

시간 09:30~18:00

장소 국회의원회관 제1소회의실

주최 국회의원 박주선, 염동열, 유승희 ※ 가나다 순



후원 방송통신위원회 KOREA COMMUNICATIONS COMMISSION 한국저작권위원회 KOREA COPYRIGHT COMMISSION

opennet.or.kr

T. 02-581-1643 E-mail. master@opennet.or.kr



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

PROGRAM | 프로그램 ..... 8

## 개회식 Opening Remarks

PROFILE | 프로필 ..... 12

개 회 사      박주선 의원 (국회의원, 교육문화체육관광위원회 위원) ..... 16

인사말씀 1    염동열 의원 (국회의원, 교육문화체육관광위원회 위원) ..... 18

인사말씀 2    유승희 의원 (국회의원, 미래창조과학방송통신위원회 위원) ..... 20

인사말씀 3    임성호 국회입법조사처장 (국회입법조사처) ..... 22

Introduction | 취지 소개 ..... 28

Intermediary liability – Not Just Backward but Going Back

(K.S. Park, Professor at KU Law School, Director of Open Net) ..... 31

인터넷의 특성과 임시조치 및 저작권 전송중단제도

(박경신 고려대학교 법학전문대학원 교수, (사)오픈넷 이사) ..... 41

# Contents

## [제1세션] 정보매개자책임에 대한 이해

### [Session 1] Safe Harbor (other parts of the world) vs. Limited Liability (Korea)

#### PROFILE | 프로필 ..... 48

- Governance Of Online Intermediaries – Observations From A Series Of National Case Studies(excerpt)  
(Urs Gasser, Director of the Berkman Center and Professor of Practice at Harvard Law School) ..... 55
- 온라인 매개자 거버넌스 – 국가 사례 연구를 통한 조사(발췌본)  
(어스 개서 교수, 미국 하버드대학교 버크맨센터 소장) ..... 67
- Case Study – Intermediary Liability Rules in Japan  
(Naoko Mizukoshi, Founder/Partner at Endeavor Law Office) ..... 79
- 사례연구 – 일본의 정보매개자 책임 관련 규정 (나오코 미즈코시 변호사, 일본 엔데버 법률사무소) ..... 83
- Act on the Limitation of Liability for Damages of Specified Telecommunications Service Providers ..... 87
- 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..... 93

#### DISCUSSION | 토론

- Prof. Youngjoon Kwon (SNU Center for Law and Technology) 권영준 교수 (서울대 기술과법센터) ..... 101
- Mr. Kyung Oh Jung (Attorney at Law, Hanjung Partners) 정경오 변호사 (법무법인 한중) ..... 107

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

**PROFILE | 프로필** ..... 114

- The Electronic Silk Road and Information Intermediaries  
 (Anupam Chander, Professor of Law at UC Davis) ..... 121  
 e-실크로드와 정보매개자 (아누팜 찬더 교수, 미국 UC데이비스 로스쿨) ..... 127
  
- Intermediary Liability in Europe – The Electronic Commerce Directive  
 (Oliver J. Süme, EuroSPA President) ..... 135  
 유럽의 정보매개자 책임 – 전자상거래지침을 중심으로 (올리버 쥬메 회장, 유럽SP협회) ..... 149

**DISCUSSION | 토론**

- Old and New Challenges in Actualizing the Ideals of Digital Public Sphere :  
 Giant Intermediaries Posing New Threats to Digital Ecosystem  
 Dr. Minjeong Kim (Associate Professor of Media and Communication, Hufs)  
 김민정 교수 (한국외대, 한국언론법학회 연구이사) ..... 163
  
- Mr. Jongsoo Yoon (Partner, Shin&Kim) 윤종수 변호사 (법무법인 세종) ..... 169
  
- Prof. Inho Lee (Chung-Ang University) 이인호 교수 (중앙대, 정보법학회 회장) ..... 177

# Contents

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

### PROFILE | 프로필 ..... 184

- How the DMCA's Online Copyright Safe Harbor Failed  
(Eric Goldman, Professor of Law at Santa Clara University School of Law) ..... 191  
DMCA의 온라인 저작권 피난처는 어떻게 실패했나 (에릭 골드먼 교수, 미국 산타클라라대학교 로스쿨)·· 197
- Precis of Research Findings – Evaluating Graduated Response  
(Rebecca Giblin, Senior Lecturer at Monash University Faculty of Law) ..... 205  
연구 결과 요약 – 삼진아웃제 평가 (레베카 킴린 교수, 호주 모나쉬대학교) ..... 215

### DISCUSSION | 토론

- Dr. Kyuhong Lee (Presiding judge, Seoul Central District)  
이규홍 부장판사 (서울중앙지방법원 지재전담)..... 225
- Prof. Pilwoon Jung (Korea National University of Education)  
정필운 교수 (한국교원대, 한국인터넷법학회 총무이사) ..... 233



# 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. <b>K.S. Park</b> (KU, Director of Open Net)
10:30~12:00	<p><b>Session 1</b></p> <p>Safe Harbor (other parts of the world) vs. Limited Liability (Korea)</p>	<p><b>Moderator</b> Prof. <b>K.S. Park</b> (KU, Director of Open Net)</p> <p><b>Main Speaker</b> Prof. <b>Urs Gasser</b> (Harvard Berkman Center for Internet and Society) : <i>Online Intermediaries Project: Findings and Recommendations</i></p> <p><b>Panelists</b> Prof. <b>Youngjoon Kwon</b> (SNU Center for Law and Technology) Dr. <b>Yoo Hyang Kim</b> (Head, NARS Science, Media and Telecommunications Team) Mr. <b>Kyung Oh Jung</b> (Attorney at Law, Hanjung Partners)</p> <p><b>Case Study</b> Ms. <b>Naoko Mizukoshi</b> (Partner, Endeavour Law Office) : <i>Intermediary Liability Rules in Japan</i></p>
12:00~13:30		Lunch
13:30~15:00	<p><b>Session 2</b></p> <p>Intermediary Liability and Digital Ecosystem</p>	<p><b>Moderator</b> Prof. <b>Jewan Kim</b> (KU Law School Research Institute)</p> <p><b>Main Speaker</b></p> <ul style="list-style-type: none"> <li>▪ Prof. <b>Anupam Chander</b> (UC Davis School of Law) : <i>The "Electronic Silk Road" and Intermediary Liability</i></li> <li>▪ Mr. <b>Oliver Süme</b> (President, EuroISPA) : <i>E-Commerce Directive and Experience of European ISPs</i></li> </ul> <p><b>Panelists</b> Prof. <b>Minjeong Kim</b> (Hankuk University of Foreign Studies) Mr. <b>Jongsoo Yoon</b> (Partner, Shin&amp;Kim) Prof. <b>Inho Lee</b> (Chung-Ang University)</p>
15:00~15:20		Coffee Break
15:20~16:50	<p><b>Session 3</b></p> <p>Intermediary Liability and Copyright</p>	<p><b>Moderator</b> Prof. <b>Deok-Young Park</b> (Yonsei University)</p> <p><b>Main Speaker</b></p> <ul style="list-style-type: none"> <li>▪ Prof. <b>Eric Goldman</b> (Santa Clara University School of Law) : <i>ISP Liability under DMCA</i></li> <li>▪ Dr. <b>Rebecca Giblin</b> (Monash University Faculty of Law) : <i>Evaluating Graduated Response</i></li> </ul> <p><b>Panelists</b> Dr. <b>Kyuhong Lee</b> (Presiding judge, Seoul Central District Court) Prof. <b>Pilwoon Jung</b> (Korea National University of Education) Mr. <b>Kyong-soo Choe</b> (Chief Senior Researcher, Korea Copyright Commission)</p>
16:50~18:00		Wrap-up Session



# 정보매개자책임의 국제적 흐름

이용자 권리 보호와 ICT 산업 발전을 위한 플랫폼사업자의 책임원칙

시간	주제	연사
09:00~10:00		참석자 등록
10:00~10:20	개회식	축사 / 인사말씀
10:20~10:30	세미나 취지 소개	<b>박경신</b> 교수 (고려대, 오픈넷 이사)
10:30~12:00	<b>제1세션</b> 정보매개자 책임에 대한 이해 (임시조치 등)	<b>좌장</b> <b>박경신</b> 교수 (고려대, 오픈넷 이사) <b>주제발표</b> <b>어스 개서</b> 교수 (미 하버드대, 버크맨센터 소장) : 온라인 정보매개자 프로젝트 : 연구결과와 제안 <b>토론</b> <b>권영준</b> 교수 (서울대 기술과법센터) <b>김유향</b> 팀장 (국회입법조사처 과학방송통신팀) <b>정경오</b> 변호사 (법무법인 한중) <b>특별토론</b> <b>나오코 미즈코시</b> 변호사 (일본 엔데버 법률사무소) : 일본의 정보매개자 책임 원칙
12:00~13:30		점심 시간
13:30~15:00	<b>제2세션</b> 정보매개자 책임과 ICT 생태계	<b>좌장</b> <b>김제완</b> 교수 (고려대 법학연구원) <b>주제발표</b> ▪ <b>아누팜 찬더</b> 교수 (미 UC데이비스 로스쿨) : “e-실크로드”와 정보매개자 책임 ▪ <b>올리버 쥬메</b> 회장 (유럽ISP협회) : EU 전자상거래지침과 유럽 ISP의 경험 <b>토론</b> <b>김민정</b> 교수 (한국외대, 한국언론법학회 연구이사) <b>윤종수</b> 변호사 (법무법인 세종) <b>이인호</b> 교수 (중앙대, 정보법학회 회장)
15:00~15:20		휴식
15:20~16:50	<b>제3세션</b> 정보매개자 책임과 저작권 제도	<b>좌장</b> <b>박덕영</b> 교수 (연세대 법학전문대학원) <b>주제발표</b> ▪ <b>에릭 골드먼</b> 교수 (미 산타클라라대 로스쿨) : 미국 디지털밀레니엄저작권법(DMCA)상 ISP의 책임 ▪ <b>레베카 킵린</b> 교수 (호주 모나쉬대) : 삼진아웃제에 대한 비교법적 평가 <b>토론</b> <b>이규홍</b> 부장판사 (서울중앙지방법원 지재전담) <b>정필운</b> 교수 (한국교원대, 한국인터넷법학회 총무이사) <b>최경수</b> 수석연구위원 (한국저작권위원회)
16:50~18:00		종합토론 및 정리





# Opening Remarks

---

개회식





개회사



**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 1



**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 2



**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, Broadcasting 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

인사말씀 3



**Lim, Seong-Ho**  
**임성호**

▪ -	Ph.D 박사.	Political Science, 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



**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 찬더 UC데이비스 로스쿨 교수님, 에릭 골드먼 산타클라라대 로스쿨 교수님, 올리버 주메 유럽ISP협회 회장님, 호주의 레베카 집린 모나쉬대 교수님, 일본의 나오코 미즈코시 변호사님께 더욱 깊은 감사의 인사를 드립니다.

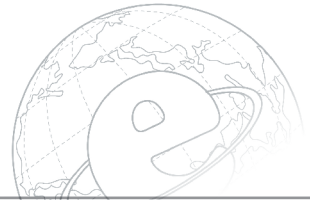
아울러 좌장으로 오늘 세미나를 이끌어 주실 박경신·김제완·박덕영 교수님을 비롯하여, 이규홍 부장판사님, 권영준·김민정·이인호·정필운 교수님 등 귀한 시간을 내어 참석해 주신 모든 패널 여러분들께 진심으로 감사드립니다.

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 지을 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 자율 규제를 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 수 만도 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.

## 인사말씀 2



### 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.

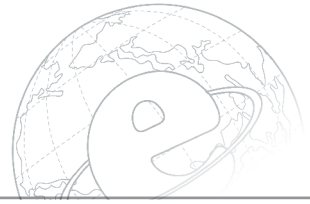
그리고, 오늘 심포지움을 위해 멀리 미국에서 찾아 주신 하버드대 어스 개서 교수님, UC데이비스 로스쿨 아누팜 찬더 교수님, 산타클라라대 에릭 골드먼 교수님과 호주 모나쉬대 레베카 키플 교수님, 일본 나오코 니즈코시 변호사님, 그리고 유럽 ISP협회 올리버쥬메 회장님께도 진심으로 감사드립니다.

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 튀 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.



**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 강화 하자는 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 발전시켜나가는 데 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 맡아주신 국내외의 저명한 전문가 여러분께 감사의 말씀을 전하면서 오늘 세미나가 한국의 인터넷산업의 지속적인 성장과 발전을 위한 생산적인 논의의 장이 되길 기원합니다.

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)







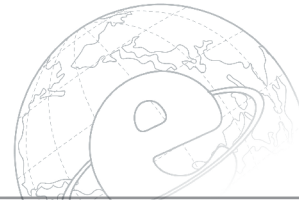
**Kyung-Sin (K.S.)  
Park**

▪ 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 tweets. 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 solidarity of [www.chillingeffects.org](http://www.chillingeffects.org), he and his former clinic students founded [www.internetlawclinic.org](http://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<sup>1)</sup>*

※ 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](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](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%<sup>2)</sup>. [. . .]

## **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.<sup>3)</sup> [. . .]

## **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”.<sup>4)</sup>

---

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 Korean Election”, November 21, 2013, [http://www.nytimes.com/2013/11/22/world/asia/prosecutors-detail-bid-to-sway-south-korean-election.html?\\_r=0](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.<sup>5)</sup> 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,<sup>6)</sup> 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.<sup>7)</sup>]

---

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<sup>8)</sup> and MP Nam Kyung-pil’s disclosure in October 2012<sup>9)</sup> 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<sup>1 0)</sup> critical of a Seoul City mayor's ban on assemblies in the Seoul Square
- A posting<sup>1 1)</sup> 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;<sup>1 2)</sup>
- A posting critical of politicians' pejorative remarks on the recent deaths of squatters and police officers in a redevelopment dispute<sup>1 3)</sup>
- A posting calling for immunity from criminal prosecutions and civil damage suits on labor strikes.<sup>1 4)</sup>
- 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.<sup>1 5)</sup>

## 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

---

1 0) <http://blog.ohmynews.com/savenature/199381>

1 1) The original posting now taken down is shown here. <http://wnsgud313.tistory.com/156>

1 2) [http://www.hani.co.kr/arti/society/society\\_general/300688.html](http://www.hani.co.kr/arti/society/society_general/300688.html)

1 3) <http://blog.jinbo.net/gimche/?pid=668>

1 4) <http://blog.jinbo.net/gimche/?pid=492>

1 5) <http://bbs1.agora.media.daum.net/gaia/do/debate/read?bbsId=D115&articleId=610524>

aforesaid provisions is that “Thou Shall Delay Saying What Others Dislike, As Long As 30 days.”<sup>16)</sup> 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[. . .]:<sup>17)</sup>

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

1 6 ) 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.artild=ART001387276>>

1 7 ) 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 요청 받으면 지체 없이 삭제·임시조치 등의 필요한 조치를 하고 즉시 신청이 및 정보게재자에게 알려야 한다. 이 경우 정보통신서비스 제공자는 필요한 조치를 한 사실을 해당 게시판에 게시하는 등의 방법으로 이용자가 알 수 있도록 하여야 한다.

④ 정보통신서비스 제공자는 제1항에 따른 정보의 삭제요청에도 불구하고 하고 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(제102조제1항 제1호의 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.

⑤ 온라인서비스제공자가 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 불법유흥업소와 연계된 호텔을 운영하다는 텔레비전보도 영상
- 용산참사 희생자를 비하한 정치인 발언을 비난한 글
- 노동자파업에 대해 형사처벌과 손해소를 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.





**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.



**Park, K.S.**  
박경신

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

PROFILE | 프로필

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 과학방송통신팀
▪ 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,<sup>1)</sup> 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,<sup>2)</sup> 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.<sup>3)</sup> While the historic motives for introducing these liability limitations were rather nuanced (in the case of

---

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>.



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),<sup>4)</sup> 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).<sup>5)</sup>

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-

---

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*)<sup>6)</sup> 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.<sup>7)</sup> The licensing regime in Vietnam imposes hard constraints under which online intermediaries have to operate, to give another example from the case study series.<sup>8)</sup>

## **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.<sup>9)</sup> 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.<sup>10)</sup>

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.<sup>11)</sup> 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.<sup>12)</sup>

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.<sup>13)</sup> 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.<sup>14)</sup> In contrast, the governance models in India,

---

1 3) 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.

1 4) 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.

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.<sup>15)</sup>

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.<sup>16)</sup> 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.<sup>17)</sup> 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

1 5) 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).

1 6) 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).

1 7) 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.<sup>1 8)</sup>

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.<sup>1 9)</sup> The contrast between automated compliance and enforcement in response to copyright issues on YouTube, versus the human and labor-intensive 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,

---

1 8) 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).

1 9) 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.<sup>2 0)</sup> 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.<sup>2 1)</sup>

---

2 0) 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>.

2 1) In this sense also see “The Manila Principles On Intermediary Liability: Version 0.9,” December 1, 2014, <https://docs.google.com/document/d/1kAkqgt3cRb65d8ik6vWYgpk6DYpP8ABA43IjgDiGOi8/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,<sup>1)</sup> 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<sup>2)</sup> 미국의 법률 제도는 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.<sup>3)</sup> 이러한 법적 책임 제한을 도입한 애초의 동기는 지금과는 다소 달랐는데, 미 통신품위법(CDA)의 경우 의원들은 온라인 매개자들이 법적 책임에 노출되지 않고 콘텐츠를 자체적으로 규제하도록 만들려고 했다.<sup>4)</sup> 하지만 오늘날 정책 논쟁에서 이러한 조력 기능은 경제적 효과(예: 법적 책임에 대한 두려움 없이 혁신에

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>.

매진하도록 하는 인센티브)나 기본권(예: 사기저하 방지)과 관련해 주로 언급된다.<sup>5)</sup>

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<sup>6)</sup> 온라인 매개자에 콘텐츠에 대한 법적 책임을 직접 부과한다. 터키 인터넷법 등 차단 법령은 온라인 매개자 영역에서 법이 주로 제약 기능을 수행하는 가장 대표적인 사례로 논란이 되고 있다.<sup>7)</sup> 베트남 인허가제도는 온라인 매개자들에게 운영상 엄격한 제약을 부여하는 또 다른 사례이다.<sup>8)</sup>

5) Bankston, Kevin, David Sohn, Andrew McDiarmid 참조, “메신저 보호: 표현과 혁신의 기반 보호” Center For Democracy and Technology, 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 공포와 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 기본적으로 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 제정되기 까지 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 방송통신심의위원회가 매개자 거버넌스 제도에 있어 주요한 역할을 하는 예이다.<sup>9)</sup> 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.<sup>10)</sup>

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.<sup>11)</sup> 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.<sup>12)</sup>

9) 박경신. “온라인 매개자 사례연구: 매개자 책임 – 후진이 아닌 후퇴”, The Global Network of Internet & Society Research Centers (2015).

1 0) Nguyen, Thuy. “온라인 매개자 사례연구: 베트남 온라인 매개자의 역할과 책임 – 희망과 공포와 혼재된 규제”, The Global Network of Internet & Society Research Centers (2015), 3.

1 1) 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).

1 2) 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.<sup>13)</sup> 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 콘텐츠를 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 콘텐츠를 삭제하거나, 놔두거나, 삭제 후 복원하던지 간에 해당 콘텐츠를 직접 작성하지 않은 한 일관되게 법적 책임을 부과하지 않는다.<sup>14)</sup> 이와 대조적으로 인도, 한국, 태국의 거버넌스 모델은 비대칭 인센티브 구조를 취하고 있는데, 과잉 준수가 되더라도 매개자들이 법적 책임을 피하기 위해 콘텐츠를 삭제하도록 유인하고 있다.<sup>15)</sup>

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

1 3) 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.

1 4) 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.

1 5) Arun, Chinmayi, Sarvejeet 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 제시했을 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.<sup>16)</sup> 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 콘텐츠 사이트가 저작권을 위반하는 대규모 문제를 처리하는데 있어 소프트웨어가 주요한 역할을 한다.<sup>17)</sup> 알고리즘은 유튜브에서 “개별 명령” 역할을 수행할 뿐 아니라 태국, 터키, 인도 사례와 같이 정부가 부과하는 모니터링과 여과 기능도 수행한다.<sup>18)</sup>

마지막으로 앞서 언급된 문제와 관련해 사례연구들은 제도의 준수와 실행에 있어 돈과 시간 모두에서 비용의 중요성을 보여준다. 비용의 역할은 다양하며 콘텐츠별로 다르다. 예를 들어 터키 사례를 보면 통지삭제제도를 둘러싼 불확실성과 비용없이 형사소송절차에 착수할 수 있다는 사실은 민간제도보다 사법 제도의 선호로 이어진다는 사실을 알 수 있다.<sup>19)</sup> 유튜브상의 저작권 문제에 대한 자동 준수 및 실행방식과 CJEU잇혀질 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.

1 6) 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).

1 7) 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.

1 8) 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).

1 9) 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 콘텐츠 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 맵핑은 여러 상황을 거쳐 풍부해질 수 있으며, 다양한 거버넌스 모델의 성과와 나아가 디지털 경제와 사회에 미치는 영향에 관한 실증적인 증거도 반영할 수 있다.<sup>20)</sup> 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.<sup>21)</sup>

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 콘텐츠 창작원은 아니지만 콘텐츠의 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 심도 있게 이해하는 것이 중요하다는 것을 사례 분석을 통해 알 수 있다. 강력한 네트워크 효과와 시장의 양면성을 고려할 때 매개자들의 경제학도 이와 마찬가지로이다.

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/1kAkqgt3cRb65d8ik6vWYgpk6DYpP8ABA43ljgDiGOi8/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. 사례 연구를 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 사례 연구를 보면 이러한 “개입”은 과잉 규제 위험을 수반하고 사용자의 기본권, 혁신, 디지털 경제에 부정적인 영향을 미친다. 또한 기존의 강력한 매개자들에게 콘텐츠 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 사례 연구는 제시한다. 특히 통지삭제 시스템을 갖춘 국가들이 직면하고 있는 유사한 난제들도 보여주는데, 효력이 있는 콘텐츠 소유자, 규제 당국 등에 통지를 해야 하는지 여부와 어떻게 해야 하는지 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.



Case Study / 특별토론

# *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

## 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

2015 Naoko Mizukoshi

2

## 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.

2015 Naoko Mizukoshi

3



## 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.

2015 Naoko Mizukoshi

4

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





# 사례연구: 일본의 정보매개자 책임 관련 규정

## 사례연구: 일본의 정보매개자 책임 관련 규정

나오코 미즈코시  
(Naoko Mizukoshi)  
엔데버 법률사무소

2015년 5월 28일 목요일

## 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

2015 나오키 미즈코시

2

## 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

2015 나오키 미즈코시

3

## 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

2015 나오키 미즈코시

4

나오키 미즈코시  
(Naoko Mizukoshi)

엔데버 법률사무소  
nmizukoshi@elaw.co.jp  
<http://english.elaw.co.jp/>





# ***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<sup>1)</sup>***

(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



譽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穩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。



Discussion / 토론

## ***Prof. Youngjoon Kwon***

(SNU Center for Law and Technology)



권영준 교수

(서울대 기술과법센터)



First of all, I should confess that I was marveled at the depth and the extensiveness of the research carried out by Professor Gasser and his colleague. At least based on my experiences, “National Case studies”, “Transnational Studies”, or “Comparative Studies” are something not commonly witnessed in the US legal academia, while such a cross-border research remains one of the primary methods in other jurisdictions. In that sense, it is quite exciting to see this sort of research carried out by someone at the Harvard University. It is also thrilling to see that South Korea being the object of such keen academic observation.

Although I am by no means a true expert in this field of law, I presume that my role today as a discussant and as a Korean law professor is to give out some information along with some of my thoughts on the legal issue of online intermediaries, which I will refer to as “ISP”. These entities have truly played a crucial role on the Internet. Given time limit, I would like to focus on the ISP and its legal implication on free speech.

Indeed, the advent of the Internet has potential to dramatically change legislations and policies on freedom of expression. The Internet is the most participatory media that widens the scope of free speech, both quantitatively and qualitatively. Anyone can share their views and thoughts with the public regardless of time and place, once they have access to the network. Since speeches made on the Internet are not limited by borders, this marketplace of ideas is truly worldwide. However, there is a dark side of the Internet as well. Cyber-violence is found everywhere. A great number of people are abusing this enhanced freedom without considering its fatal consequences. Defamations, invasion of privacy, obscenity and other forms of wrongdoings are prevalent. Damages incurred by these torts are exacerbated due to the unique nature of the Internet.



Specifically in Korea, this contrast seems even more dramatic. Freedom of expression in Korea was somewhat curbed under authoritarian governments in the past, although a notable change has taken place in last two decades. Yet, the growth of the Internet essentially changed the free speech regime in this nation. Online democracy has reached its pinnacle, due mainly to two reasons; a remarkably high broadband penetration rate and a great number of electronic bulletin boards. However, Korea is not free from the adverse effects of the Internet, either. A so-called citizen journalism, in which swarms of surfers mobilize together in formation on what the traditional media isn't covering, is often going too far to dig up and post every detail of the targeted person in a defaming way. People irresponsibly express extreme opinions from behind a cloak of anonymity.

As we witness a clash between freedom of expression and freedom from defamation, balancing these two conflicting interests has become a very difficult, yet significant issue. In an effort to balance these societal interests, liability of ISP is being discussed. ISPs are performing unique functions in cyberspace, such as providing access to the Internet, transmitting or storing information. In a highly decentralized cyberspace, they have great control over the content once it comes under their domain, just like a government or publishing companies do off-line. Thus, broader liability on ISPs will force them to involve themselves with the regulation of the content, which will possibly protect a great number of potential victims from cyber-violence. However, it is likely to have a chilling effect on free speech. In contrast, completely exempting ISPs from legal liability might be helpful in fostering freedom of expression on the Internet, but it seems to be unduly leaning toward the side of free speech. Hence, determining the scope of ISP liabilities will greatly influence the delicate balance between free speech and personal reputations.

Now, it is interesting to note that the Korean Courts have strived to find subtle balance in between these two values at each end. I understand that the US has addressed this issue by legislation. The CDA (Communications Decency Act) exempts ISPs from liability arising from defamation by their users, thereby enabling them to self-regulate the content without fear of being exposed to liability. It is certainly not

the case in Korea. Devoid of such liability-exemption legislation, Korean courts have figured out a way to address this issue by applying general legal doctrine of negligence. It is as simple as this. If ISPs are negligent, they are liable. If not, they get off the hook.

For example, in one case back in 2001, the Supreme Court proposed a guideline that the ISP has a duty to take suitable measures, including deletion of a defamatory message on its electronic bulletin board, when the ISP knew or could have known that the defamatory message had been posted. In another case two years later, however, the Supreme Court moved back a little from its initial stance by stating that the ISP is not always liable merely for the reason that it knew or could have known the fact that the defamatory content has been posted by the third party on the bulletin board. It stated that various factors, including the purpose and contents of the posted message, its posted period, the way it was posted, the extent of the damage, the relationship between the plaintiff and the defendant, the actions and responses of both parties after uploading the contents, the size and characteristic of the website and so forth, should be considered in determining whether an ISP has a duty to take necessary measures on the defamatory message.

Several decisions along this line followed until the most notable Supreme Court decision in 2009 was handed down on the ISP liability issue. In this case, where ISP was allegedly negligent in dealing with defamatory statements, the majority opinion held that ISP has duty to take necessary measures, as long as they are technically and economically feasible, such as blocking access to such defamatory materials or deleting them when the illegality of the materials are obvious and the ISPs could know or could not have been unaware of such materials. Such stance was to recognize monitoring duty, albeit under strict requirements. Whereas, the minority opinion stated that the ISPs do not bear progressive monitoring duty, and that they bear such duty only upon the request by the victims were made.



I am rather of the position that narrower scope of liability on ISPs is more desirable in the defamation context. This conclusion might not be pleasing to the plaintiff in a defamation suit. Most of the time, ISPs have deeper pockets than defamers who may be judgment-proof. Putting less liability on ISPs means there is less of a possibility to be compensated for the damages. Moreover, it is true that protecting potential or actual victims of illegal speeches is some value that needs to be cherished as well. However, ISP liability is only one of the vehicles by which we can balance competing interests on the Internet. Broadening ISP liability is not an adequate solution to protect personal reputations. Some alternative ways can be considered. These measures should focus on preventing defamations in advance rather than providing recoveries for damages afterward. Promoting ethics among the Internet users, self-regulation measures voluntarily led by ISPs, by virtue of contractual relationships with their subscribers, are some soft measures that can contribute to accomplishing a pertinent balance. Although controversial, criminal sanctions against malicious and inveterate defamers might be one of these alternative measures, while it remains to be seen whether or not this can be an optimal implementation in balancing two conflicting values.



Discussion / 토론

## ***Mr. Kyung Oh Jung***

(Attorney at Law, Hanjung Partners)



정경오 변호사

(법무법인 한중)



## 온라인 매개자에 대한 거버넌스 체계

### ■ 거버넌스 체제

- 발제문에서 온라인 매개자에 대한 거버넌스 체계에 대하여 정부의 역할을 기준으로 조력자, 균등자, 제약자로서 기능하는 3가지 범주로 구분하고 있음
- 조력자로서 기능은 온라인 매개자에 대한 법적 책임이 거의 없는 경우로서 온라인 매개자들이 수행하는 기능을 촉진하는 역할
- 균등자로서 기능은 통지 및 삭제(notice and takedown)제도를 갖춘 경우로 권리자와 이용자 간 이익의 균형을 유지하는 역할
- 제약자로서 기능은 온라인 매개자들에게 특정행동이나 조치를 취하도록 명령함으로써 행위를 규제하는 역할

## 한국의 거버넌스 체계

- 온라인 매개자에 대한 한국의 거버넌스 체계는 일률적으로 정의할 수 없으나, 세 가지 범주가 공존하고 있음

### 1 진입규제

- 사업의 진입규제 측면에서는 전기통신사업법상 가장 완화된 진입규제인 신고제(notification)로 운영함으로써 진입에 있어 정부의 규제는 거의 없음

「전기통신사업법」

제22조(부가통신사업의 신고 등) ① 부가통신사업을 경영하려는 자는 대통령령으로 정하는 요건 및 절차에 따라 미래창조과학부장관에게 신고(정보통신망에 의한 신고를 포함한다)하여야 한다.

## 2 행위규제

### ① 사후규제

- 인터넷상 표현물에 대하여 사전에 심의를 하는 사전규제를 하지 않고 인터넷에 유통(게재)된 이후에 심의하는 사후규제 방식을 취하고 있음

#### 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」

제44조의7(불법정보의 유통금지 등) ① 누구든지 정보통신망을 통하여 다음 각 호의 어느 하나에 해당하는 정보를 유통하여서는 아니 된다. <개정 2011.9.15.>

1. 음란한 부호·문언·음향·화상 또는 영상을 배포·판매·임대하거나 공공연하게 전시하는 내용의 정보
2. 사람을 비방할 목적으로 공공연하게 사실이나 거짓의 사실을 드러내어 타인의 명예를 훼손하는 내용의 정보
3. 공포심이나 불안감을 유발하는 부호·문언·음향·화상 또는 영상을 반복적으로 상대방에게 도달하도록 하는 내용의 정보
4. 정당한 사유 없이 정보통신시스템, 데이터 또는 프로그램 등을 훼손·멸실·변경·위조하거나 그 운용을 방해하는 내용의 정보
5. 「청소년 보호법」에 따른 청소년유해매체물로서 상대방의 연령 확인, 표시의무 등 법령에 따른 의무를 이행하지 아니하고 영리를 목적으로 제공하는 내용의 정보
6. 법령에 따라 금지되는 사행행위에 해당하는 내용의 정보
7. 법령에 따라 분류된 비밀 등 국가기밀을 누설하는 내용의 정보
8. 「국가보안법」에서 금지하는 행위를 수행하는 내용의 정보
9. 그 밖에 범죄를 목적으로 하거나 교사(敎唆) 또는 방조하는 내용의 정보

#### 「방송통신위원회의 설치 및 운영에 관한 법률」

제21조(심의위원회의 직무) 심의위원회의 직무는 다음 각 호와 같다.

1. 「방송법」 제32조에 규정된 사항의 심의
2. 「방송법」 제100조에 따른 제재조치 등에 대한 심의·의결
3. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제44조의7에 규정된 사항의 심의
4. 전기통신회선을 통하여 일반에게 공개되어 유통되는 정보 중 건전한 통신윤리의 함양을 위하여 필요한 사항으로서 대통령령이 정하는 정보의 심의 및 시정요구
5. 전기통신회선을 이용하여 유통되는 정보의 건전화에 관한 사항
6. 심의위원회의 사업계획·예산 및 결산에 관한 사항
7. 심의위원회 규칙의 제정·개정 및 폐지에 관한 사항
8. 다른 법령에 의하여 심의위원회의 심의사항으로 정한 사항

## ② 본인확인제

- 2007년 6월 28일에 인터넷 이용자가 주민등록번호, 신용카드 인증 등을 통해 본인 확인을 받은 뒤 사이트에 글을 올리도록 하는 제도로서 본인확인후 게시판 등에는 다른 별명이나 ID를 사용할 수 있음
- 본인확인제는 개인의 표현의 자유, 개인정보 자기결정권 및 사업자의 언론의 자유를 침해한다는 이유로 2012년 8월 23일 헌법재판소에서 위헌결정을 받아 폐지됨

## ③ 임시조치

- 정보통신망을 통하여 일반에게 공개를 목적으로 제공된 정보로 사생활 침해나 명예 훼손 등 타인의 권리가 침해된 경우 그 침해를 받은 자는 해당 정보를 취급한 정보통신서비스 제공자(이하 ‘사업자’라 함)에게 침해사실을 소명하여 그 정보의 삭제 또는 반박내용의 게재(이하 “삭제등”이라 한다)를 요청할 수 있고, 사업자는 침해 여부를 판단하기 어렵거나 이해당사자 간에 다툼이 예상되는 경우에는 해당 정보에 대한 접근을 임시적으로 차단하는 조치
- 발제문에 따르면 임시조치는 비대칭 인센티브 구조의 대표적인 예라고 볼 수 있음
- 인터넷 표현의 자유를 증진하기 위하여 정보통신서비스 제공자의 임시조치에 대한 정보게재자의 이의제기 절차를 마련하고, 정보통신망을 통한 명예훼손 분쟁의 조정 기능을 강화하기 위하여 방송통신심의위원회에 온라인명예훼손분쟁조정위원회를 설치하며, 정보통신서비스 제공자의 임시조치에 대하여 이의제기가 있는 경우에는 온라인명예훼손분쟁조정위원회가 직권조정을 하도록 하는 개정안이 2014. 12. 29. 국회 제출된 상태
- 개정안은 법원을 통한 분쟁해결이 장시간이 소요되고 많은 비용을 부담한다는 점에서 시간과 비용이 경감되는 분쟁조정절차에 의한 분쟁해결을 시도함으로써 표현의 자유와 피해구제의 균형을 추구하고 있음



## 결론

- 한국은 저작권 분야에 있어서는 법원 중심의 거버넌스 체계를 유지하고 있고, 비저작권 분야에서는 방송통신심의위원회 중심의 거버넌스 체계를 구축하고 있음
- 비저작권 분야에서 정부의 역할 중 제약자 역할로 볼 수 있는 측면이 있는데, 본인 확인제 폐지, 임시조치 개정안 중 정보계재자의 이의제기권 인정, 정보계재자의 이의 제기 시 분쟁조정제도도 진행하게 함으로써 제약자에서 균등자로 정부의 역할이 변화 중